IT-security
for the new generation
International Students' Conference
KASPERSKY lab

II МЕЖДУНАРОДНАЯ СТУДЕНЧЕСКАЯ КОНФЕРЕНЦИЯ ПО ПРОБЛЕМАМ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

II INTERNATIONAL STUDENT CONFERENCE ON COMPUTER SECURITY ISSUES "IT SECURITY FOR THE NEW GENERATION"

Тезисы докладов

THESIS

www.kaspersky.com

Москва, 28-29 апреля 2009 г.

Moscow, 28-29 April 2009

Содержание:

Студенческая конференция по проблемам компьютерной безопасности «IT security conference for the new generation» 8
Программный комитет 10
Организационный комитет....11
Итоги конференции 13
1 **Секция Компьютерная преступность 16**
Кибersквоттинг
Базенков Д.Е. 16
Концепция компьютерной безопасности высшего учебного заведения
Бухаров И.В., Шкеда А. **19**
Компьютерная преступность в России
Гимазетдинов М.А. 21
Интернет-преступность
Дремлюга Р.И. 22
Компьютерная преступность
Заводсков А.Д. соавторы: Малышев В.В., Осокин Д.В., Данилов В.О., Уртемеева М.А. 26
Восприятие национального кибер закона: Распознавание образов в группах пользователей.
Имран Аскрения, Гамид Якаххани, Кристина Драгонова 28
Транснациональные Интернет-преступления : проблемы юрисдикции и особенности решений по законодательству России и Германии
Парамонова С.Л., LL.M. 37
Проблема правового регулирования
Печкуров А.В. 40
Методика обнаружения и классификации криптографически преобразованных файлов
Речицкий А.С. 41
Возможности кибернетического нарушителя по сохранению конфиденциальности своей информации и собственной анонимности перед лицом Государственных служб глобального электронного надзора
Шабанов А.В. 43
Компьютерные преступления и Российское законодательство
Шаймарданов Д.И. 46
2 **Секция Компьютерные угрозы. Угрозы для мобильных устройств 49**
Мобильные вирусы и технологии борьбы с ними
Алексеев И.С, Атапин А.В, Тухтаманов Д.В. 49
К вопросу уязвимостей Web-браузеров
Ануфриев А.В., Сидоров М.В. 50
Беспроводные сети Wi Fi. И их Безопасность
Босова М. 51
Защита flash-носителей от вредоносного программного обеспечения
Вальгер С.А., Сорокин Н.В. 58
Всесторонний анализ вируса Voidman
Эрденебат Чулуун 59
Разработка системы пассивного сбора событий сетевых атак (Honeypot): Bluetooth сети
Пустобаева Д. 60
Безопасность Ajax-приложений
Князев А.Д., Стуров А.С. 64
Ограничение привилегий неуправляемого кода в .NET Framework
Семенова Н.А. 72
3 **Секция Криптография. Её актуальность в современном обществе 76**

Симметричное и асимметричное шифрование
Гончаров Н.О. 76
Криптография. Ее актуальность в современном обществе
Егоров Г.В. 79
Кодирование информации на мобильных устройствах
Ершов Д.И. 80
Алгоритм шифрования ГОСТ 28147-89
Крайнов Н.А. 82
Разработка нового подхода к оценке эффективности криптографической защиты информации
Савельева А.А. 83
Метод защиты закрытого ключа при криптографической аутентификации в системах дистанционного обучения
Сергеева Е.Н. 91
Разработка средств защиты программного продукта «Учет проживающих в сельской местности» для территориального органа Федеральной службы государственной статистики по Республике Башкортостан «Башкортостанстат»
Фатхинуров А.Р. 93

4 **Секция Методы обнаружения и предотвращения компьютерных угроз 98**

Методы обнаружения и предотвращения инсайдерских компьютерных угроз в локальных вычислительных сетях
Баринов А.Е. 98
Создание методики распознавания сетевых соединений вредоносных программ
Голованов С.Ю. 101
Разработка фильтра - анализатора сетевых пакетов с функцией контроля приложений
Ишемгулов Р.Ф. 102
XSS и Iframe. Зараженные сайты. Опасности. Методы защиты
Калинин А.В. 104
Анализ руткит технологий под операционную систему Linux
Кожанов Е.А., Степина А.Н. 105
Метод проактивного обнаружения сетевых аномалий на основе реконструкции математической модели сетевого трафика
Копыстко А.Л., Саварцов А.В. 106
Обфускация
Коромысов С.Ю. 110
Служба реагирования предприятия на инциденты компьютерной безопасности
Космачев А.В. 111
Создание унифицированного средства защиты от угроз
Кукало И.А. 114
Активная система обнаружения опасных серверов
Логинов В.В. 118
Автоматизированная система защиты сайта, разработанного на языке программирования PHP с использованием сервера баз данных MySQL, от атак типа SQL-инъекция, PHP-инъекция и межсайтовый скриптинг лужба реагирования предприятия на инциденты компьютерной безопасности
Приходько М.А. 120
Проактивные методы защиты
Рашевский Р. 122
Защита программных продуктов: методы обфускации и деобфускации программного кода. Деобфускация вредоносного кода, написанного на JavaScript
Рой К.С. 123
Применения искусственных иммунных сетей в задачах детектирования вредоносного кода
Снегурский А.В. 128
Способы борьбы со скрытыми каналами
Халитова К.И. 130
Анализ протокола аутентификации Керберос, построенного с помощью "штампа времени", с использованием функций CSP-RANK
Йони Кирсал, Орхан Гемиконакли 134

Обмен электронными документами с ЭЦП по телекоммуникационным каналам связи в унифицированной системе приема, хранения и первичной обработки налоговых деклараций и бухгалтерской отчетности
Шалимов М.А. 154

5 Секция Образовательные проекты (программы и методики обучения) в области компьютерной безопасности 159

Учебный курс «Компьютерные угрозы: методы обнаружения и анализа»
Адамов А.С. 159

Учебная программная система для изучения методов криптографической защиты информации
Азизян Н.А., Косолапова Е.Н. 161

Формирование устойчивости к негативному влиянию интерне
Зорина И.В. 164

Обучение основам компьютерной безопасности младших школьников
Олевская Л.Н. 165

6 Секция Спам. Методы обнаружения спама с анализом содержимого и без него. Фишинг 168

Автоматизированный контент-анализ спам-сообщений на различных языках. Концептуальный анализ
Ермакова Л.М. 168

Методы обнаружения спама без анализа содержимого текста сообщения
Кириченко С. 173

Спам и методы его обнаружения. Фишинг
Сергеева А.М., Файзуллин Р.В. 180

Распознавание фишинговых веб-страниц без использования "черных" списков
Чувило Олег Александрович 182

7 Секция Средства анализа и тестирования 184

Система автоматического обнаружения ошибок в коде параллельных программ на языке Си++, использующих OpenMP (VivaMP)
Колосов А.П., Рыжков Е.А. 184

Компьютерный вирус как инструмент анализа и модернизации современных средств защиты
Приходько М.А. 186

8 Секция Экономические модели и аналитические аспекты информационной безопасности 189

Расчет финансовых потерь предприятий от деятельности вредоносных программ
Бочарникова М.В. 189

Некоторые подходы к обоснованию затрат на обеспечение системы информационной безопасности хозяйствующего субъекта
Курнавина Т.С. 192

Состояние рынка мобильных антивирусов: теоретические перспективы и практические методы. Особенности рынка платного мобильного контента и способы продвижения
Новоселов Н.А. 202

Экономические модели и аналитические аспекты информационной безопасности
Семенихина В.С. 207

Метод оценки экономической эффективности внедрения криптографических систем
Смирнов М.О. 209

Разработка генератора паролей на основе мнемонических формул
Шакирова Р.И. 215

Авторский указатель The authors 221

Contents:

Student Conference on Computer Security Issues «IT security conference for the new generation» 9
The Program Committee: 12
The Organizational Committee: 12
Conference result 15

1 **Computer crime 16**

Cybersquatting
Bazenkov D.E. 16

The concept of computer safety of a higher educational institution
Bukharov I.V., Shkeda A.I., 19

Computer crime in Russia
Gimazetdinov M.A. 21

Internet crime
Dremluga R.I. 22

Computer crime
Zavodskov A.D. co-author: Malyshev V.V., Osokin D.V., Danilov V.O., Urtemeeva M.A. 26

Perceptions of national Cyber law: Pattern recognition in Human groupings
Imran Askerniya, Hamid Jahankhani, Chrisina Draganova 28

Transnational Cybercrimes: Problems of Jurisdiction and Peculiarities of Solutions According to the Legislation of Russia and Germany
Paramonova S.L., LL,M. 37

Problem of legal regulation
Pechkurov A.V. 40

Technique for detecting and classifying cryptographically transformed files
Rechitskiy A. S. 41

Possibilities of a cybercriminal preserving confidentiality of information and own anonymity in the face of Public services of global electronic supervision
Shabanov A.V. 43

Computer crimes and Russian Legislation
Shaimardanov D.I. 46

2 **Computer threats and threats targeting mobile devices 49**

Transportable viruses and technologies of struggle against them
Alekseev I.S., Atapin A.V., Tuhtamanov D.V. 49

On the problem of Web-browser vulnerabilities
Anufriev A.V., Sidorov M.V. 50

Wireless networks Wi Fi. And their Safety
Bosova M. 51

The security of flash-mediums against of the malicious software
Val'ger S.A., Sorokin N.V. 58

"Voidman" virus comprehensive analysis
Erdenebat Chuluun 59

System development of passive collection of events network attacks (Honeypot): Bluetooth networks
Pustobaeva D. 60

Safety of Ajax-appendices
Knyazev A.D., Sturov A.S. 64

Enabling security restrictions for unmanaged code in .NET Framework
Semenova N.A. 72

3 **Cryptography and its relevance today 76**

Symmetric and asymmetric encryption
Goncharov N.O. 76

Cryptography and its relevance today
Egorov G.V. 79
The coding of information on mobile devices
Ershov D.I. 80
Algorithm of enciphering GOST 28147-89
Krainov N.A. 82
A new Approach to the problem of evaluating the efficiency of cryptographic systems
Savelieva A.A. 83
Method of protecting a closed key with cryptographic authentication in systems of remote training
Sergeeva E.N. 91
Development of the protection software "The Accountant living in the countryside" for the Federal Service for State Statistics of the Republic of Bashkortostan (Bashkortostanstat)
Fathinurov A.R. 93

4 **Methods used to detect and prevent computer threats.....98**

Methods of detecting and preventing insider computer threats in local area networks (LAN)
Barinov A.E. 98
Creating a methodology for recognizing malware network connections
Golovanov S.Y. 101
Filter dvelopment - analysing network packages with the control of appendices function
Ishemgulov R.F. 102
XSS and Iframe. Infected sites. Dangers. Protection methods
Kalinin A.V. 104
Rootkit analysis technologies under Linux operating systems
Kojanov E.A.,Stepina A.N. 105
Method of proactive anomaly detection using a reconstructed mathematical model of network traffic
Kopystko A.L., Savartsov A.V. 106
Obfuscation
Koromysov S.Y. 110
Enterprise response service to incidents of computer safety
Kosmachev A.V. 111
Creation of a unified threat management system
Kukalo I.A. 114
Active system for detecting dangerous servers
Loginov V.V. 118
An automated security system for a web-site developed using PHP and MySQL, protecting against SQL-injection, PHP-injection and Cross Site Scripting
Prihodko M.A. 120
Proactive methods of protection
Rashevsky R. 122
Protection of software products: methods of obfuscating and deobfuscating a program code. Debfuscation of harmful code written on JavaScript
Roy K.S. 123
Application of artificial immune networks in problems of detecting of malware code
Snegursky A.V. 129
Ways of combating hidden channels
Khalitova K.I. 130
Analysing the Kerberos timed authentication protocol using CSP-RANK functions
Yoney Kirsal and Orhan Gemikonakli 134
Exchange of electronic documents with the electronno-digital signature on telecommunication channels in a unified system for receiving, storing and processing tax declarations and accounting reports
Shalimov M.A. 154

5 **Educational projects (training programs and methods) in computer security.....159**

Training course "Computer threats: detection and analysis methods"
Adamov A.S. 159

Educational software system for research into methods of the cryptographic protection of information
Azizyan N.A., Kosolapova Y.N. 161
Developing resistance to the negative effects of the Internet
Zorina I.V. 164
Teaching primary school children the basics of computer security
Olevskaya L.N. 165

6 **Spam: detecting spam with and without content analysis. Phishing 168**

The automated content-analysis of spams messages in various languages. A conceptual analysis
Ermakova L.M. 168
Methods of detecting spam without analysis of the message text
Kirichenko S. 173
Spam: detecting spam with and without content analysis. Phishing
Sergeeva A.M., Fayzullin R.V. 180
Detection of phishing web pages without using blacklist's
Chuvilo O.A. 182

7 **Analyzing and testing modern means of protection 184**

System for the autodetection of errors in code of parallel programs in the C++ language using OpenMP (VivaMP)
Kolosov A.P., Ryzhkov E.A. 184
The computer virus as an instrument for analysing and modifying modern security systems
Prihodko M.A. 186

8 **Economic models and analytical aspects of IT security 189**

Calculation of an enterprise's financial losses caused by malware activities
Bocharnikova M.V. 189
Some approaches to a substantiation of expenses for system of information safety
Kurnavina T.S. 192
The state of the transportable antiviruses market: theoretical perspectives and practical methods. Features of the paid mobile content market and methods of advancement
Novoselov N.A. 202
Economic models and analytical aspects of information safety
Semenihina V.S. 207
Method for estimating the economic efficiency of introducing cryptographic systems
Smirnov M.O. 209
Development of a password generator on the basis of mnemonic formulas
Shakirova R.I. 215

Авторский указатель The authors 221

Студенческая конференция по проблемам компьютерной безопасности «IT security conference for the new generation»

Цель конференции:

Объединить специалистов, молодых ученых, исследователей, изучающих проблемы компьютерной безопасности для обмена опытом, развития инноваций и повышения уровня безопасности в сфере информационных технологий. Обеспечить поддержку молодых ученых для развития исследований в области ИБ.

Даты проведения:

Заочный тур: 01 ноября 2008 г. – 15 марта 2009 г.

Подача работ для участия в конференции до 15 марта 2009 года

Оценка работ программным комитетом: до 03 апреля 2009 года

Очный тур: 27-29 апреля 2009 г., г. Москва, офис «Лаборатории Касперского»

Организаторы: ЗАО «Лаборатория Касперского».

Темы конференции:

- Компьютерная преступность.
- Криптография. Актуальность в современном обществе.
- Компьютерные угрозы. Угрозы для мобильных устройств.
- Спам. Методы обнаружения спама с анализом содержимого и без него. Фишинг.
- Методы обнаружения и предотвращения компьютерных угроз.
- Средства анализа и тестирования современных средств защиты.
- Образовательные проекты (программы и методики обучения) в области компьютерной безопасности.
- Экономические модели и аналитические аспекты информационной безопасности.

Student Conference on Computer Security Issues
«IT security conference for the new generation»

The goal of this conference is to bring together students, young experts, scientists and researchers examining computer security issues in order to share experience, develop new ideas and improve the level of security in information technology. The conference is also meant to support young scientists and research in information security.

Dates:

Pre-conference deadlines – Round 1: 1 November 2008 – 15 March 2009

Papers for conference attendance must be submitted by 15 March 2009.

Papers will be evaluated by the program committee by 03 April 2009.

Conference – Round 2: 27-29 April 2009, Moscow, Kaspersky Lab

Organizers: Kaspersky Lab

Conference Topics:

- Computer crime.
- Cryptography and its relevance today.
- Computer threats and threats targeting mobile devices.
- Spam: detecting spam with and without content analysis. Phishing.
- Methods used to detect and prevent computer threats.
- Analyzing and testing modern means of protection.
- Educational projects (training programs and methods) in computer security.
- Economic models and analytical aspects of IT security

Программный комитет

1. **Абрамов Сергей Владимирович**, тест-менеджер группы тестирования и управления качеством ЗАО «Лаборатория Касперского»
2. **Березин Борис Иванович**, кандидат физико-математических наук, заместитель декана факультета вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова
3. **Волков Дмитрий Владимирович**, главный редактор журнала «Открытые системы»
4. **Гребенников Николай Андреевич**, директор по исследованиям и разработке ЗАО «Лаборатория Касперского»
5. **Гужов Андрей Владимирович**, старший разработчик отдела разработки общих компонент ЗАО «Лаборатория Касперского»
6. **Хамид Джаханкани (Hamid Jahankhani)**, заместитель декана, факультет компьютеризации, информационных технологий и инженерного дела, Университет Восточного Лондона (Великобритания)
7. **Загребин Максим Андреевич**, разработчик отдела разработки общих компонент ЗАО «Лаборатория Касперского»
8. **Ершов Игорь Валерьевич**, кандидат физико-математических наук, доцент кафедры информационных систем и технологий, Новосибирский государственный архитектурно-строительный университет
9. **Ефимова Светлана Николаевна**, руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского»
10. **Медведев Николай Викторович,** кандидат технических наук, доцент, заведующий кафедрой информационной безопасности, Московский государственный технический университет им. Н.Э. Баумана
11. **Мельников Николай Викторович**, доктор технических наук, профессор, заведующий кафедрой информационной безопасности, Российский государственный социальный университет
12. **Миронов Андрей Михайлович**, кандидат физико-математических наук, старший научный сотрудник кафедры математической теории интеллектуальных систем и лаборатории проблем теоретической кибернетики механико-математического факультета, МГУ им. М. В. Ломоносова
13. **Минзов Анатолий Степанович**, доктор технических наук, профессор, заведующий кафедрой «Комплексная безопасность бизнеса», Институт безопасности бизнеса Московского энергетического института (ТУ)
14. **Никишин Андрей Викторович**, директор антиспам-лаборатории ЗАО «Лаборатория Касперского»
15. **Новиков Сергей Валерьевич**, менеджер по работе с внешними структурами отдела антивирусных исследований ЗАО «Лаборатория Касперского»
16. **Петров Вячеслав Александрович**, кандидат технических наук, доцент, заместитель декана факультета информационной безопасности, Московский инженерно-физический институт (государственный университет)
17. **Трубникова Елена Владимировна**, старший инженер по тестированию группы тестирования и управления качеством ЗАО «Лаборатория Касперского»
18. **Хеннес Федерат (Hannes Federrath)**, профессор университета г. Регенсбурга и глава исследовательской группы по управлению информационной безопасностью департамента информационных систем
19. **Стивен Фёрнелл (Steven Furnell)**, профессор Центра информационной безопасности и исследования сетей университета г. Плимут (Великобритания) и по совместительству профессор университета им. Эдит Коуэн (Австралия)

20. **Хаханов Владимир Иванович**, профессор, доктор технических наук, декан факультета компьютерной инженерии и управления, Харьковский национальный университет радиоэлектроники
21. **Шевченко Станислав Борисович**, заместитель директора департамента исследований и разработки ЗАО «Лаборатория Касперского»

Организационный комитет

1. **Горелова Анастасия Ивановна**, координатор образовательных программ ЗАО «Лаборатория Касперского».
2. **Ефимова Светлана Николаевна**, руководитель направления по работе с образовательными учреждениями ЗАО «Лаборатория Касперского».
3. **Бацкова Кристел**, менеджер образовательных программ «Лаборатории Касперского» в Европе.

The Program Committee:

1. **Anatoly Minzov**, PhD in Technical Sciences, the Head of the Division of Complex security of business, Moscow State Institute of business security.
2. **Andrey Nikishin**, Director of Kaspersky Lab's Anti-Spam Lab.
3. **Andrey Guzov**, Senior Developer, Kaspersky Lab.
4. **Andrey Mironov**, Candidate of Physics and Mathematics under the Division of the mathematical theory of intellectual systems and laboratory of Problems of theoretical cybernetics, Moscow State University.
5. **Dmitry Volkov**, Editor, Open System Magazine.
6. **Elena Trubnikova**, Senior Testing Engineer, Kaspersky Lab.
7. **Hannes Federrath**, Professor at the University of Regensburg and Head of the Research Group "Management of IT Security" at the Department of Information Systems, PhD.
8. **Steven Furnell**, Professor, the Center for Information Security & Network Research at the University of Plymouth in the United Kingdom, and an Adjunct Professor with Edith Cowan University in Australia.
9. **Igor Ershov**, Candidate of Physics and Mathematics under the Division of Information Systems and Technologies at Novosibirsk State University of Architecture and Construction.
10. **Dr. Hamid Jahankhani**, Associate Dean, School of Computing, Information Technology and Engineering, University of East London (UK).
11. **Maxim Zagrebin**, Senior Developer, Kaspersky Lab.
12. **Nikolay Grebennikov**, Vice-president Research & Development, Kaspersky Lab.
13. **Nikolay Medvedev**, Candidate of Technical Sciences, Associate Professor and Head of the Division for Information Security at the Bauman Moscow State Technical University.
14. **Nikolay Berezin**, Candidate of Physics and Mathematics under the Division, Assistant Dean of the Division of mathematics and cybernetics, Moscow State University.
15. **Prof. Nikolay Melnikov**, PhD in Technical Sciences, Head of the Division of Information Security at the Russian State Social University.
16. **Prof. Vladimir Khakhanov**, PhD in Technical Sciences and Dead of the Computer Engineering and Management Division at the Kharkov National University of Radio-electronics.
17. **Sergey Novikov**, Manager of corporate communication under Kaspersky Lab's Antivirus Research Department.
18. **Sergey Abramov**, Test Engineering Group Manager, Kaspersky Lab.
19. **Stanislav Shevchenko**, Deputy Vice-president Research & Development, Kaspersky Lab.
20. **Svetlana Efimova**, Director of Collaboration with Educational Institutions, Kaspersky Lab.
21. **Vyacheslav Petrov**, Candidate of Technical Sciences, Associate Professor and Assistant Dean of the Information Security Division at the Moscow Engineering and Physics Institute (a state university).

The Organizational Committee:

1. **Anastasiya Gorelova**, Kaspersky Lab Educational Program Coordinator.
2. **Svetlana Efimova**, Director of Collaboration with Educational Institutions, Kaspersky Lab.
3. **Christel Bazkowa**, Educational manager Europe.

Итоги конференции

Лучшие работы заочного тура конференции по результатам оценки программного комитета

Ф.И.О.	Название работы	Номинация	Город
Сергеева Елена	Метод защиты закрытого ключа при криптографической аутентификации в системах дистанционного обучения	Криптография, актуальность в современном обществе	Москва, Россия
Парамонова Светлана Леонидовна	Транснациональные Интернет-преступления: проблемы юрисдикции и особенности решений по законодательству России и Германии	Компьютерная преступность	Фрайбург, Германия
Князев Артем Дмитриевич, Стуров Алексей.	Безопасность Ajax-приложений	Компьютерные угрозы, угрозы для мобильных устройств	Самара, Россия
Чувило Олег	Распознавание фишинговых веб-страниц без использования "черных" списков	Спам, методы обнаружения спама с анализом содержимого и без него, фишинг	Харьков
Баринов Андрей	Методы обнаружения и предотвращения инсайдерских компьютерных угроз в локальных вычислительных сетях	Методы обнаружения и предотвращения компьютерных угроз	Челябинск, Россия
Приходько Максим Александрович	Компьютерный вирус как инструмент анализа и модернизации современных средств защиты	Средства анализа и тестирования современных средств защиты	Москва, Россия
Семенихина Варвара Сергеевна	Экономические модели и аналитические аспекты информационной безопасности	Экономические модели и аналитические аспекты информационной безопасности	Пермь, Россия
Азизян Нина Ашотовна, Косолапова Елена Николаевна	Учебная программная система для изучения методов криптографической защиты информации	Образовательные проекты (программы и методики обучения) в области компьютерной безопасности	Ереван, Армения

Лучший доклад очного тура конференции

Ф.И.О.	Название работы	Номинация	Город
Смирнов Михаил	Метод оценки экономической эффективности внедрения криптографических систем	Экономические модели и аналитические аспекты информационной безопасности	Нижний Новгород, Россия
Yoney Kirsal	Analysing the Kerberos timed authentication protocol using CSP-RANK funktions	Методы обнаружения и предотвращения компьютерных угроз	London, United Kingdom
Рой Константин Сергеевич	Защита программных продуктов: методы обфускации и деобфускации программного кода. Деобфускация вредоносного кода, написанного на JavaScript	Методы обнаружения и предотвращения компьютерных угроз	Пермь, Россия

Conference result

The best paper 1-th round

Author name	Title	Conference Topics	City
Sergeeva E.N.	Method of protecting a closed key with cryptographic authentication in systems of remote training	Cryptography and its relevance today	Moscow, Russia
Paramonova S.L.	Transnational Cybercrimes: Problems of Jurisdiction and Peculiarities of Solutions According to the Legislation of Russia and Germany	Computer crime	Freiburg, Germany
Knyazev A.D., Sturov A.S.	Safety of Ajax-appendices	Computer threats and threats targeting mobile devices	Samara, Russia
Chuvilo O.A.	Detection of phishing web pages without using blacklist's	Spam: detecting spam with and without content analysis. Phishing	Kharkov, Ukraine
Barinov A.E.	Methods of detecting and preventing insider computer threats in local area networks (LAN)	Methods used to detect and prevent computer threats	Chelyabinsk, Russia
Prihodko M.A.	The computer virus as an instrument for analysing and modifying modern security systems	Analyzing and testing modern means of protection	Moscow, Russia
Semenihina V.S.	Economic models and analytical aspects of information safety	Economic models and analytical aspects of IT security	Perm, Russia
Azizyan N.A., Kosolapova Y.N.	Educational software system for research into methods of the cryptographic protection of information	Educational projects (training programs and methods) in computer security	Erevan, Armenia

The best speaker 2 round

Author name	Title	Conference Topics	City
Mikhail Smirnov	Method for estimating the economic efficiency of introducing cryptographic systems	Economic models and analytical aspects of IT security	Nizhny Novgorod, Russia
Yoney Kirsal	Analysing the Kerberos timed authentication protocol using CSP-RANK funktions	Methods used to detect and prevent computer threats	London, United Kingdom
Konstantin Roy	Protection of software products: methods of obfuscating and deobfuscating a program code. Debfuscation of harmful code written on JavaScript	Methods used to detect and prevent computer threats	Perm, Russia

1 Секция

Компьютерная преступность

Computer crime

Кибersквоттинг

Базенков Д.Е.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
ank@ssau.ru

Cybersquatting

Bazenkov D.E.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
ank@ssau.ru

Домен нельзя купить в собственность, вы можете лишь зарегистрировать доменное имя на юридическое или физическое лицо на определенный период времени. По истечении этого периода регистрацию доменного имени необходимо продлять. В случае если владелец домена не оплатил продление доменного имени в течение 30-45 суток (для разных зон — разные правила), домен сможет зарегистрировать любой желающий. Услугу по регистрации и продлению доменного имени предоставляет компания регистратор. Зарегистрированные домены можно передавать в пользование другим лицам и компаниям — это «вторичный» рынок доменов.

Ценность доменов второго уровня, как самых востребованных, определяется тем, из каких слов он состоит, а также принадлежностью к той или иной зоне. Наиболее востребованы, следовательно, и дороги домены второго уровня в международной зоне com. Если слова, из которых состоит имя домена, являются «ключевыми», то ценность такого домена резко возрастает. «Ключевыми» называют слова, которые наиболее часто вводят пользователи в строке поисковых систем: business, car, hotel, food, sell, rent, photo, fly, electronics, poker, traffic и т. д. Ценность имеют двух- и трехсимвольные домены. Их количество ограничено и, во-первых, домен, состоящий из двух-трех символов легко запомнить, а во-вторых, названия многих крупных компаний складываются в двух- и трехсимвольные аббревиатуры.

Людей, регистрирующих доменные имена с целью перепродажи, называют «кибersквоттерами» (от английского слова «squat» — самовольный захват земли). Тысячи людей по всему миру занимаются или пытаются заниматься бизнесом, связанным с перепродажей доменов. Кто-то едва сводит концы с концами, небольшая часть зарабатывает себе на жизнь и лишь единицы зарабатывают на этом сотни тысяч долларов.

Что нужно, чтобы заработать на доменных именах? Во-первых, зарегистрировать ценное доменное имя, желательно чтобы это было ключевое слово в одной из популярных зон. Во-вторых, найти компанию или человека, для которого это доменное имя особенно ценно, и он готов заплатить за него сумму, превышающую сумму регистрации. Однако чаще все происходит с точностью до наоборот — заинтересованные лица сами обращаются к владельцам с предложением продажи домена. Простой пример: домен vodka.com был продан компании «Русский стандарт» за 3 миллиона долларов. Это притом, что регистрация доменного имени в зоне com на год стоит 13 долларов. Конечно же, не все так просто, и большинство «ключевиков» в популярных зонах уже заняты, но баснословные прибыли и азарт, возникающий в процессе поиска, компенсируют все минусы этого бизнеса.

Всего можно выделить четыре вида кибersквоттинга:

- брендовый кибersквоттинг;
- географический кибersквоттинг;
- отраслевой кибersквоттинг;
- тайпсквоттинг.

- это поиск и регистрация (перехват) доменных имен по написанию совпадающих с названиями известных товарных знаков, фирменных наименований или совпадающих с именами известных персон.

Согласно законодательству Российской Федерации, товарный знак имеет приоритет перед доменным именем, то есть владелец товарного знака может запретить использование своего знака в доменном имени. Фактически это означает возможность отобрать домен у кибersквоттера.

Отобрать домен, т.е. признать регистрацию недействительной и получить приоритет при последующей регистрации домена можно только на основании вынесенного судебного решения. Такая процедура разрешения доменных споров означает возникновение значительных судебных издержек, и поэтому зачастую компании предпочитают договориться с кибersквоттерами о выкупе интересующего их домена.

- это поиск и регистрация (перехват) доменных имен связанных, с какой либо местностью или географическим объектом. Почти у каждого города есть сайт. Для крупных городов сайтов может быть несколько, для Москвы, например, есть сайты отдельных районов города. Такие домены интересны туристическим фирмам (по понятной причине), а также компаниям чье название совпадает с названием географического объекта (частое явление). Обладание географическим доменом позволит постоянно получать тематический трафик. Раскрутить такой домен проще - лучше запоминается.

- это поиск и регистрация (перехват) доменных имен связанных, с какой либо отраслью экономики или названиями товаров и услуг. Отраслевой ки-бersквоттинг - наиболее выгодный вид кибersквоттинга.

Составляющие коммерческого успеха здесь следующие:

- получение трафика за счет набора транслита в адресную строку браузера;
- престижность обладания таким доменом;
- легкая запоминаемость домена пользователями Интернет;
- лучшее ранжирование в выдаче поисковых систем (ключевое слово в имени домена).
- юридическая чистота домена, на слово, вошедшее во всеобщее употребление нельзя зарегистрировать товарный знак, следовательно, и выиграть доменный спор в суде тоже нельзя.
- Ценность отраслевого домена зависит от многих факторов:
- распространенность доменного имени - количество поисковых запросов с таким словом;
- развитость рынка или отрасли, к которым этот домен принадлежит;
- проникновение рынка или отрасли в Интернет, количество потенциальных клиентов, пользующихся Интернет;
- количество участников рынка или отрасли, инвестирующих в Интернет рекламу значительные средства.

- это поиск и регистрация (перехват) доменных имен созвучных созвучных крупным торговым маркам или созвучным крупным, раскрученным проектам в Интернет. При регистрации такого момента существует возможность получения части посетителей ресурса, к которому регистрируется такой домен.

Тайпсквоттинг основан на использовании «человеческого фактора» -ошибок (опечаток), которые возникают при наборе доменного имени.

В связи со стремительным развитием сети Интернет в России и во всем мире, проблема кибersквоттинга встает достаточно остро. На данный момент в России накоплена значительная судебная практика по доменным спорам,

что позволяет ссылаться на уже вынесенные судебные решения при рассмотрении дела в суде. В различное время становились предметом громкого судебного разбирательства, следующие доменные имена:

- Mosfilm.ru
- Kodak.ru
- Quelle.ru
- Kamaz.ru
- Coca-cola.ru
- Sprite.ru
- Miele.ru
- Ntv.ru
- Baxter.ru
- Megashop.ru
- Kapel.ru

Однако крупные компании зачастую предпочитают не судиться, а выкупать доменные имена у кибersквоттеров, принося им баснословные прибыли. Одно ясно точно - когда будет создана доменная зона .рф - эта война разгорится с новой силой.

1. http://wwhois.m/?urls=32 - Доменный бизнес или кто такие кибersквот-теры.
2. http://ru.wikipedia.org/wiki/KH6epcKBOTTHHr - Кибersквоттинг
3. http://cybersquatting.ru/ - Виды кибersквоттинга, рынок купли продажи

Концепция компьютерной безопасности высшего учебного заведения

Бухаров И.В., Шкеда А.

Сибирский государственный технологический университет
г. Красноярск, Россия
shkeda_ai2005@mail.ru

The concept of computer safety of a higher educational institution

Bukharov I.V., Shkeda A.I.

The Siberian state technological university
Krasnoyarsk, Russia
shkeda_ai2005@mail.ru

The essence of the given work consists in search of parameters which should characterize any system of information safety of a higher educational institution of Russia. In work specificity of the Russian educational institutions and the requirement shown for developed system of computer safety is considered.

Now more and more actual there is a theme of computer safety of the Russian Institute of higher education, the general tendency of transition to the centralized storage of the information is observed.

There is a problem of protection of the information, an information field, office-work transition in the electronic form.

Because in our country long time nobody thought of the given problem of high-grade, complex techniques with reference to Institute of higher education does not exist.

On an example of own university we will consider, how the system of electronic control by educational activity functions. At the system analysis, the basic sources of threats come to light, their analysis is carried out, and substantive provisions which are developed the developed system of information safety should answer.

The main feature of the given system of safety would be its orientation on protection of an information field of an educational institution. Such software would be created especially for Institute of higher education, and carried in itself all specificity of the organization of protection of the information of any university of Russia.

World tendencies show on necessity of transition of office-work for the electronic form. It will help to raise essentially the international rating of Russia of an index so-called «electronic development».

Суть данной работы состоит в поиске параметров, которые должны характеризовать любую систему информационной безопасности высшего учебного заведения России. В работе учитывается специфика российских учебных заведений и требования, предъявляемые для разрабатываемой системы компьютерной безопасности.

В настоящее время все более актуальной становится тема компьютерной безопасности российских ВУЗов, наблюдается общая тенденция перехода на централизованное хранение информации.

Возникает проблема защиты информации, информационного пространства, перевода делопроизводства в электронную форму.

В связи с тем, что в нашей стране долгое время никто не задумывался над данной проблемой полноценных, комплексных методик применительно к ВУЗам не существует.

На примере собственного университета мы рассмотрим, как функционирует система электронного управления учебной деятельностью. При анализе системы, выявляются основные источники угроз, проводится их анализ, и разрабатываются основные положения которым должна отвечать разрабатываемая система информационной безопасности.

Главной особенностью данной системы безопасности являлось бы ее направленность на защиту информационного пространства учебного заведения. Такое программное обеспечение создавалось бы специально для ВУЗа, и несло в себе всю специфику организации защиты информации любого университета России.

Мировые тенденции показывают на необходимость перехода делопроизводства в электронную форму. Это поможет существенно повысить международный рейтинг России индекса так называемого «электронного развития».

Компьютерная преступность в России

Гимазетдинов М.А.

Елабужский государственный педагогический университет
г. Менделеевск, Россия
carma2004@mail.ru , marat_1983@mail.ru

Computer crime in Russia

Gimazetdinov M.A.

Elabuzhsky state pedagogical university
Mendeleevsk, Russia
carma2004@mail.ru , marat_1983@mail.ru

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего вычислительных систем. Это дает основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Компьютерная преступность в России становится одним из наиболее опасных видов преступных посягательств. Согласно экспертным оценкам, она способна нанести ущерб, сопоставимый с объемом хищений произведений искусства во всем мире.

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого внедрения во все сферы жизни общества электронно-вычислительной техники. Она служит не только для хранения и обработки соответствующей информации на уровне отдельных управленческих или хозяйственных единиц или использования как средства связи между гражданами, но и широко внедряется в целях обеспечения внутренней и внешней безопасности государства.

Но развертывание научно-технической революции обусловливает не только коренные прогрессивные изменения в составе факторов экономического развития России, но и негативные тенденции развития преступного мира, приводит к появлению новых форм и видов преступных посягательств. Это ярко проявляется в том, что преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники.

Особую тревогу в этом плане вызывает факт появления и развития в России нового вида преступных посягательств, ранее неизвестных отечественной юридической науке и практике и связанный с использованием средств компьютерной техники и информационно-обрабатывающих технологий - компьютерных преступлений.

Наибольшую опасность представляет компьютерная преступность в финансовой сфере. Отмечается тенденция к росту компьютерных преступлений в банковской сфере.

Это небольшое исследование, поможет наверняка новичкам – предусмотреть и предвидеть угрозы, которые их могу ожидать в нашем «современном компьютерном мире».

Интернет-преступность

Дремлюга Р.И.

Дальневосточный государственный университет
г. Владивосток
dreamluck@mail.ru

Internet crime

Dremluga R.I.

Far Eastern National University
Vladivostok, Russia
dreamluck@mail.ru

Annotation: The author describes the most uninvestigated socially dangerous phenomenon Internet crime. The main features of this new form of crime in Russia are researched in this monograph. General results of author's study are theoretical analysis of the state, the structure and the dynamic of Internet crime in Russia, basic offender's and victim's portraits, representation of hacker's subculture etc. it can be used for Internet crime prevention, prosecution and counteraction.

Стремительное внедрение цифровых технологий во все сферы человеческой жизни в конце XX – начале XXI вв. предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая соединила людей по всему земному шару, сделала коммуникации дешевыми и беспрепятственными и открыла новые горизонты для всего мирового сообщества. Интернет в последнее время дал человеку безграничные возможности в области передачи, распространения и рассылки информации, позволил выполнять финансово-банковские операции, несмотря на расстояния и границы. Интернет стал не просто технологией, а уникальным новшеством, изменившим мир.

Представляется, что кроме положительного эффекта появление Интернет содержит ряд отрицательных моментов и приводит к негативным последствиям. Некоторые особенности данной технологии, которые помогли ей распространиться по всему миру, в то же время создают благоприятные возможности для многих видов преступной деятельности. Новизна общественных отношений, возникших в результате появления Интернет, и отсутствие соответствующего правового поля, касающегося данной технологии, привели к множеству проблем, отрицательно влияющих на становление отношений в мировой компьютерной сети, основанных на законе.

Вызывает опасение, что огромный технический потенциал и безграничные возможности Интернет все чаще в современных условиях могут быть использованы в преступных целях. При этом Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные мировому сообществу еще совсем недавно виды общественно опасных посягательств.

Анализ статистических данных о преступности в сфере компьютерной информации показывает, что с 1997 по 2005 гг. в России количество зарегистрированных преступлений в сфере компьютерной информации (Глава 28 УК РФ) выросло более чем в 300 раз и достигло около 10000 преступлений за год. Хотя в 2006-2007 гг. наблюдается снижение регистрируемых преступлений, в 2008 году количество, зарегистрированных преступлений опять выросло на 24,5%. Из года в год растет применение компьютерных технологий для совершения широкого круга преступлений (например, ст. ст. 146, 159, 242 УК РФ и т.д.). Интернет активно используется преступными элементами, широко распространены в сети сайты террористических организаций, рекламирующие и продающие наркотики и оружие, публикующие порнографические материалы, а также порталы расистской, националистской, экстремистской направленности и другие преступно ориентированные Интернет-ресурсы.

Высокая социальная опасность преступлений в Глобальной сети вытекает, прежде всего, из их транснационального характера, так как последствия подобных деяний могут охватывать неограниченный круг лиц в самых разных странах. При этом количество пользователей Интернет во всем мире в 2009 г. насчитывает около двух миллиардов и продолжает в наши дни стремительно

увеличиваться, что предполагает дальнейший рост возможного ущерба, причиненного Интернет-преступлениями.

Необходимо отметить, что недостаток комплексных исследований, высокая латентность, как и отсутствие официальной статистки Интернет-преступности в России, приводят к неэффективности выработанных мер предупреждения, которые носят фрагментарный и противоречивый характер, предопределяя трудности в противодействии и борьбе с данным видом общественно опасных деяний. Как правило, в существующих на данный момент исследованиях не подвергалась анализу криминологическая характеристика преступности в Интернет. Чаще всего авторы останавливались на изучении уголовно-правовых проблем преступлений, предусмотренных в Главе 28 УК РФ. Другие виды общественно опасных деяний, которые благодаря информационным технологиям вышли на новый качественный и количественный уровни, ими не затрагивались, а если в некоторых работах и давалась общая криминологическая характеристика компьютерной преступности, то она практически не отражала особенностей Интернет-преступности.

Существующие работы освещали проблему лишь частично и не касались таких важных для Интернет-преступности вопросов, как особая криминальная субкультура сетевых преступников, детерминация современной Интернет-преступности; анализ характеристики личности преступника и потерпевшего; глубоко не исследовались и другие социально-значимые аспекты, связанные с Интернет-преступностью.

В представленной монографии рассматривается Интернет-преступность как негативное социальное явление, влияющие на нее процессы, а также характер воздействия на Интернет-преступность и возможные следствия подобного воздействия. Целью работы было выявление детерминирующих факторов и особенностей характеристики современной российской Интернет-преступности, криминологическая оценка ее основных показателей, разработка системы уголовно-правовых и криминологических мер профилактики и противодействия.

Согласно этой общей цели автором решались следующие задачи:

- провести исторический анализ формирования и становления Интернет-преступности;
- проанализировать криминологические характеристики Интернет-преступности за последнее десятилетие в РФ;
- выявить характеристики личности Интернет-преступника в зависимости от вида совершаемого деяния;
- выявить виктимологические факторы, влияющие на совершение Интернет-преступлений ;
- провести анализ преступной субкультуры и ее роли в развитии и воспроизводстве Интернет-преступности;
- выявить общие и специфичные детерминанты Интернет-преступности в РФ;
- определить основные направления мер по борьбе с преступностью в Глобальной сети;
- разработать меры и рекомендации по предупреждению и борьбе с Интернет-преступностью в РФ.

Эмпирической базой научной работы стали статистические данные, полученные в ГИАЦ МВД России, ИЦ УВД Приморского края, материалы 137 уголовных дел Хабаровского и Приморского краев, Камчатской области по статьям Главы 28 УК РФ за 2002-2007 гг. Характеристика 144 лиц, выявленных в ходе следствия по данным уголовным делам легла в основу исследования личности преступника (всего в за эти годы в ДФО около 400 лиц). Для анализа личности потерпевших взяты 42 дела, содержавшие подробные сведения о жертвах Интернет-посягательств. Также были проанкетированы разные группы населения (363 человека): 1) специалисты в компьютерных технологиях – компьютерные «Профессионалы» (127 чел.); 2) не имеющие образования в сфере информационных технологий, но пользующиеся Интернет, – «Гуманитарии» (149 чел.); 3) не умеющие и никогда не пользующиеся Интернет (87 чел.).

Было изучено в динамике последних лет более 2000 сайтов антисоциального и преступного содержания, в том числе для исследования доступности сведений и средств, облегчающих совершение преступлений в сфере компьютерной информации (1200 сайтов); «хакерской» субкультуры (257 сайтов); наркопреступности в Интернет (200 сайтов), террористической деятельности в Интернет (126 сайтов) и т.д.

Для поиска сайтов преступной направленности использовались популярные общедоступные российские поисковые системы. Проанализированы материалы 114 уголовных дел по компьютерным преступлениям за рубежом, взятых с официального сайта департамента юстиций США, и других Интернет-ресурсов.

Проведено исследование 27 фильмов («Hackers», «Трон», «Сеть», «Взломщик» и др.); более 100 книг («Библия хакера», «Лабиринт отражения», «Дневник злобного хакера», «The art of deception», «The hacker's hadbook», «The hacker crackdown», «The Little Black Book of Computer Viruses» и другие); 24 песен («Про кардера Джекса», «О хакерах», «Вовка Хаккерр»), Интернет-сайты (257 - ресурсов); 14 периодических изданий («Хакер», «2600», «Phrack», «K-1ine» и т.д.) и других значимых для субкультуры хакеров источников на английском и русском языках. В этой работе впервые определено понятие «Интернет-преступность» и данный вид преступности выделен в отдельную предметную область исследования; описаны уголовно-правовая и криминологическая характеристики основных показателей преступности в Глобальной сети.

Новым подходом является и то, что в отличие от других научных работ, преступность в Интернет и компьютерная преступность, их механизмы возникновения, функционирования и развития объяснены в рамках теории субкультур. Определено понятие субкультуры Интернет-преступников, впервые системно проанализированы и описаны идеологическая база, обычаи, ритуалы, модели поведения, характерные для данной субкультуры, на основе не только научных трудов других авторов, но и работ самих хакеров как идеологического, художественного, публицистического, так и технического характера.

Впервые было проведено исследование общественного мнения об Интернет-преступности, анализ виктимологических аспектов, изучение и описание портрета личности современного Интернет-преступника; выделены особенности Интернет-преступности в России и выявлена система детерминирующих ее факторов; предложены методы борьбы с данным видом общественно опасных деяний. В монографии есть ряд научных выводов и предположений, которые могут представлять научную ценность и также определяют научную новизну исследования. Вкратце их можно резюмировать следующими положениями:

- С момента возникновения Интернет-преступности в ходе ее эволюции автор выделяеи 5 последовательных этапов развития. Эти этапы, представленные в монографии, проходит Интернет-преступность в любой стране мира, меняются лишь быстрота прохождения того или иного этапа, но порядок остается тем же. В настоящее время, несмотря на отставание рассматриваемой категории российской преступности в прошлом, национальная преступность в Глобальной сети успешно интегрирована в международную Интернет-преступность и находится на четвертом этапе развития. Этап быстрого количественного роста совершаемых Интернет-преступлений совпал с ростом популярности субкультуры хакеров.
- Интернет-преступность является частью компьютерной преступности и смежна с такими ее видами, как преступность в сфере компьютерной информации, киберпреступность и т.д. Интернет-преступность отличается от других видов особыми свойствами: глобальность, широкая распространенность, крайне высокая латентность и др., определяющими бурный рост и общественную опасность.
- Личность Интернет-преступника имеет свои специфические особенности, которые отличают ее от лиц, совершающих общеуголовные преступления традиционным путем. Интернет-преступники, по сравнению с исследованиями предыдущих лет, сильно «помолодели» и обладают большими профессиональными навыками.
- Для виктимологической профилактики исследуемого вида преступных деяний должны использоваться специфические компьютерные средства защиты, которые ранжируются в зависимости от ценности охраняемой компьютерной информации и навыков пользователя, а также средства защиты от «социальной инженерии». Автор приходит к выводу, что наиболее значимыми факторами виктимности исследуемых преступлений являются несоблюдение элементарных средств компьютерной безопасности и доверчивость пользователя, хотя причины меняются в зависимости от вида Интернет-преступления.
- Официальная статистика недостаточно точно отражает характеристику структуры, состояния и динамики современной российской Интернет-преступности. В связи с этим требуются дополнительные альтернативные источники информации, а также применение методик сбора и обработки данных для исследования преступности – как ее разновидностей, так и в целом. Из-за высокой латентности Интернет-преступности для

установления истинных масштабов ее распространения требуется использование новых методов и источников получения информации, таких как контент-анализ сайтов, содержащих преступные сведения; анализ структуры сайтов с помощью поисковых систем, анализ числа посещений тех или иных сайтов, лингвистический анализ псевдонимов хакеров и т. д.

- Выявлено, что некоторая часть населения склонна идеализировать образ Интернет-преступника, и часто воспринимает его как «борца за свободу». Преступная субкультура в Интернет определяется автором как совокупность идей, ценностей, обычаев, традиций, норм поведения, направленная на организацию образа жизни, целью которого является совершение Интернет-преступлений, их сокрытие и уклонение от правовой ответственности. Ценностный комплекс данной субкультуры служит также для легитимации и популяризации идеи хакерства в обществе.
- Сама природа сети Интернет является достаточно благоприятной для совершения преступлений. Такие свойства сети, как глобальность, трансграничность, анонимность пользователей, охват широкой аудитории, распределение основных узлов сети и их взаимозаменяемость создают преступникам, использующим Интернет, преимущества на всех этапах совершения преступления, а также позволяет эффективно скрываться от правоохранительных органов. Определяющими факторами, детерминирующими российскую Интернет-преступность, является специфическая криминальная субкультура, а также неразвитость экономического сектора компьютерных технологий, что не всегда дает возможности легального заработка.
- Меры борьбы с Интернет-преступностью, которые существуют в настоящее время, не отвечают современным реалиям. Связано это не только с неэффективностью отдельных мер, но и с отсутствием целостной их системы, направленной на противодействие Интернет-преступности. Наиболее эффективным в борьбе с Интернет-преступностью является комплекс криминологических мер профилактики, согласующихся с мерами социально-экономического, нравственно-идеологического, организационного, воспитательно-психологического и технического характера. Среди них выделяется одно из главных направлений – нейтрализация негативного влияния криминальной субкультуры компьютерных преступников.
- Действующий в настоящее время УК РФ не в полной мере соответствует современным требованиям борьбы с Интернет-преступностью и нуждается во внесении ряда изменений, отвечающих реалиям нашего времени, в общую и особенную части УК РФ. В монографии проведен анализ криминологических оснований изменения уголовного закона для совершенствования борьбы с компьютерной и Интернет-преступностью.

Значимость работы заключается в том, что данное монографическое исследование затрагивает уголовно-правовую и криминологическую проблемы, решение которых является необходимым условием для создания безопасного и прозрачного информационного пространства, а также напрямую связано с безопасностью многих сфер функционирования Российского государства. Именно от Интернет в современных реалиях зависит конкурентоспособность и безопасность большинства стран мира. Данная технология играет решающую роль в современной жизни, урегулирование вопросов правового контроля Интернет и установления надежного заслона для распространения Интернет-преступности является одной из основных проблем современного информационного общества.

Проведенное исследование восполняет недостаточную научную проработанность проблем, возникших в результате интенсивного роста количества и видоизменения качественных характеристик Интернет-преступлений, увеличения опасности деяний, с одной стороны, и отсутствия комплексных исследований в этой области – с другой.

Сформулированные теоретические выводы и положения могут быть полезны при разработке программ по борьбе с преступностью в Интернет в процессе осуществления системы мер государственной уголовной политики, совершенствования современного законодательства и правоприменения в области компьютерной и Интернет-преступности; а практические рекомендации могут быть использованы в области изучения Интернет-преступников и их группировок в оперативно-розыскной деятельности правоохранительных органов и во всесторонней профилактике данного вида преступлений. Кроме того, материалы исследования найдут применение при разработке и чтении лекции по курсам уголовного права, уголовно-исполнительного права, криминологии, криминалистики, юридической антропологии и психологии.

Компьютерная преступность

Заводсков А.Д.
соавторы: Малышев В.В., Осокин Д.В., Данилов В.О., Уртемеева М.А.

Ульяновский электромеханический колледж
г. Ульяновск, Россия
andzav@list.ru

Computer crime

Zavodskov A.D.
co-author: Malyshev V.V., Osokin D.V., Danilov V.O., Urtemeeva M.A.

Ulyanovsky electromechanical college
Ulyanovsk, Russia
andzav@list.ru

This work contains detailed information:

- about the types of computer crimes;
- about the ways of opposition to virus and hacker's attacks;
- statistical data on the crimes in the sphere of information technologies, in the Ulyanovsk region;
- opinions of independent experts and employees of the Department of Internal Affairs of the Ulyanovsk district, of the Department "K";
- problems of provision of safety of the network in FGOU SPO "Ulyanovsk Electromechanical College".

As of today, computer criminality is one of the most actual problems of mankind. One could not simply imagine the scales of damage that can be caused by crackers of systems (hackers). The only goal of our research is to show to everybody that at the present time it is necessary show extreme care as regards storage of information, and that as practice shows, crime detection in this sphere increases by several times every year …

In the given creative work the following items are considered:

1. Vulnerability of PC.

   A review of the basic problems of vulnerability of computers and computer networks is given.

2. Kinds of computer crimes.

   Full classification of the kinds of computer crimes, by various parameters, is presented.

3. Articles of the Criminal Code of the Russian Federation.

   A selection of articles of the CC of the Russian Federation is made, associated with computer criminality.

4. Struggle against computer criminality.

   The information on the most effective methods of struggle against computer crimes is systematized. Statistical data on crimes in the sphere of information technology in the Ulyanovsk region.

5. Anti-virus software.

Classification of viruses and anti-virus programmes.

6. "Virus" results for 2008.

   Results of virus attacks, for 2008, based on data available from IBM.

7. Construction of networks and anti-virus protection at FGOU SPO "Ulyanovsk Electromechanical College".

Hands-on experience of FGOU SPO "UEMC" in anti-virus and anti-hacker protection of networks.

Данная работа содержит подробную информацию:

- о видах компьютерных преступлений;
- о способах противостояния вирусным и хакерским атакам;
- статистические данные преступлений в сфере информационных технологий Ульяновской области;
- мнения независимых экспертов и сотрудников УВД Ульяновской области Отдела «К»;
- проблемы обеспечения безопасности сети в ФГОУ СПО «Ульяновский электромеханический колледж».

На сегодняшний день, компьютерная преступность является одной из самых актуальных проблем человечества. Масштабы ущерба, которые могут нанести взломщики систем (хакеры) просто не возможно вообразить. Цель нашего исследования одна – показать всем, что в настоящее время нужно очень бережно относиться к хранению информации и то, как показывает практика, раскрываемость в этой сфере с каждым годом увеличивается в разы…

В данной творческой работе рассмотрены следующие вопросы:

8. Уязвимость ПК.

   Дан обзор основных проблем уязвимости компьютеров и компьютерных сетей.

9. Виды компьютерных преступлений.

   Приведена полная классификация видов компьютерных преступлений, по различным параметрам.

10. Статьи УК РФ.

    Выполнена подборка статей УК РФ, связанных с компьютерной преступностью.

11. Борьба с компьютерной преступностью.

    Систематизирована информация о наиболее эффективных методах борьбы с компьютерными преступлениями. Статистические данные преступлений в сфере информационных технологий Ульяновской области

12. Антивирусное программное обеспечение

    Классификация вирусов и антивирусных программ.

13. «Вирусные» итоги за 2008 год

    Итоги вирусных атак, за 2008 год, по данным IBM.

14. Построение сетей и антивирусная защита в ФГОУ СПО «Ульяновский электромеханический колледж»

    Практический опыт ФГОУ СПО «УЭМК» по антивирусной и антихакерской защите сетей.

Восприятие национального кибер закона: Распознавание образов в группах пользователей

Имран Аскрения, Гамид Якаххани, Кристина Драгонова
Университет Восточного Лондона(UEL)
Лондон, Великобритания
catastrofka@yahoo.co.uk

Perceptions of national Cyber law: Pattern recognition in Human groupings

Imran Askerniya, Hamid Jahankhani, Chrisina Draganova
University of East London
School of Computing, Information Technology and Engineering
London, UK
catastrofka@yahoo.co.uk

Abstract:

The research in progress will examine the potential impacts of cyber attacks on Russian society and will determine a framework for pattern recognition from Russian cyber space to identify the major clusters of people's knowledge and skills in protecting themselves against cyber crime. This system will be used to build culturally-sensitive response model/mechanism for fighting cyber-crime.

Introduction:

The revaluation of ICT since the 1980s has provided the criminals with great opportunities to transform what was known as traditional "old-fashioned" crimes such ID theft, fraud, and many other types of crimes to new mischief's, unwanted and damaging behavior such as what have come to be known as hacking, spoofing, credit card fraud and spamming.

According to the general-colonel Boris Miroshnikov, chief of bureau for special technical undertakings at the RF Ministry of the Interior, only in 2007 about 12 thousand computer crimes were recorded, and more than 600 resources containing 'undesirable content' were closed. More than half are sites with child pornography and that is only the top of the iceberg.(Myakisheva, 2008).

The anonymous nature of the internet makes it possible for many individuals to engage into a variety of criminal activities in cyberspace. Hollinger (1988) conclude that individuals were more likely to be involved in illegal computer activity if they had friends who also were engaged in the activity.

These trends of crime could:

- Have grave social consequences for the society.
- Be of immediate concern to national government.
- Have a serious impact on the national economy.

In the face of these challenges, the criminal code of Russian Federation have produced the first piece of law, which includes the articles against cyber crime (The Criminal Code of the Russian Federation, Chapter 28, Federal Law No. 64-FZ of June 13, 1996 on the Enforcement of the Criminal Code of the Russian Federation)

Chapter 28. Crimes in sphere of the computer information

- Article 272. Illegal Accessing of Computer Information
- Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses
- Article 274. Violation of Rules for the Operation of Computers,

Computer Systems, or Their Networks

However despite the numerous attempts, there is a lack of an agreement in frame works for either understanding or responding to these issues, their impacts and their interrelationships in Russia.

“It is clear that organized cyber crime has taken root in countries that don’t have response mechanisms, laws, infrastructure and investigative support set up to respond to the threat quickly,” said Ronald K. Noble, secretary general of Interpol, an organization that facilitates transnational law enforcement cooperation. He declined to discuss the Russian Business Network specifically”, (Richard Koman, 2007).

The research will examine the potential impacts of cyber attacks on Russian society and will determine a framework for pattern recognition from Russian cyber space to identify the major clusters of people’s knowledge and skills in protecting themselves against cyber crime.

The main aim of this research is to create the map of Russian society showing the more and less educated districts of the country. The researcher will identify what initiative is being employed to secure user-individuals.

The objectives of the research are therefore:

- To determine how best to protect the user-individuals from cyber crime attacks.
- To determine more specifically how such incidents are perceived and the possible effects this may have.
- To identify the clusters of people and explaining the similarities, differences and how the different clusters of people can be connected.

Cyber crime in Russia

Cyber crime is the modern and one of the most serious problems in the world and affecting to the almost every people’s life stages. In 21 century cyber world and real world are very close. As Jahankhani (2008) said: “Identify theft is a growing criminal phenomenon which presents a major threat to individuals, businesses, governments and society in general”. (Jahankhani and George. 2008). The cyber crime can be identify in different ways, one of them is: “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime”.(Pawan, 2003). Stephenson (2000), defines the cyber crime as all criminal activities where committed using the computer or against the computer or network also using any tool to do so.

(Stephenson, 2000)

The current situation of cyber crime in Russia is one of the most complicated. According to Washington post article: finds that of all the cyber crime coming out of Russia, it is actually Russian victims that top the list for hackers (this apparently contradicts the widespread myth that hackers based in Eastern Europe and Russia focus all their energy on attacking Western sites). (Brian Krebs, 2009). In the report IBM Internet Security Systems confirmed that Russia remains the world centre for spamming. In 2008 Russia took the 1 place in world spam, which make around 11.6 percent of world spam senders. (IBM, 2008).

According to Mr. Miroshnikov: “at present the penalty is too tolerant, i.e. 2-3 years of imprisonment, while in other countries people are sentenced to 10-15 years of imprisonment with property confiscation, such an inadequately tolerant penalty encourages criminals to continue committing more sophisticated crimes.”(Myakisheva, 2008)

All these facts, explores that Russian internet community ((around 38,000,000 Internet users as of Dec/08) according to The Internet world statistics, usage and population, Russian Federation) is vulnerable to cyber crime. To minimize the harm and impact on the community, the awareness level of cyber crime risks will be examined and analyzed in this research project.

Clustering and mapping.

In the propose research project, the main part of the research will be heavily rely on grouping (clustering and mapping) the Russian cyber society. According to Hichem Frigui et al, 1997.: “Clustering, also known as unsupervised classification, is a process by which a data set is divided into different clusters such that elements of the same cluster are as similar as possible and elements of different clusters are as dissimilar as possible”.(Hichem Frigui et al.1997). In the article of Jan Puzicha 1999 et al.: “clustering or grouping problem, i.e., the general goal is to identify groups of similar image primitives. Depending on the specific problem these primitives can be entities like pixels, line elements, image patches and regions, real-world objects, or even complete images being part of an image sequence or an image database.” (Jan Puzicha et al, 1999)

In the scientific research there are many different types and methods of clustering. The choice of the method depends of the data and context of examined data. Generally, there are two main different methods of clustering;

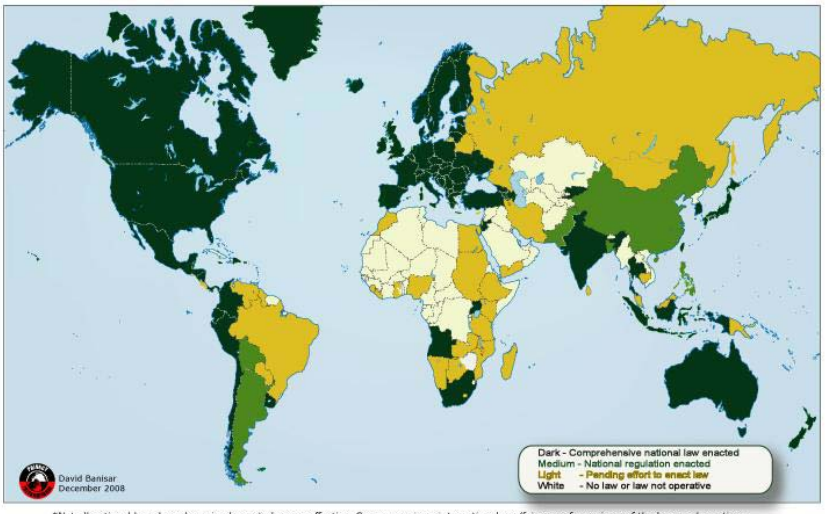
- Hierarchical clustering
- Partitional clustering (Raza Ali et al, 1998)

Also clustering is a method for statistical analysis, which can be applied in machine learning, data mining, pattern recognition, image analysis and bioinformatics.

Previous researchers have relied on mapping as a part of their research process because it is

"a well- established practice in action research approaches to international development. Any kind of available local materials are used to create the maps which usually record geographical dispersement, resource allocation, services, physical barriers and social networks and relations".(Stratton, 2008). The research map below shown the different peoples cluster, which was created by David Bonisar. The aim of this map is to show the National Freedom of the Information Laws, Regulation and Bills for the Privacy international group in 2008.

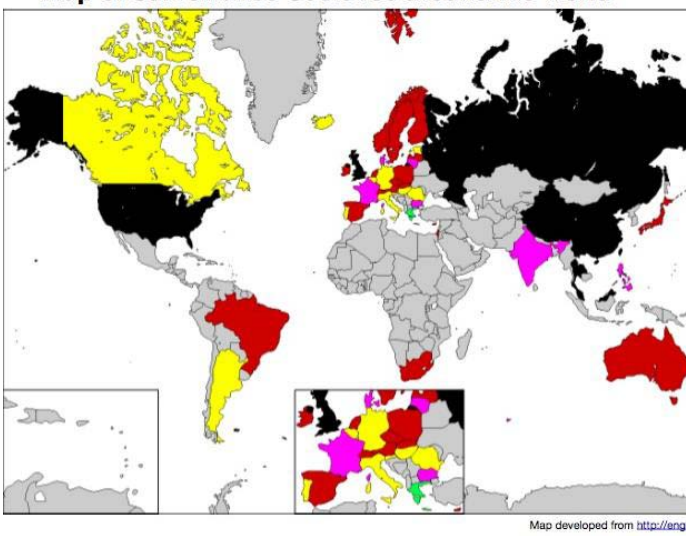
National Freedom of Information Laws, Regulations and Bills 2008



*Not all national laws have been implemented or are effective. See www.privacyinternational.org/foisurvey for reviews of the laws and practices

In addition, The Privacy International group has produced a Map of surveillance Societies around the world in 2007. This map shows different levels of the societies all over the world.

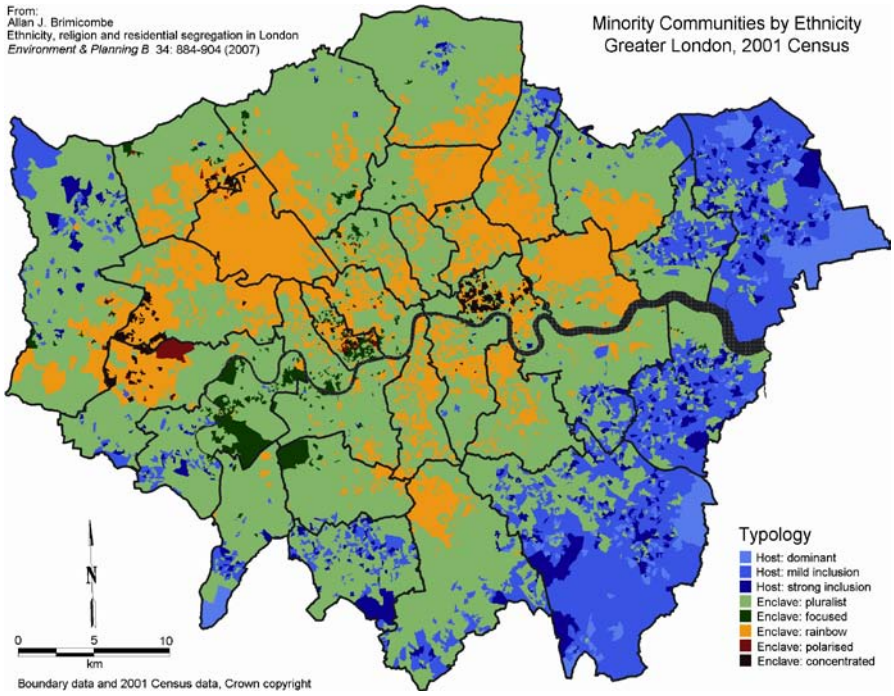
Map of Surveillance Societies around the world



Map developed from http://eng



Allan Brimicombe in his research has used clustering technique to show how London society is divided into communities by ethnic indications and different religions.



The research will contribute to Russian literature of cyber crime, there is no previous studies identified the cyber skills of Russian society before-to the researcher best of knowledge- and that why this research will be interesting for the cyber crime expert and will have the additional effect as information about Russian Federation and its cyber society.

Methodology

To achieve the aim of the proposed research, which is measuring cyber skills in Russia web society and trying to cluster individuals into groups according to their awareness of cyber security skills, the researcher believes on using Artificial Intelligent (AI) tools for pattern recognition, which will help to analyse data from the designed questionnaire. The questionnaire will be scenario-style questions which will be analyse using the pattern recognition AI software tools. The researcher will rely in a five scenario questions of different categories of individuals such:

Russian Federation.	
MEN	**WOMEN**
new users (young; medium age; old)	new users (young; medium age; old)
experienced users (young; medium age; old)	experienced users (young; medium age; old)
internet workers	internet workers
Social users	social users

Conclusions

This investigation is quite new and progressive, because nowadays the internet is wildly used for work, shopping and entertainment. Also, every day the enormous amount of data transmitting all over the world. In this case even the single user has had some skills about the cyber crime and cyber legislation. This research project allows finding out the different clusters of people and analyzing their knowledge in cyber crime and legislation system.

References

1. Antti Aarnio , Aki Enkenberg , Jukka Heikkilä and Sanna Hirvo., 2002. Adoption and Use of Mobile Services, Empirical Evidence from a Finnish Survey, University of Jyväskylä, Finland , Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 3 - Volume 3, [online]. Available online: The guide to computing literature UEL Available online: http://portal.acm.org/citation.cfm?id=820978 [Accessed 24 March 2009].
2. Barham, J., 2008, Russia's Cyber crime Haven. Available online: http://www.securitymanagement.com/article/russias-cybercrime-haven-004818 [Accessed 25 March 2009].
3. Bonisar, D., 2008, National freedom of Information laws, regulations and bills 2008. Available online: http://www.privacyinternational.org/foi/foi-laws.jpg [Accessed 28 March 2009].
4. Brimicombe, A., 2007, Ethnicity, religion, and residential segregation in London: evidence from a computational typology of minority communities. Available online: http://www.swetswise.com/FullTextProxy/swproxy?url=http%3A%2F%2Fwww.envplan.com%2Fepb%2Ffulltext%2Fb34%2Fb3309.pdf&ts=1238172776384&cs=2780043169&userName=0016063.ipdirect&emCondId=16063&articleID=38369249&yevoID=2346075&titleID=520062&referer=0&remoteAddr=161.76.196.146&hostType=PRO [Accessed 29 March 2009].
5. Jahankhani, H. George, C., 2008, Challenges of Identity theft in the information society. Given by author.
6. Hichem, F. & Raghu K., 1997: Clustering by competitive agglomeration. Pattern Recognition, Volume 30, Issue 7, July 1997, Pages 1109-1119. Available online: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V14-3SNVHWM-M-1&_cdi=5664&_user=132444&_orig=search&_coverDate=07%2F31%2F1997&_sk=999699992&view=c&wchp=dGLzVlz-zSkzS&md5=11c6b36550a81c892d9629885a43af6e&ie=/sdarticle.pdf [Accessed 28 March 2009].
7. Hierarchical clustering diagram. Available online: http://en.wikipedia.org/wiki/File:Hierarchical_clustering_diagram.png
8. IBM Internet Security Systems X-Force® 2008 Mid-Year Trend Statistics, July 2008. Available online: http://www-935.ibm.com/services/us/iss/xforce/midyearreport/xforce-midyear-report-2008.pdf [Accessed 28 March 2009].
9. International Privacy group, Anon., 2007, Leading surveillance societies in the EU and the World 2007. The 2007 International Privacy Ranking, 2007. Available online: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 [Accessed 28 March 2009].
10. Internet world statistics, usage and population, Russian Federation. Available online: http://www.internetworldstats.com/europa2.htm [Accessed 25 March 2009].
11. Koman. R., 2007. Russian company is hub for all manner of cybercrime, ZDNet Government. Available online: http://government.zdnet.com/index.php?p=3443 [Accessed 21 March 2009].
12. Krebs, B., 2009, From (& To) Russia, With Love. Available online: http://voices.washingtonpost.com/securityfix/2009/03/from_to_russia_with_love.html?hpid=sec-tech [Accessed 28 March 2009].
13. Myakisheva, M., 21. 03. 2008, What is Russia's answer to cyber threats?, National Software Development Alliance. Available online: http://www.silicontaiga.org/home.asp?artId=8175 [Accessed 27 March 2009].
14. Pawan, D., 2003. The Internet: Legal Dimensions. Availiable online: http://lawspace.law.uct.ac.za:8080/dspace/bitstream/2165/239/1/Pawan_2003.pdf [Accessed 23 March 2009].
15. Puzichaa, J, Hofmannb, T. & Joachim M. Buhmann,. 1999, Histogram clustering for unsupervised segmentation and image retrieval star.
16. Raza, A, Usman. & G, Aasim. S., 1998, Data Clustering and Its Applications. Available online: http://members.tripod.com/asim_saeed/paper.htm [Accessed 29 March 2009].
17. Rogers. K. M., 2001. A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Available online: http://www.dvara.net/HK/cybercrime-thesis.pdf [Accessed 29 March 2009].
18. Stratton, M., 2008. Community-Based Mapping: A Research Tool for Justice System Research. Available online: http://www.cleonet.ca/conference/content/docs/stratton-mapping-en.pdf. [Accessed 26 March 2009].
19. Stephenson, P., 2000, Investigating Computer- Related Crime. CRC Press LLC, USA.
20. The Convention on Cyber crime, 2004, ETS No 185 Explanatory Note
21. Thompson, H., 2006. What do we really understand when we talk about computer crime. Trusted-Management Ltd. Available online: http://www.trusted-management.com/whitep/White-Paper-Crime.pdf [Accessed 26 March 2009].

Краткий обзор:

Данный проект предполагает глубокое исследование потенциального влияния кибер атак на российское общество и систематизацию распознавания образов внутри российского кибер пространства для идентифицирования знаний в основных кластерах пользователей для защиты их от кибернетических угроз. Главной целью исследования является создание карты российского общества, демонстрирующая более или менее образованные слои населения.

Краткий обзор:

Данный проект предполагает глубокое исследование потенциального влияния кибер атак на российское общество и систематизацию распознавания образов внутри российского кибер пространства для идентифицирования знаний в основных кластерах пользователей для защиты их от кибернетических угроз. Главной целью исследования является создание карты российского общества, демонстрирующей уровень образования различных слоев населения.

Введение:

По данным проверки, проведенный ИКТ(информационно-коммуникационные технологии) с 1980-х годов, было установлено, что криминал, занимающийся традиционными преступлениями-известными, как «старомодные», воровство, мошенничество, подделка документов и др., получили возможность для создания новых форм кибер криминала, наиболее нежелательных и опасных, таких как хакерство, спуфинг, мошенничество с кредитными картами и спамминг.

По заявлению начальника бюро, по техническим соглашениям при МВД РФ, генерал-полковника Бориса Мирошникова, только в 2007 году, зарегистрировано около 12 000 компьютерных преступлений и более 600 ресурсов, имеющих «нежелательное содержание» было закрыто. Более половины- сайты с детской порнографией и это лишь вершина айсберга (Мякишева 2008).

Анонимность интернета делает возможной для многих пользователей присоединятся к различным видам криминальной активности в кибер пространстве. Холлигер(1988), пришел к заключению, что пользователи наиболее активно включаются в нелегальную компьютерную деятельность, если они имеют друзей, вовлеченных в эту деятельность ранее. Эти негативные тенденции создают:

- Угрозу национальной безопасности;
- Опасность для нац. экономики;
- Социальную угрозу для общества в целом и влекут за собой тяжелые последствия.

Перед лицом, вышеперечисленных опасностей в УК РФ был введен ряд новых законов содержащих статьи, направленные против кибер преступлений. (УК РФ гл.28 федеральный закон №64 ФЗ от 13 июня 1996, направленные на усиление РФ).

Глава 28. Преступления в сфере компьютерной информации.

- *Статья 272. Нелегальный доступ к компьютерной информации*
- *Статья 273. Создание, использование и распространение вредоносных компьютерных вирусов.*
- *Статья 274. Нарушение правил использования компьютеров, компьютерных систем и их сетей.*

Но, невзирая на многочисленные попытки улучшения существующего положения, наблюдается ряд системных недостатков из- за внутренних отношений в российском обществе и несоблюдении или игнорировании существующих законов.

Как заявил Рональд К Нобель, генеральный секретарь Интерпола, организации, чьи возможности позволяют достичь межконтинентального взаимного сотрудничества. «Становится ясным, что организованная кибер преступность берет свое начало в тех странах, которые не имеют строгой законодательной базы, инфраструктуры и правового регулирования, способного быстро реагировать на угрозу» Он подчеркнуто уклонился от обсуждения ситуации в РБК. (Ричард Коман, 2007).

Целью исследования является:

- Наилучшие способы защиты пользователей от кибр атак;
- Разработка наиболее эффективных способов выявления инцидентов и их последствий.

- Идентификация кластеров людей и выявление сходства, различий и связей между ними.

Кибер криминал в Российской Федерации.

Кибер преступность является очень острой проблемой современности, так как затрагивает интересы практически всех людей современного общества на различных этапах их жизни. В XXI веке кибер и реальный миры тесно взаимосвязаны. Как сказал доктор Якаханни(2008): «Идентификация нарушителя- это необходимость, так как растущая кибер преступность, представляет собой угрозу личности, бизнесу, правительственным структурам, всему обществу в целом.»

Кибер криминал, может определяться по- разному, Паван 2003 «Любая деятельность использующая компьютер, как инструмент, мишень или средство для совершения преступления, является криминальной». Стивенсон 2000, определил кибер преступления, как любую криминальную деятельность, где преступления совершаются с использованием компьютера или против компьютера или сети, используя при этом различные инструменты. (Стивенсон, 2000)

Существующая ситуация в кибер преступности, одна из наиболее острых и сложнейших проблем современной России. Согласно статье Вашингтон пост, кибер преступления, происходящие на территории России в первую очередь затрагивают самих россиян, которые являются основными жертвами российских хакеров (это противоречит широко распространенному мифу о том, что хакеры, находящиеся в Восточной Европе и России сосредотачивают все свое внимание на западных сайтах) (Брайн Кребс, 2009). В отчете IBM утверждается, что Россия остается мировым центром по распространению спама, 11.6% распространения спама в мире. (IBM, 2008).

Согласно заявлению генерал- полковника Мирошникова «в настоящее время наказание за кибер преступления весьма незначительно, всего 2-3 года заключения, в то время, как в других странах подобные преступления карается 10- 15 годами заключения с конфискацией имущества, что является адекватным ответом преступникам и удерживает их от совершения подобных преступлений в дальнейшем» (Мякишева, 2008).

Все вышеперечисленные факты указывают на то, что российское интернет сообщество ((около 38 000 000 пользователей на дек. 2008) согласно данным мировой интернет статистике пользователей и населения РФ) является уязвимыми для кибер преступности. Чтобы минимизировать ущерб и негативное влияние на общество, в настоящей работе будет исследован и проанализирован уровень осведомленности пользователя об опасности кибер преступлений.

Кластеринг и создание карт.

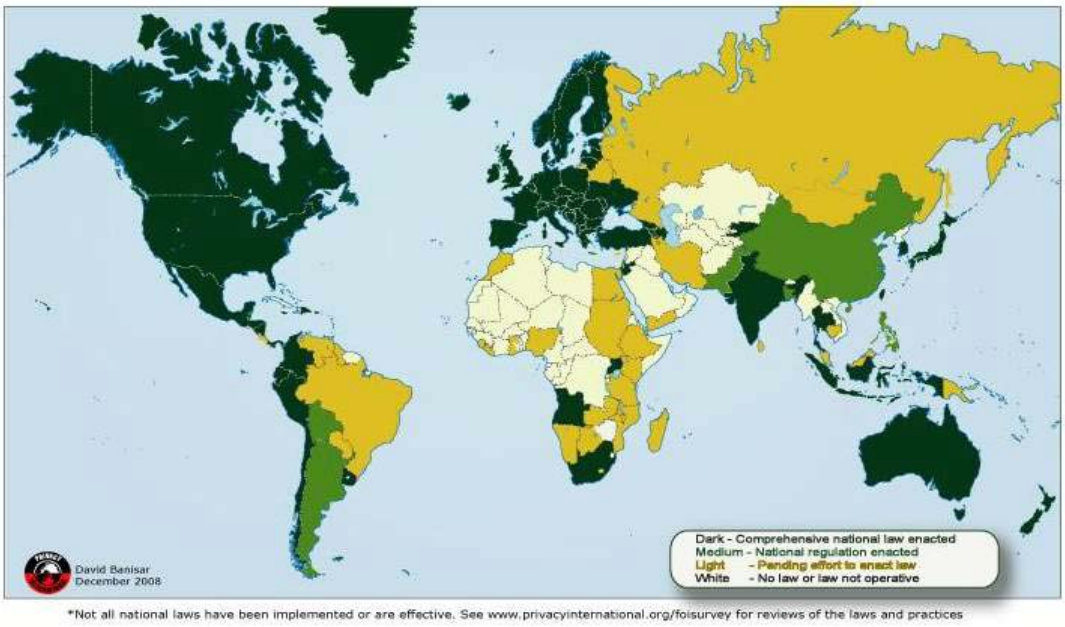
Основная часть предполагаемой работы будет направлена на создание кластеров и карт российского кибер сообщества. Согласно Хичем Фрикьи(Hichem Frigui) 1997 «Кластеринг известен как не контролируемая классификация, являющаяся процессом, с помощью которого наблюдаемые группы подразделяются на различные кластеры, элементы которых похожи друг на друга и кластеры элементы которых абсолютно различны» (Фрикью, 1997). В статье Жана Пузича «Кластеринг или группирование проблем, например общей цели, позволяет определять группы похожих образов. В зависимости от специфики проблемы эти образы могут быть представлены как пиксели, линейные элементы, образные элементы и районы, реальные существующие объекты и даже части образа, согласующего с БД» (Jan Puzicha, 1999)

В научных исследованиях существуют различные типы и методы кластеринга. Выбор метода зависит от существующих фактов, контекста и исследуемых данных. В общем различают 2 основных метода кластеринга.

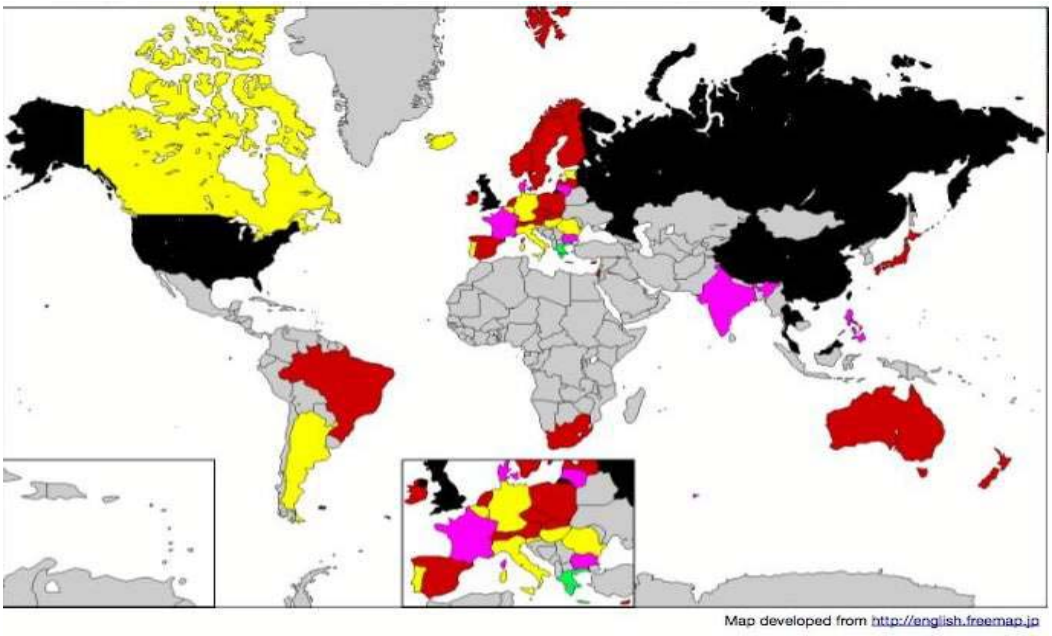
- Иерархический кластеринг;
- Частичный кластеринг (Раза Али, 1998)

Кластеринг, также является методом статистического анализа, извлечения информации, распознавания образов, анализирования образов и био- информатики. Любые имеющиеся данные, используются для создания карт, которые обычно отражают действительное географическое распространение, расположение ресурсов, физические препятствия, социальные сети и отношения». (Старттон, 2008)

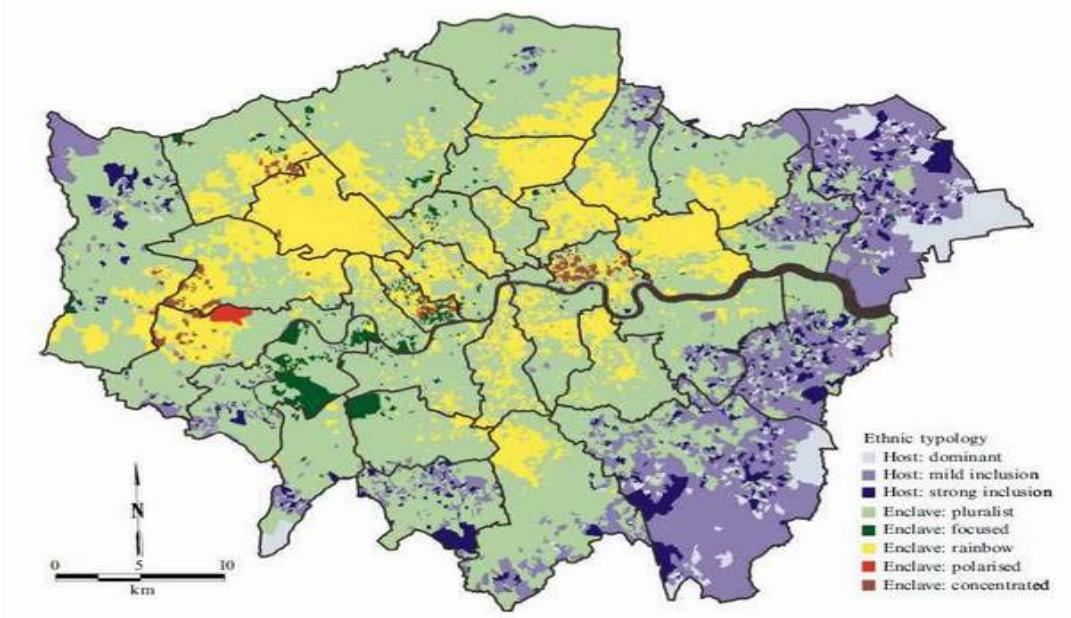
Карта исследования, созданная Дэвидом Бонисаром и представленная ниже, демонстрирует различные кластеры людей. Цель этой карты, показать национальные свободы и регулирование информационных законов и билли для PIG(Privacy International Group) 2008.



В дополнение к этому PIG выпустила карту контролируемых сообществ за период 2007 года обществ по всему миру. (PIG 2007)



Алан Бримиком, в своем исследовании использовал технику кластеринга, чтобы показать, как лондонское общество разделяется на группы по этнической и религиозной принадлежности. (Allan Brimicombe 2007)



Предполагаемое исследование будет являться дополнительной информацией по РФ, ее кибернетическому обществу, должно стать вкладом в российскую науку о кибер преступности и заинтересовать экспертов, так как до настоящего времени работ на подобную тему в РФ не выполнялось.

Методология.

Для достижения целей данного исследования, которые должны определить кибер навыки в интернет сообществе и попытаться создать кластеры в зависимости от их уровня осведомленности о мерах безопасности, исследователь считает необходимым использование программы искусственного интеллекта для распознавания образов, которые помогут анализировать информацию полученную путем анкетирования. Анкетирование предполагает создание ситуативности, которая будет анализирована путем распознавания образов с использованием системы искусственного интеллекта. Исследователь предполагает использовать 5 ситуативных вопросов среди различных категорий пользователей, представленных в таблице.

Российская Федерация	
Мужчины	**Женщины**
Новые пользователи (молодые; среднего возраста; пожилые)	Новые пользователи (молодые; среднего возраста; пожилые)
Опытные пользователи (молодые; среднего возраста; пожилые)	Опытные пользователи (молодые; среднего возраста; пожилые)
Работники компьютерной сферы	Работники компьютерной сферы
Работники сферы управления	Работники сферы управления

Заключение

Это исследование является абсолютно новым и прогрессивным, так как в настоящее время интернет широко используется во всех сферах деятельности человека: науке, бизнесе и развлечениях. Ежедневно большое количество информации распространяется по всему миру через интернет. В этой ситуации любой пользователь должен обладать необходимыми навыками в области интернет преступлений и кибер. законодательства. Данный проект предполагает выявление различных кластеров людей и анализ их знаний в области кибер преступности и законодательной системы.

Транснациональные Интернет-преступления : проблемы юрисдикции и особенности решений по законодательству России и Германии

Парамонова С.Л., LL.M.

Макс-Планк-Институт по иностранному и международному уголовному праву, г. Фрайбург;

аспирант Университета Пассау, Германия

s.paramonova@mpicc.de; sunshinesvet2@yandex.ru

Transnational Cybercrimes: Problems of Jurisdiction and Peculiarities of Solutions According to the Legislation of Russia and Germany

Paramonova S.L., LL,M.

Max Planck Institute for Foreign and International Criminal Law, Freiburg

PhD-Student at the University of Passau, Germany

s.paramonova@mpicc.de; sunshinesvet2@yandex.ru

Cybercrime is a primary example of cross-border crime, and so, it raises the issue of jurisdiction. It turns out that countries think quite differently on this issue. The cybercrime statutes of numerous countries show varying and diverging jurisdiction clauses. In this article, these approaches are outlined regarding Russia and Germany, by indicating when states claim jurisdiction and under which jurisdictional principles, legislative provisions of Russia and Germany allow that claim and how jurisdiction conflicts should be solved.

The purpose of the work is to show, during research of the legislation of Russia and Germany concerning the issues of jurisdiction as regards the Internet crimes, by the example of real and invented legal cases, the necessity of reform of the Russian legislation in the field of jurisdiction, to give particular recommendations.

Tasks:

1. Examination of criminal legislation of Russia and Germany, applicable to the solution of issues of legal foundation for the propagation of own jurisdiction in the Internet space.

2. The analysis of jurisdictional conflicts arising in the absence of country for solution of legal situation (negative jurisdictional conflict) or in case of collision of interests of the states in application of the own criminal law (positive jurisdictional conflict).

3. Detailed analysis of principles on the basis of which, the application is implemented, of the national law concerning the Internet crimes.

4. Conclusions and particular recommendations, proved practically and theoretically, for perfection of the Russian legislation, based on practical and theoretical substantiations.

Urgency

Trans-national crimes is not a new phenomenon, they always existed. In the modern world various kinds of Internet crimes represent vivid example of trans-boundary offences. The Internet getting increasing significance in the modern life is accompanied by new virtual capabilities which entail growing legal uncertainty and instability.

When solving any legal situation with a foreign element, in particular, concerning the trans-boundary crimes, the first arising question is a question of jurisdiction: which state is authorized to apply the own national law with respect to the criminal case. The solutions have their features within the framework of Internet space. In the cyberspace, when committing crimes, it is possible to quickly and frequently cross, if not territorial, then jurisdictional borders of states. At that, the victims can potentially be all the users of the Internet. There is a

correct question regarding the law that should be applied with respect to Internet crimes. Whether criminal law and order of multitude of states shall be declared to be applicable, whereas huge amount of information, including illegal information available in the Internet, is accessible from practically any country of the world. Within the frameworks of the given research, the analysis of criminal jurisdiction is carried out, mainly by the example of the Russian and German legislation as regards the Internet crimes.

The main results of the research:

Particular proposals on changing the clauses 11 and 12 of chapter 2 (action of the criminal law in time and space) of the Criminal Code of the Russian Federation, with the consideration of the specificities of the Internet space.

Practical application in the sphere of information safety

Practical application of the given research consists in that the inserted changes in the Russian legislation on the part of jurisdictional problems of Internet crimes would allow to protect in a greater degree, the rights of citizens of the Russian Federation outside the territory of the Russian Federation. On the other hand, they would allow the Russian Federation to extend the own jurisdiction to those cases where the state interests are directly affected by the crimes committed in the Internet space. It is first of all concerned with the alteration of territorial (item 1 of clause 11 of the CC of the Russian Federation) and actual (item 3 of clause 12 of the CC of the Russian Federation) jurisdictional principle.

Целью работы является в ходе исследования законодательства России и Германии в отношении вопросов юрисдикции, касающихся Интернет-преступлений, на примере реальных и вымышленных правовых случаев, показать необходимость реформы Российского законодательства в области юрисдикции, дать конкретные рекомендации.

Задачи:

1. Исследование уголовного законодательства России и Германии, применимого к разрешению вопросов законного основания для распространения собственной юрисдикции в Интернет-пространстве.

2. Анализ юрисдикционных конфликтов, возникающих при отсутствии страны для разрешения правовой ситуации (негативный юрисдикционный конфликт) или при столкновении интересов государств в применении собственного уголовного права (позитивный юрисдикционный конфликт).

3. Подробный анализ принципов, на основе которых решается применение национального права в отношении Интернет-преступлений.

4. Выводы и конкретные рекомендации, обоснованные практически и теоретически, для совершенствования российского законодательства, основанные на практических и теоретических обоснованиях.

Актуальность

Транснациональные преступления - не новое явление, они всегда существовали. В современном мире различные виды Интернет-преступлений представляют собой самый яркий пример трансграничных правонарушений. Интернет, приобретающий все большее значение в современной жизни, сопровождается новыми виртуальными возможностями, которые влекут за собой возрастающую правовую неопределенность и нестабильность.

При решении любой правовой ситуации с иностранным элементом, в особенности в отношении трансграничных преступлений, первый возникающий вопрос - это вопрос юрисдикции: какое государство уполномочено применять в отношении уголовного дела собственное национальное право. Свои особенности имеют решения в рамках Интернет-пространства. В кибер-пространстве, при совершении преступлений можно быстро и часто пересекать, если не территориальные, то юрисдикционные границы государств. При этом жертвами могут становиться потенциально все пользователи интернета. Возникает справедливый вопрос о праве, которое должно применяться в отношении Интернет-преступлений. Должны ли объявляться применимыми уголовные правопорядки множества государств, при том, что огромное количество информации, в том числе незаконной, имеющейся в Интернете, доступно из практически любой страны мира. В рамках данного исследования проводится анализ уголовной юрисдикции главным образом на примере российского и немецкого законодательства в отношении Интернет-преступлений.

Основные результаты исследования:

Конкретные предложения по изменению статей 11 и 12 главы 2 (действие уголовного закона во времени и пространстве) УК РФ, с учетом специфики Интернет-пространства.

Практическое применение в сфере информационной безопасности

Практическое применение данного исследования состоит в том, что внесенные изменения в российское законодательство в отношении юрисдикционных проблем Интернет-преступлений, позволят в большей степени защищать права граждан РФ за пределами территории РФ. С другой стороны позволят Российской Федерации распространять собственную юрисдикцию на те случаи, когда непосредственно задеты государственные интересы преступлениями совершенными в Интернет-пространстве. Это прежде всего касается изменения территориального (п. 1 ст. 11 УК РФ) и реального (п. 3 ст. 12 УК РФ) юрисдикционного принципа.

Проблема правового регулирования

Печкуров А.В.

Кубанский Государственный Технологический Университет
г. Краснодар, Россия

pechkyrov@mail.ru

Problem of legal regulation

Pechkurov A.V.

Kuban State Technology University
Krasnodar, Russia

pechkyrov@mail.ru

The work's goal is next development laws in protect of information sphere in Russia. Author considers that it is important to work out and pass the bill "About struggle with computer's crime". Author formulates fundamental articles of this bill and reasons of passing this bill.

Реалии современной жизни таковы, что часть информации необходимо оградить, сделав её достоянием только необходимому вам кругу лиц. Но существуют лица (компьютерные преступники, хакеры), способные взломать барьеры защиты конфиденциальных сведений.

Современное законодательство в области защиты информации и информационной безопасности разработано тщательно.

Однако отсутствует проработка вопроса о правовом статусе нарушителя ИС. В целях лучшего понимания ИБ, понятия «компьютерный преступник», его средства, следует приложить усилия для разработки и принятия законопроекта «О борьбе с компьютерными преступлениями», который послужит основой для разработки новых средств ИБ не только в правовой сфере.

В данной работе автор попытался сформулировать основные пункты этого законопроекта. Были рассмотрены основные причины необходимости принятия такого законопроекта и его актуальность.

Методика обнаружения и классификации криптографически преобразованных файлов

Речицкий А.С.

Ставропольский Государственный Университет
г. Ставрополь, Россия
art1st-tm@ya.ru

Technique for detecting and classifying cryptographically transformed files

Rechitskiy A. S.

Stavropol State University, chair of Organization and technology of data protection
Stavropol, Russia
art1st-tm@ya.ru

The methodology of proving base collection during court computer-technical examination performance in case of using on studied object cryptographic facilities and devices of processing and storing the information is worked out. It is stressed the necessity to work out detailed manuals concerning expert research of computer technologies and soft programs which should be used in such circumstances.

Разработана методология сбора доказательной базы в ходе проведения судебной компьютерно-технической экспертизы в случае применения на исследуемом объекте криптографических средств и устройств обработки и хранения информации. Подчеркивается необходимость в разработке детальных руководств по экспертному исследованию средств компьютерных технологий и программных продуктов для действий в подобных обстоятельствах.

В настоящей работе разрабатывается методология сбора доказательной базы в ходе проведения судебной компьютерно-технической экспертизы, в том случае, если имеются основания предполагать применение на исследуемом объекте криптографических средств и устройств обработки и хранения информации, которые в настоящее время стали широко доступны. Большинство руководств по экспертному исследованию средств компьютерных технологий и программных продуктов не содержат исчерпывающих рекомендаций для действий в подобных обстоятельствах. Восстановление структуры данных – только половина пути, гораздо более сложное препятствие представляет задача идентификации криптографических контейнеров, а также их классификация для последующих попыток дешифрования.

Актуальность работы заключается в удовлетворении потребности компьютерно-технической экспертизы в эффективных инструментах обнаружения и классификации криптографически преобразованных файлов.

Целью работы является разработка комплекса методик для обнаружения криптографически преобразованных файлов и их классификации.

Для достижения поставленной цели автором сформулированы и решены следующие частные **задачи**:

- проанализированы особенности следообразования конкретных образцов средство криптографической защиты информации (СКЗИ);
- проанализированы возможности идентификации СКЗИ, использовавшегося совместно с исследуемым носителем информации, по его «следам»;
- разработан метод отбора «подозрительных» файлов, которые возможно были подвергнуты криптографическим преобразованиям, из общей массы информационных объектов на исследуемом носителе информации;

- разработан метод экспресс-анализа отобранных «подозрительных» файлов на предмет идентификации использованного СКЗИ.

Применительно к особенностям следообразования рассмотрены типичные ситуации использования СКЗИ и распространенные приемы, к которым прибегают для усложнения задачи поиска и идентификации криптографических контейнеров, а так же вызываемые этим возможные осложнения проведения экспертизы. Для сокращения времени поиска и классификации информации, находящейся на исследуемом объекте, предложено использовать процедуру, включающую в себя два метода: экспресс-оценки аутентичности и интегральной оценки подозрительности.

Предложенный метод экспресс-оценки аутентичности, основан на проверке логических ассоциаций между приложениями, расширениями типов файлов, и типами данных. Для его реализации необходимо произвести сбор информации для анализа по указанным критериям. После чего все собранные данные на данном этапе подвергаются перекрестной проверке, а так же сравниваются с эталонной "базой" соответствий. На основании результатов проверки принять решение о необходимости детального исследования определенных объектов (файлов, записей в реестре, установленных приложений). Произведен выбор доступного инструментария для реализации предложенного метода.

Метод интегральной оценки подозрительности объектов, заключающийся в последовательном «опросе» всех обнаруженных объектов, основанном на заранее определенном ограниченном множестве простых критериев. Результатом проверки по каждому критериев является увеличение (или не увеличение) интегрально рейтинга подозрительности объекта на заданную величину. Целесообразна совместная реализация данного метода со средствами индексирования объектов на носителе информации, а так же его расширение применением весовых коэффициентов. Собран возможный вариант опроса. Итогом работы метода является база данных файлов с индексом подозрительности.

Таким образом, в ходе выполнения работы выявлены особенности следообразования конкретных образцов средств криптографической защиты информации ряда отечественных и зарубежных производителей; выявлены пути идентификации СКЗИ, использовавшегося совместно с исследуемым носителем информации, разработан вероятностный метод сортировки, позволяющий выявить файлы, подвергавшиеся криптографическим преобразованиям, а также метод экспресс-анализа файлов на предмет идентификации использованного при их создании СКЗИ.

Возможности кибернетического нарушителя по сохранению конфиденциальности своей информации и собственной анонимности перед лицом Государственных служб глобального электронного надзора

Шабанов А.В.

Кубанский Государственный Технологический Университет
г. Краснодар, Россия
sapka@pisem.net

Possibilities of a cybercriminal preserving confidentiality of information and own anonymity in the face of Public services of global electronic supervision

Shabanov A.V.

The Kuban State Technological University
Krasnodar, Russia
sapka@pisem.net

The purpose of the given work is acquaintance to effective methods of which the malefactor for detour of the state systems of the global electronic control can take advantage and which are necessary for taking into consideration to special services to provide the complete control of the information extended on communication channels and effective disclosing of crimes made by means of cybernetic networks.

Целью данной работы является приведение и применение к сведениям действенных методов, которыми может воспользоваться злоумышленник для обхода государственных систем глобального электронного контроля и которые необходимо принимать во внимание спецслужбам, дабы обеспечить целостный контроль распространяемой по каналам связи информации и эффективное раскрытие совершаемых посредством кибернетических сетей преступлений.

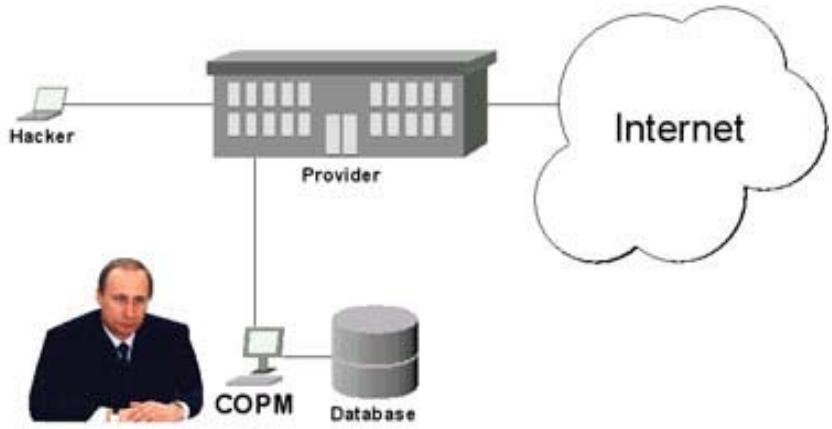
Высокий уровень развития информатизации общества позволяет кибернетическим преступникам применять все более изощренные методы в области обеспечения скрытности и безопасности своих противозаконных действий. Ввиду этого государственные службы, ведущие глобальный электронный надзор в сети ИНТЕРНЕТ должны принимать все более действенные программы по пресечению незаконных действий такого рода. Такие международные системы глобального позиционирования как «Carnivore» (Европа), и более серьезная «Echelon» (NATO), призваны контролировать весь поток информации, циркулирующей в сетях связи. Данные программы выполняют роль «всевидящего ока», задача которого знать все обо всех, или если не все обо всех, то о потенциальных нарушителях точно (сюда входит любая информация, включающая не только интернет-данные, но данные сотовой и спутниковой связи, а также любые сертифицированные способы коммуникации). Подобная система информационного контроля глобального позиционирования есть и у Российской спецслужбы «СОРМ». В данной работе собраны наиболее действенные методы обхода данной системы правопорядка, которые в такой же мере применимы и к зарубежным аналогам. Однако! Государственные системы информационного надзора – лишь техническая сторона своевременного пресечения и поиска кибер-преступника. Для своевременной и эффективной работы спецслужбам необходима разработка высокоэффективных организационных мер. В настоящее время серьезным препятствием для служб, а также лазейкой для кибер-преступников является отсутствие государственных границ в пространстве интернет при возможности получения доступа в любую точку мира с противоположной стороны планеты. В решении данной проблемы достигнуты определенные договоренности, такие как «Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» ратифицированное Советом Федерации 19 сентября 2008г. Однако! Порой становится невозможным договориться с другим государством о выдаче данных с требуемого персонального компьютера или выдаче самого преступника. Целью данной работы является приведение и применение к сведениям действенных методов, которыми может воспользоваться злоумышленник для обхода

государственных систем глобального электронного контроля и которые необходимо принимать во внимание спецслужбам, дабы обеспечить целостный контроль распространяемой по каналам связи информации и эффективное раскрытие совершаемых посредством кибернетических сетей преступлений.

Теперь рассмотрим подробно схему работы спецслужб по выявлению киберпреступника.

В большинстве случаев спецслужбе удается установить IP-адрес хакера, но это ничего не значит, т. к. главная цель — узнать ФИО «преступника» и возможно дом. адрес. Здесь все упирается в провайдера, т. к. только провайдер может сказать, кому принадлежит IP, а в случае с DialUP — с какого телефона осуществлялось подключение. Если хакер находится в России, то российским спецслужбам в этом плане значительно проще (практически все отечественные провайдеры находятся под контролем российских спецслужб). Но не нужно считать, что иностранным спецслужбам вообще никак не удастся установить личность. Если совершенный хак будет достаточно серьезным, то не исключено, что спецслужбам обоих сторон удастся договориться. Если нет, то нарушителя будут вычислять по косвенным признакам. Например, если после совершенного взлома, он, пользуясь одной и той же цепочкой прокси, заказывает себе домой на amazon.com какой-нибудь стафф, то, в случае, если дело ведут американские спецслужбы, им не составит никакого труда «надавить» на админов магазина, с требованием выдать его адрес (в свете 11 сентября это вообще не проблема, достаточно объявить тебя террористом). В общем, пока в Интернете есть хоть немного личной информации, ее могут раскопать, способов для этого много и службы ими хорошо владеют (к тому же, вполне реально хакнуть и самого провайдера).

Но существует механизм, о котором почему-то многие нарушители забывают.



Государство следит за потоком данных в сети.

COPM расшифровывается как «система оперативно-розыскных мероприятий», подразделяется на две системы: **COPM-1 и COPM-2**. Первая предназначена для контроля телефонной связи, вторая анализирует Интернет-трафик. Требования COPM реализованы и для российского сегмента системы спутниковой связи Глобалстар. Согласно ПРИЛОЖЕНИЮ к приказу Госкомсвязи России от 27.03.99г. №47 «ОБЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СИСТЕМЕ ТЕХНИЧЕСКИХ СРЕДСТВ ПО ОБЕСПЕЧЕНИЮ ФУНКЦИЙ ОПЕРАТИВНО – РОЗЫСКНЫХ МЕРОПРИЯТИЙ НА СЕТЯХ (СЛУЖБАХ) ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ», в рамках этой системы каждый интернет-провайдер был обязан установить оборудование, программы и выделенную линию для местного отделения ФСБ. Этот комплекс мер предоставляет ФСБ и МВД возможность дистанционно отслеживать, перехватывать и прерывать связь любого клиента этого провайдера. Сегодня сотрудники спецслужбы смогут осуществлять несанкционированный доступ к данным, передаваемым любым абонентом Internet и других сетей непосредственно из своих помещений и о факте такого доступа не будет известно даже провайдеру.

Итак о самих возможностях системы COPM-2, все эти операции могут вестись в режиме реального времени. Список конечно неполный:

1. Просмотр содержания передаваемых сообщений, т.е оператор системы может совершенно свободно читать и перехватывать всю электронную почту, файлы и другую интересующую его информацию, просматривать загружаемые на компьютер наблюдаемого лица HTML-страницы, WML-страницы, содержимое TCP/UDP сессий, отправляемые SMS-сообщения;

2. Прослушивание звонков операторов стационарной и мобильной телефонной связи, а также разговоров с использованием IP-телефонии;

3. Сканирование и фильтрация информации по различным параметрам (имени получателя и отправителя, ключевым словосочетаниям и адресам сайтов, которые могут идентифицировать их автора и посетителя как потенциально опасный объект;

4. Отслеживание адресов электронной почты, их источников и адресатов, времени их передачи, IP-адресов, номеров телефонов (SIM-карт) и внутренних идентификаторов самих мобильных терминалов (IMEI), номеров телефонов стационарных АТС и номеров телефонов в звонках IP-телефонии. Контроль учетных записей и UIN пользователей ICQ и другой подобной информации;

5. Анализ информации одновременно от многих источников и возможность получения вывода о ее принадлежности одному физическому лицу, концессированной группе или интернет-сообществу. Анализ контактов объектов наблюдения;

6. Создание специализированной базы данных для хранения и обработки информации.

Возможный алгоритм работы системы можно показать на конкретном примере, а именно почему не может быть полностью анонимным вариант работы в Internet с мобильного телефона из собственного дома.

Во время сеанса Internet через мобильник у оператора связи остаются логи вашего входа-выхода в сеть и посещенных вами сетевых адресов. В этом логе кроме данных самого телефона (номера SIM-карты и внутреннего аппаратного идентификатора мобильника IMEI – проверяется набором комбинации *#06#) остается еще идентификатор вышки ретранслятора (базовой станции) – а это ваше примерное место жительства с точностью до нескольких сот метров (+/- 200 метров). Понятно, что в этом радиусе может проживать несколько тысяч человек, но здесь есть одно большое НО. Мы не сегодня начали пользоваться Internet. Мы тысячи раз выходили в сеть со своего «белого» IP-адреса и посещали разные «интересные» сайты и форумы. Не важно писали мы там что-то или нет. Мы так же тысячи раз пользовались Яндексом или Рамблером для поиска нужной нам информации. При этом вводили в строку «поиск» определенные слова. Проблема в том, что таких «опасных» слов (имен, названий, определений и.т.п.) на самом деле не так уж и много – в пределах тысячи-двух, что для их анализа при помощи современных ЭВМ является несложной задачей. Т.е. в случае работы в сети Internet с мобильника из своей квартиры, при пересечении вами некой запретной черты – срабатывает как бы «звоночек» и ваша пока виртуальная личность ставится на контроль. Далее из тех нескольких тысяч человек (видите, уже «круг» сузился, т.к. компьютер хотя уже почти и в каждом доме, но не все пользуются Internet, если и пользуются, то для семьи из 4 человек точка доступа в сеть в 99% случаев всего одна.) остается уже несколько сотен. Затем СОРМ обращается к базам данных по провайдерам, работающим в вашей местности. Конкретно анализируются логи тех интернет-адресов, которые с некоторых IP-адресов, расположенных в уже очерченном круге, посещались за последнее время. Здесь опять используются определенные «опасные» маркеры – адреса конкретных «экстремистских» и «вольнодумских» сайтов. Круг еще сузился, причем очень сильно – до нескольких человек, а возможно уже и до вас одного. Далее может делается запрос к российским поисковикам - включается лингвистический анализ ваших запросов, и на этом этапе делается вывод о том , просто так вы заходите на те самые сайты, или это у вас уже образ жизни такой «неправильный». Все – вы попались, как птичка в клетку.

Обозначенные ниже пункты, при полном рассмотрении которых становится очевидным возможность полного ухода из под наблюдения каких-либо систем глобального оперативного контроля в сети интернет, не представляется возможным раскрыть в рамках данного презентационного сообщения..

- **определение порога срабатывания СОРМ.** (Как определить, какие именно виды сетевой деятельности гражданина являются «компрометирующими»);
- **описание методов и средств по обеспечению информационной безопасности от СОРМ;**
- **разрыв цепочки СОРМ.** (Возможности ухода от непосредственного ведения наблюдения за вами в текущий момент времени).

Компьютерные преступления и Российское законодательство

Шаймарданов Д.И.

Ноябрьский Колледж профессиональных и информационных технологий
г. Ноябрьск, Россия
dia1479@mail.ru

Computer crimes and Russian Legislation

Shaimardanov D.I.

Professional and Informational Technologies College
Noyabrsk, Russia
dia1479@mail.ru

This work represents the full research of crimes dealing with information technology field in Russian legislation. The author examines computer crime classification, the way of perpetration and prevention of wrong.

The growth of scientific and technological advance, connecting with realization of up-to-date information technologies, leads to unlawful interference in electronic computer processing, systems and network, theft, misappropriation and extortion of computer information. According to these crimes' mechanisms, the ways of perpetration and information hiding these types of crimes are possessed of definite structure and are characterized by the high level of latency and the low level of crime detection.

The main purpose of this research work is to examine such crimes in computer information field from the point of view of Russian legislation; to discover the way of computer crime perpetration.

The main aspects:

- to study the literature and the other information sources dealing with the problem of the research work;
- define the terms "computer information", "computer crime" from the point of view of Russian legislation;
- to make the classification of computer crimes;
- to observe the way of perpetration and prevention of computer crimes.

"Computer crime", as the penal term, is provided in punitive law for culpable infringement someone's rights and interests concerning the computer- aided system of data processing perpetrated harmful to the rights and interests of natural and legal persons, societies and states, which are subject to legal safeguard.

The distinguishable features of such crimes are high latency, complexity of collection evidence, transnational character (as a rule the telecommunication system usage), the meaning of property damage, and also the specificity of such criminals.

Computer crimes are committed crimes using the computer information. Ft this case computer information is the subject and (or) means of committed crimes.

Computer crimes are divided into several categories according Russian legislation:

- in circulation computer information field;
- in telecommunication field (article 138 of Russian Federation criminal code);
- in information equipment field;
- in defense of protected information field;

- in information legal relationship field;
- in economy and computer information field.

The most important and determinant element of any crime's criminalistic description is the way of its perpetration

Computer crimes, determined as socially dangerous acts, in which the computer information is the method or object of criminal tresspass, may be combined in four main groups according to the methods of computer information usage by criminals:

1. information interception;
2. unauthorized access;
3. data manipulation;
4. complex methods.

Three main action groups are distinguished for preventing computer crimes, putting together the whole system of struggle with these socially dangerous phenomena: legal, technical-organizational and criminalistic groups.

Theoretical meaning of this research work consists in the opportunity of usage such materials in educational process.

В представленной работе проведено исследование вопроса отражения преступлений в области информационных технологий в Российском законодательстве. Рассмотрена классификация компьютерных преступлений, способы их совершения и предупреждения.

Развитие научно-технического прогресса связанное с внедрением современных информационных технологий, привело незаконному вмешательству в работу электронно-вычислительных машин, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации. По своему механизму, способам совершения и сокрытия эти виды преступлений имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости.

Цель работы: Рассмотреть преступления в сфере компьютерной информации с точки зрения Российского законодательства, выявить способы совершения компьютерных преступлений

Задачи:

- Изучить литературу и другие информационные источники по теме исследования;
- Определить понятия «компьютерная информация», «компьютерное преступление» с точки зрения Российского законодательства;
- Провести классификацию компьютерных преступлений;
- Рассмотреть способы совершения и предупреждения компьютерных преступлений.

Компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Отличительными особенностями данных преступлений являются высокая латентность, сложность сбора доказательств, транснациональный характер (как правило, с использованием телекоммуникационных систем), значительность материального ущерба, а также специфичность самих преступников.

Компьютерные преступления - это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и (или) средством совершения преступления.

Компьютерные преступления по российскому законодательству делятся на несколько категорий:

- в сфере оборота компьютерной информации;
- в сфере телекоммуникаций (ст. 138 УК РФ);

- в сфере информационного оборудования;
- в сфере защиты охраняемой информации;
- в сфере информационных правовых отношений;
- в сфере экономики и компьютерной информации.

Важнейшим и определяющим элементом криминалистической характеристики любого преступления является способ его совершения.

Компьютерные преступления, определяемые как общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства, можно объединить в четыре основные группы по методам использования преступниками машинной информации:

1. перехват информации;
2. несанкционированный доступ;
3. манипуляция данными;
4. комплексные методы.

Выделяются три основные группы мер предупреждения компьютерных преступлений, составляющие в своей совокупности целостную систему борьбы с этим социально опасным явлением: правовые, организационно-технические и криминалистические.

Теоретическая значимость работы состоит в систематизации информации в области компьютерных преступлений с точки зрения Российского законодательства

Практическая значимость заключается в возможности применения материалов исследования в образовательном процессе.

2 Секция

Компьютерные угрозы. Угрозы для мобильных устройств

Computer threats and threats targeting mobile devices

Мобильные вирусы и технологии борьбы с ними

Алексеев И.С, Атапин А.В, Тухтаманов Д.В.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
ank@ssau.ru

Transportable viruses and technologies of struggle against them

Alekseev I.S., Atapin A.V., Tuhtamanov D.V.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
ank@ssau.ru

Мы живем в век, когда средства коммуникации достигли того уровня развития, о котором, пожалуй, еще полсотни лет назад можно было только мечтать. Мы не задумываемся над тем, какое расстояние преодолеваем, набирая номер мобильного телефона человека, находящегося за тысячи километров от нас. Думаю, никто не будет спорить с тем, что удобство использования мобильного телефона в качестве записной книжки, почтового ящика и средства доступа в Интернет значительно экономит наше время и облегчает ведение дел. Но это одна из сторон медали. С другой стороны развитие мобильных технологий подготовило для хакерского сообщества огромное поле для работы. Тогда как в компьютерной среде к появлению нового вируса мы относимся как к должному, в среде мобильных технологий этого встречается не часто, но всё же происходит. Пока хакеры ведут разведку боем, изредка посылая своих «бойцов». Наши телефоны, смартфоны, КПК пока еще не подвергались массированным атакам и будем надеяться, что этого не будет и в будущем, но мы уже сейчас должны быть во всеоружии, чтобы встретить врага в любой момент.

В данной работе мы расскажем об уже существующих мобильных вирусах и о способах борьбы с ними. Попробуем спрогнозировать, что нас ждет в будущем, какие перспективные направления борьбы с мобильными вирусами можно будет развивать в будущем.

К вопросу уязвимостей Web-браузеров

Ануфриев А.В., Сидоров М.В.

Новосибирский государственный архитектурно-строительный университет
г. Новосибирск, Россия

god_dja@list.ru

On the problem of Web-browser vulnerabilities

Anufriev A.V., Sidorov M.V.

Novosibirsk state architectural - building university
Novosibirsk, Russia

god_dja@list.ru

Nowadays it is almost impossible to imagine human activity without the Internet which has penetrated through many spheres of everyday life. Of course, it has been noticed by various hacker communities, and that can be proved by numerous publications and reports of leading world IT-companies dealing with the development of antivirus software. For example, the company Symantec has investigated that nearly 80 % of all hacker attacks in the Internet aim at web-cites and web-browsers, and the diversity of these hacker operations is very wide – from fishing to user's private information espionage (www.egovernment.com).

This particular work has a review nature, and the producers have tried to analyze and systematize the principal threats and hacker attacks existing in web-security from the point of view of web-browsers. As the latter are the programs providing PC users with the access to the Internet, researches of various vulnerabilities of web-browsers and their shooting have become quite urgent research issue to date. The producers have pointed out the vulnerabilities or imperfections and defects in web-browsers, with a help of which hackers can influence IMS to cheat the integrity or cause the misoperation of different applets. They have also adduced the arrangement of the applets and the comparison of web-browsers in the presence of loopholes or defects. The producers also adduce guidelines making possible to secure users against attacks appearing in line with the vulnerabilities of web-browsers.

В настоящее время невозможно представить деятельность человека без Internet, который проник практически во все сферы деятельности человечества. Естественно, это не осталось незамеченным различными хакерскими сообществами, что подтверждается многочисленными публикациями и отчетами ведущих мировых IT-компаний по разработке антивирусного программного обеспечения. Так, например, по результатам исследований, проведенных компанией Symantec, примерно 80% всех хакерских атак в сети Internet нацелены на web-сайты и web-браузеры, причем палитра проводим хакерских акций самая разнообразная – от фишинга до шпионажа конфиденциальной информации пользователя (http://www.egovernment.ru/main.php).

Данная работа носит обзорный характер, где авторы попытались провести анализ и систематизацию основных угроз и хакерских атак, которые существуют в web-безопасности, с точки зрения web-браузеров. Поскольку web-браузеры являются программами, обеспечивающими пользователям персональных компьютеров (ПК) доступ в сеть Internet, то исследования различных уязвимостей web-браузеров и их устранения становится достаточно актуальной темой сегодняшнего дня. Показаны уязвимости в web-браузерах, т.е. недостатки и недоработки, с помощью которых хакеры могут воздействовать на операционную систему ПК для нарушения ее целостности или вызвать неправильную работу различных приложений, приведена их классификация, сравнение web-браузеров по наличию "дыр"-недоработок. Также авторы приводят ряд рекомендаций, позволяющих обезопасить пользователя от угроз, возникающих в связи с уязвимостями web-браузеров.

Беспроводные сети Wi Fi. И их Безопасность

Босова М.

Самарский государственный аэрокосмический университет им. академика С.П. Королева

г. Самара, Россия

ank@ssau.ru

Wireless networks Wi Fi. And their Safety

Bosova M.

The Samara state space university of academician S.P. Koroleva

Samara, Russia

ank@ssau.ru

1. Беспроводные сетевые технологии (wi-fi)

Беспроводные сетевые технологии все глубже и глубже входят в нашу жизнь. Сегодня уже немыслимо представить рабочий офис без компьютеров, локальных сетей и защиты от проникновения извне. Домашние компьютеры стали практически бесполезны без подключения к Интернету. Беспроводные сетевые технологи позволяют Вам, где бы Вы не находились, быть подключенными к сети, обмениваться данными, находить нужную информацию в Интернете или же просто играть с кем-то.

Постоянно расширяющийся спектр оборудования, усовершенствование стандартов и улучшение защиты делает возможным применение wi-fi в корпоративный локальных сетях. Новейшее оборудование соответствует высочайшим требованиям безопасности, устойчивости и высокой скорости.

Удобство использования и хорошая защищенность делают возможным применение беспроводных сетевых технологий и в домашних условиях. Независимость от проводов, возможность объединения нескольких компьютеров дома в беспроводную сеть и еще многое другое уже стали практически стандартом у многих пользователях Интернета.

2. Стандарты беспроводных сетей

На данный момент существует четыре основных стандарта Wi-Fi - это 802.11a, 802.11b, 802.llg и 802.Hi. Из них в России используются два из них: 802.11b и 802.llg. В 2006 году в России должен появиться и 802.Hi. К 2007 году планируется начать внедрение еще одного стандарта - 802.11п.

802.11b

Это первый беспроводной стандарт появившийся в России и применяемый повсеместно до сих пор. Скорость передачи довольно невысокая, а безопасность находиться на довольно низком уровне. При желании злоумышленнику может потребоваться меньше часа для расшифровки ключа сети и проникновения в вашу локальную сеть. Для защиты используется протокол WEP, который охарактеризовал себя не с лучшей стороны и был взломан несколько лет назад. Мы рекомендуем не применять данных стандарт не дома ни тем более в корпоративных вычислительных сетях. Исключение может составлять те случаи, когда оборудование не поддерживает другой, более защищенный стандарт.

- Скорость: 11 Mbps
- Радиус действия: 50 м
- Протоколы обеспечения безопасности: WEP –Уровень безопасности: низкий

802. llg

Это более продвинутый стандарт, пришедший на смену 802.11b. Была увеличена скорость передачи данных почти в 5 раз, и теперь она составляет 54 Mbps. При использовании оборудования поддерживающего технологии superG* или True MIMO* предел максимально достижимой скорости

составляет 125 Mpbs. Возрос и уровень защиты: при соблюдении всех необходимых условий при правильной настройке, его можно оценить как высокий. Данный стандарт совместим с новыми протоколами шифрования WPA и WPA2*. Они предоставляют более высокий уровень защиты, нежели WEP. О случаях взлома протокола WPA2* пока не известно.

*- Поддерживается не всем оборудованием

-54 Mbps, до 125* Mbps

- Радиус действия: 50 м

- Протоколы обеспечения безопасности: WEP, WPA, WPA2* -Уровень безопасности: высокий

802.Hi

Это новый стандарт, внедрение которого только начинается. В данном случае непосредственно в сам стандарт встроена поддержка самых современных технологий, таких как True MIMO и WPA2. Поэтому необходимость более тщательного выбора оборудования отпадает. Планируется, что это стандарт придет на смену 802.llg и сведет на нет все попытки взлома.

- Скорость: 125 MbpsK

- Радиус действия: 50 м

- Протоколы обеспечения безопасности: WEP, WPA, WPA2

-Уровень безопасности: Высокий

802.11П

Будущий стандарт, разработки которого ведутся в данный момент. Этот стандарт должен обеспечить большие расстояния охвата беспроводных сетей и более высокую скорость, вплоть до 540 Мбит/сек.

- Скорость: 540 MbpsK

- Радиус действия: неизвестно м

- Протоколы обеспечения безопасности: WEP, WPA, WPA2

-Уровень безопасности: Высокий

Однако, следует помнить, что неправильная настройка оборудования, поддерживающего даже самые современные технологии защиты, не обеспечит должный уровень безопасности вашей сети. В каждом стандарте есть дополнительные технологии и настройки для повышения уровня безопасности. Поэтому мы рекомендуем доверять настройку Wi-Fi оборудования только профессионалам.

3. Безопасность беспроводных сетей

Введение

У беспроводных сетей очень много общего с проводными, но есть и различия. Для того, чтобы проникнуть в проводную сеть, хакеру необходимо физически к ней подключиться. В варианте Wi-Fi ему достаточно установить антенну в ближайшей подворотне в зоне действия сети.

Хотя сегодня в защите Wi-Fi-сетей и применяются сложные алгоритмические математические модели аутентификации, шифрования данных, контроля целостности их передачи, тем не менее на начальных этапах распространения Wi-Fi нередко появлялись сообщения о том, что даже не используя сложного оборудования и специальных программ можно было подключиться к некоторым корпоративным сетям просто проезжая мимо с ноутбуком. Появились даже легенды о разъезжающих по крупным городам хакерах (war driver) с антеннами, сооруженными из консервной банки или упаковки из-под чипсов. Якобы у них даже была своя условная система знаков, которые рисовались на тротуаре и указывали незащищенные должным образом точки доступа. Возможно, так и было, лишь вместо банок из-под чипсов использовались мощные антенны, а условные знаки обозначались на карте, связанной с системой глобального позиционирования (GPS).

Что же теоретически может получить злоумышленник в беспроводной сети, настройке которой не было уделено должного внимания? Вот стандартный список:

- доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё — и к ресурсам LAN; подслушивание трафика, извлечение из него конфиденциальной информации; искажение проходящей в сети информации; воровство интернет-траффика;
- атака на ПК пользователей и серверы сети (например, Denial of Service или даже глушение радиосвязи);
- внедрение поддельной точки доступа;
- рассылка спама, противоправная деятельность от имени вашей сети. *Развитие защиты Wi-Fi*

В 1997 году вышел первый стандарт IEEE 802.11, безопасность которого, как оказалось, далека от идеала. Простой пароль SSID (Server Set ID) для доступа в локальную сеть по современным меркам нельзя считать защитой, особенно, учитывая факт, что к Wi-Fi не нужно физически подключаться.

Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII, что соответствует 40 или 104-разрядному шифрованию на статическом уровне. Как показало время, WEP оказалась не самой надёжной технологией защиты. И, кстати, все основные атаки хакеров пришлись как раз-таки на эпоху внедрения WEP.

После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.IX, который использует вариант динамических 128-разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows XP поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам.

В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.IX с кодированием протокола интеграции временного ключа Temporal Key Integrity Protocol (TKIP), протоколом расширенной аутентификации Extensible Authentication Protocol (EAP) и технологией проверки целостности сообщений Message Integrity Check (MIC).

Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPA2, или 802.Hi, — максимально защищенный стандарт.

Технологии защиты

WEP

Эта технология была разработана специально для шифрования потока передаваемых данных в рамках локальной сети. Данные шифруются ключом с разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 (40+24) до 128 (104+24) бит. Идея очень здравая, поскольку при шифровании мы оперируем и постоянными, и случайно подобранными символами.

Но, как оказалось, взломать такую защиту можно — соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack). Основное её слабое место — это как раз-таки вектор инициализации. Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций (2 в 24 степени) — после использования этого количества ключ начинает повторяться. Хакеру необходимо найти эти повторы (от 15 минут до часа для ключа 40 бит) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

802. IX

IEEE 802.IX — это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. На данный момент он поддерживается только со стороны ОС Windows XP и анонсирован для Windows Server 2003. За основу взято исправление недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, зависимость от технологий производителя и т. п. 802.IX позволяет подключать в сеть даже PDA-устройства, что

позволяет более выгодно использовать саму идею беспроводной связи. С другой стороны, 802.IX и 802.11 являются совместимыми стандартами. В 802.IX применяется тот же алгоритм, что и в WEP, а именно — RC4, но с некоторыми отличиями.

802.IX базируется на протоколе расширенной аутентификации Extensible Authentication Protocol (EAP), протоколе защиты транспортного уровня Transport Layer Security (TLS) и сервере доступа RADIUS (Remote Access Dial-in User Server). Плюс к этому стоит добавить новую организацию работы клиентов сети. После того, как пользователь прошёл этап аутентификации, ему высылается секретный ключ в зашифрованном виде на определённое незначительное время — время действующего на данный момент сеанса. По завершении этого сеанса генерируется новый ключ и опять высылается пользователю. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

WPA

WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.Hi. По сути, WPA = 802.IX + EAP + TKIP + MIC, где:

WPA — технология защищенного доступа к беспроводным сетям (Wi-Fi Protected Access),

EAP — протокол расширенной аутентификации (Extensible Authentication Protocol),

TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol),

MIC — технология проверки целостности сообщений (Message Integrity Check).

Как видим, ключевыми здесь являются новые модули TKIP и MIC. Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищенной.

От внешнего проникновения и изменения информации также обороняет технология проверки целостности сообщений (Message Integrity Check). Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены

изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, кстати говоря, уже давно используется в VPN. Что касается WPA, поддержка AES уже реализована в Windows XP, пока только опционально.

VPN

Технология виртуальных частных сетей Virtual Private Network (VPN) была предложена компанией Intel для обеспечения безопасного соединения клиентских систем с серверами по общедоступным интернет-каналам. VPN очень хорошо себя зарекомендовали с точки зрения шифрования и надёжности аутентификации. Плюс технологии состоит и в том, что на протяжении более трёх лет практического использования в индустрии данный протокол не получил никаких нареканий со стороны пользователей. Информации о его взломах не было.

Технологий шифрования в VPN применяется несколько, наиболее популярные из них описаны протоколами PPTP, L2TP и IPSec с алгоритмами шифрования DES, Triple DES, AES и MD5. IP Security (IPSec) используется примерно в 65—70% случаев. С его помощью обеспечивается практически максимальная безопасность линии связи.

И хотя технология VPN не предназначалась изначально именно для Wi-Fi, она может использоваться для любого типа сетей, и идея защитить с её помощью беспроводные их варианты одна из лучших на сегодня.

Для VPN выпущено уже достаточно большое количество программного (ОС Windows NT/2000/XP, Sun Solaris, Linux) и аппаратного обеспечения. Для реализации VPN-защиты в рамках сети необходимо установить специальный VPN-шлюз (программный или аппаратный), в котором создаются туннели, по одному на каждого пользователя. Например, для беспроводных сетей шлюз следует установить непосредственно перед точкой доступа. А пользователям сети необходимо

установить специальные клиентские программы, которые в свою очередь также работают за рамками беспроводной сети и расшифровка выносится за её пределы.

Хотя всё это достаточно громоздко, но очень надёжно, главный недостаток такого решения — необходимость в администрировании. Второй существенный минус — уменьшение пропускной способности канала на 30—40%.

Методы защиты

Таким образом, на сегодняшний день у обычных пользователей и администраторов сетей имеются все необходимые средства для надёжной защиты Wi-Fi, и при отсутствии явных ошибок (пресловутый человеческий фактор) всегда можно обеспечить уровень безопасности, соответствующий ценности информации, находящейся в такой сети. Основные же правила при организации и настройке частной Wi-Fi-сети (если нет задачи сделать её общедоступной) таковы:

максимальный уровень безопасности обеспечит применение VPN — используйте эту технологию в корпоративных сетях;

если есть возможность использовать 802.IX (например, точка доступа поддерживает, имеется RADIUS-сервер) — воспользуйтесь ей (впрочем, уязвимости есть и у 802.IX);

перед покупкой сетевых устройств внимательно ознакомьтесь с документацией. Узнайте, какие протоколы или технологии шифрования ими поддерживаются. Проверьте, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов;

обратите внимание на устройства, использующие WPA2 и 802.111, поскольку в этом стандарте для обеспечения безопасности используется новый Advanced Encryption Standard (AES);

если точка доступа позволяет запрещать доступ к своим настройкам с помощью беспроводного подключения, то используйте эту возможность. Настраивайте AP только по проводам. Не используйте по радио протокол SNMP, web-интерфейс и telnet;

если точка доступа позволяет управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List), используйте эту возможность. Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника;

если оборудование позволяет запретить трансляцию в эфир идентификатора SSID, используйте эту возможность (опция может называться "closed network"), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента;

запретите доступ для клиентов с SSID по умолчанию "ANY", если оборудование позволяет это делать. Не используйте в своих сетях простые SSID — придумайте что-нибудь уникальное, не завязанное на название вашей организации и отсутствующее в словарях. Впрочем, SSID не шифруется и может быть легко перехвачен (или подсмотрен на ПК клиента);

располагайте антенны как можно дальше от окон, внешних стен здания, а также ограничивайте мощность радиоизлучения, чтобы снизить вероятность подключения «с улицы». Используйте направленные антенны, не используйте радиоканал по умолчанию;

если при установке драйверов сетевых устройств предлагается выбор между технологиями шифрования WEP, WEP/WPA (средний вариант), WPA, выбирайте WPA (в малых сетях можно использовать режим Pre-Shared Key (PSK)). Если устройства не поддерживают WPA, то обязательно включайте хотя бы WEP. При выборе устройства никогда не приобретайте то, что не поддерживает даже 128bit WEP.

всегда используйте максимально длинные ключи. 128-бит — это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырёх заранее заданных ключей — сообщите клиентам о том, в какой день недели какой ключ используется).

не давайте никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание траффика путем внедрения в передаваемый поток — очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор;

если вы используете статические ключи и пароли, позаботьтесь об их частой смене. Делать это лучше одному человеку — администратору;

если в настройках устройства предлагается выбор между методами WEP-аутентификации "Shared Key" и "Open System", выбирайте "Shared Key". Если AP не поддерживает фильтрацию по MAC-адресам, то для входа в "Open System" достаточно знать SSID, в случае же "Shared Key" клиент должен знать WEP-ключ (www.proxim.com/ support/ all/ harmony/ technotes/ tn2001-08-10c.html). Впрочем, в случае "Shared Key" возможен перехват ключа, и при этом ключ доступа одинаков для всех клиентов. В связи с этим многие источники рекомендуют "Open System";

обязательно используйте сложный пароль для доступа к настройкам точки доступа. Если точка доступа не позволяет ограничивать доступ паролем, её место на свалке;

если для генерации ключа предлагается ввести ключевую фразу, то используйте набор букв и цифр без пробелов. При ручном вводе ключа WEP вводите значения для всех полей ключа (при шестнадцатеричной записи вводить можно цифры 0—9 и буквы a—f).

по возможности не используйте в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее. Не разрешайте гостевой доступ к ресурсам общего доступа, используйте длинные сложные пароли;

по возможности не используйте в беспроводной сети DHCP — вручную распределить статические IP-адреса между легитимными клиентами безопаснее;

на всех ПК внутри беспроводной сети установите файерволлы, старайтесь не устанавливать точку доступа вне брандмауэра, используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл стоит обычно один — на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл;

регулярно исследуйте уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновляйте прошивки и драйвера устройств, устанавливайте заплатки для Windows.

Наконец, просто не отправляйте особо секретные данные через Wi-Fi. А ещё можно использовать точки доступа-приманки (AP honeypot, www.blackalchemy.to/Projects/fakeap/fake-ap.html), специальное оборудование (www.airdefense.net/products/), SSL и SSH.

4. Новые возможности защиты беспроводных сетей, используемые в Windows XP.

Вы думаете, что ваша беспроводная сеть в безопасности? Лучше подумайте еще раз. Новейший Wi-Fi стандарт, называемый «Wireless Protected Access 2» (WPA2), предоставляет профессиональный уровень шифрования данных, однако, не смотря на то, что стандарт существует уже более года, большинство пользователей все еще не используют его.

Безопасность WPA2 безусловно стоит тех скромных усилий, которые требуются для её установки. Стандарт безопасности WPA, являющийся базовым, может быть относительно легко взломан, даже если вы используете парольное слово длиной более 20 символов, и это не одно из тех слов, которые можно легко найти в словаре (не важно русском или каком-либо другом).

Пока же широко распространен предшественник стандарта WPA-"Wired Equivalent Privacy" (WEP), однако доверять данному стандарту безопасности, это все равно что не иметь безопасной сети вовсе. WEP может быть взломан буквально в секунды, и не имеет значения насколько сложный ключ вы для него использовали. WEP достаточен только для того, чтобы защитить трафик вашей сети от соседей или прохожих, т.е. тех, кто не будет тратить время на взлом вашей системы безопасности. Однако если вы серьёзно заботитесь о сохранении ваших личных данных, то вам нужен WPA2.

Прежде чем вы сможете защитить вашу сеть при помощи WPA2, вы должны загрузить и установить \Л/PA2-обновление для Windows XP (KB893357). Возможно, что вам так же понадобиться установить самую последнюю версию драйвера для вашей карты Wi-Fi. Такой драйвер можно найти на сайте Microsoft в каталоге Windows Update, но я бы рекомендовал обращаться непосредственно на сайт производителя карты.

Следующим шагом вам необходимо загрузить и установить новую прошивку для вашей беспроводной точки доступа, если она еще не имеет поддержки стандарта WPA2. Прошивку можно найти на сайте производителя вашей точки доступа. (Альянс Wi-Fi постоянно обновляет список продуктов, которые поддерживают стандарт WPA2. Здесь вы можете проверить, поддерживает ли

ваша точка доступа этот стандарт.) Если ваша беспроводная точка доступа слишком стара и не может быть обновлена до стандарта WPA2, или даже до базового стандарта WPA, то лучше всего её заменить; новая обойдется вам не дороже 40$.

После того как ваше оборудование будет обновлено, откройте страничку управления вашей точкой доступа при помощи Web-браузера (изучите руководство пользователя для получения более точной информации) и измените настройки безопасности на WPA2: Выберите TKIP+AES в качестве алгоритма использования WPA и введите парольное слово в поле, которое обычно называется «WPA Shared Key» и в поле подтверждения парольного слова. Ваше слово может содержать любую комбинацию букв и цифр длиной до 63-х знаков. Сохраните изменения, и на этом настройку точки доступа можно считать законченной.

При следующем подключении к точке доступа, защищенной при помощи WPA2, ваша система попросит вас ввести парольное слово (в терминах Windows это называется «ключ сети»). Введите парольное слово, которое вы использовали при настройке точки доступа, в соответствующие поля в диалоговом окне «Беспроводное сетевое подключение», и нажмите кнопку «Подключить». Теперь вы можете спокойно продолжать работать с вашей беспроводной сетью, при следующих подключениях пароль не будет запрашиваться, а соединение будет устанавливаться автоматически.

Защита flash-носителей от вредоносного программного обеспечения

Вальгер С.А., Сорокин Н.В.

Новосибирский государственный архитектурно-строительный университет
г. Новосибирск, Россия

swetlaya@mail.ru

The security of flash-mediums against of the malicious software

Val'ger S.A., Sorokin N.V.

Novosibirsk state architectural - building university
Novosibirsk, Russia

swetlaya@mail.ru

Nowadays it is impossible to imagine any human activity without the Internet which has crept into all the spheres of our life. It is natural that the current situation wasn't left unnoticed by the hacker communities which are proved by numerous publications and accounts given by the leading world IT-companies in the sphere of antiviral software (www.kaspersky.com, www.esetnod32.com). Consequently, the malware also tends to become more and more perfect day after day. This conclusion is also proved by the data of the Malware Rating Table issued by the Kaspersky Laboratory in January, 2009 (www.viruslist.com/ru/analysis?pubid=204007643).

The analysis of the before-mentioned data shows that the malware spread by means of USB-devices take more and more profound positions. That leads to the supposition that mail-spread and script-spread malware attacking a user's personal computer from afar are gradually substituted by other kinds of malware which is not perfect yet, but develops rapidly. It doesn't mean that such malware harms the USB-device itself. It accentuates the method of spreading and the special features of such attacks: the malware has an opportunity to get the access to the hardware as soon as you insert the USB-device into a USB-drive. This kind of malware takes various actions and achieves a wide range of results from interference with the normal work of the PC software to stealing passwords and other sorts of confidential information. It often happens that even PCs of experienced users appear to be infected by means of the before-mentioned method.

This investigation concerns the methods of penetration, infection and struggling with USB-malware. It is hard to contradict the fact that nowadays information is one of the main means of the defense of the users: "Forewarned is forearmed". That is why the profound investigation of the problem is the primary aim of this report.

В настоящее время не возможно представить деятельность человека без Internet, который проник практически во все сферы деятельности человечества. Естественно, что такое положение дел не осталось незамеченным со стороны различных хакерских сообществ, что подтверждается многочисленными публикациями и отчетами ведущих мировых IT-компаний по разработке антивирусного программного обеспечения (www.kaspersky.ru, www.esetnod32.ru). Следовательно, и тенденции в распространении вредоносного программного обеспечения (ПО) с каждым днем все более и более совершенствуются. Эти выводы также подтверждаются данными таблицы рейтинга вредоносных программ, опубликованной ЗАО «Лабораторией Касперского» в январе 2009 года (www.viruslist.com/ru/analysis?pubid=204007643).

Анализ данных таблицы рейтинга вредоносного ПО показывает, что вредоносное ПО, распространяющиеся через USB-носители, занимают все более и более прочные позиции. Из этого следует, что на смену почтовым и скриптовым вредоносным программам, атакующим компьютер пользователя удаленно, приходят другие пока еще не достигшие совершенства, но имеющие интенсивную динамику развития. Из этого не следует, что такое вредоносное ПО наносит урон

непосредственно USB-носителю. Здесь имеется в виду способ распространения и специфика атаки – достаточно вставить накопитель в USB-разъём, как вредоносное ПО получает возможность проникнуть на жесткий диск. Действия и результаты работы такого вредоносного программного обеспечения самые разнообразные – от нарушения работы программного обеспечения персонального компьютера (ПК) до кражи паролей и другой конфиденциальной информации пользователя ПК. Зачастую даже компьютеры опытных пользователей оказываются зараженными, и именно таким способом, который указанным выше.

В данной работе речь пойдет о методах проникновения, заражения и способах борьбы с USB-вредоносным программным обеспечением. Сложно спорить с тем, что информация является на сегодняшний день одним из главных средств защиты пользователя: «Предупрежден, значит вооружен». Именно поэтому всестороннее изучение вопроса – основная цель данного доклада.

“Voidman” virus comprehensive analysis

Erdenebat Chuluun

Mongolian University of Science and Technology
Ulaanbaatar, Mongolia
Ch.Erdenebat@gmail.com

In this article, we have aimed to examine and inspect the origin of “voidman” viruses that are “made in Mongolia” on a profound level. This anti-program is one of few viruses that are labeled “made in Mongolia” and from 2006 to 2007 it has damaged number of computers and their functioning in laboratories of many large universities of the country, causing immense inconvenience at the time.

The most computer viruses are thought to develop using the basis of the previous version and re-engineering them by investigating, recovering and neutralizing them is therefore thought to be possible. For this, we need to determine the method and the way of functioning of the virus, which will allow us to develop the system of “cure” (treatment), to detect the threat, also to handle any resistance programs accordingly. These issues are faced often.

When examining the “Voidman” viruses we have used the method of re-engineering of code tracking.

Keywords: virus, analysis, re-engineering.

Всесторонний анализ вируса Voidman

Эрденебат Чулуун

Монгольский университет науки и технологии
Улан-Батор, Монголия
Ch.Erdenebat@gmail.com

Цель настоящей статьи заключается в том, чтобы изучить и проверить происхождение вирусов voidman, которые "созданы в Монголии", на основательном уровне. Эта антипрограмма является одним из нескольких вирусов, которые имеют метку "Сделано в Монголии", и в период с 2006 г. по 2007 г. она нанесла вред ряду компьютеров и их работе в лабораториях многих больших университетов страны, вызывая при этом огромные неудобства.

Считается, что большинство компьютерных вирусов разрабатывается с использованием предыдущей версии, и поэтому предполагается, что возможен их реинжиниринг путем исследования, извлечения и нейтрализации. Поэтому для обнаружения угрозы и, соответственно, для работы с любыми антивирусными программами необходимо определить метод и способ функционирования вируса, которые позволят разработать систему "лечения". С этими вопросами часто приходится сталкиваться.

При анализе вирусов Voidman мы использовали метод реинжиниринга с отслеживанием кода.

Ключевые слова: вирус, анализ, реинжиниринг.

Разработка системы пассивного сбора событий сетевых атак (Honeypot): Bluetooth сети

Пустобаева Д.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
ank@ssau.ru

System development of passive collection of events network attacks (Honeypot): Bluetooth networks

Pustobaeva D.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
ank@ssau.ru

Технология **honeypot** - это один из методов, позволяющих отследить ранние признаки атаки, локализовать проблему до того, как атака затронет важные объекты системы, затормозить атаку, дав администратору время на принятие контрмер.

Honeypot - это информационная система, предназначенная для неправомерного доступа. Фактически, это обманка, привлекательный объект для атаки, при этом находящийся под полным контролем специалистов по безопасности. Информационная система honeypot может представлять собой как отдельный хост в сети, так и сеть, наполненную разного рода объектами: маршрутизаторами, серверами, рабочими станциями, реальными или виртуальными.

Выделяют два основных типа реализаций, эмулирующие и реальные, иногда их определяют как слабо- и высокоинтерактивные.

Первые способны эмулировать взаимодействие от лица определенного сервиса, например, принять соединение на tcp порт 22, принять от атакующего имя пользователя и пароль и так далее, при этом фиксируя все действия атакующего.

Высокоинтерактивные honeypot, основанные на применении реальных ОС и реальных сервисов, несколько сложнее в применении. Фактически они представляют собой специально спроектированные сетевые сегменты, подключенные к сетям общего пользования. Сетевой трафик между honeypot и внешним миром контролируется и фиксируется, чтобы полностью сохранить все действия атакующих.

Применение honeypot-систем в реальной жизни позволяет определять факт атаки, предотвращать атаки на реальные сервисы и обеспечивать службу безопасности материалами для анализа и ответной деятельности.

Определение факта атаки заложено в саму идею honeypot - к honeypot не могут обращаться за сервисом реальные клиенты. Если к нему обратились, это свидетельствует о том или ином нарушении. Определение факта атаки является важным моментом для администраторов, так как это позволяет оперативно принять меры противодействия.

Bluetooth - это новая технология беспроводной передачи данных малой мощности, разрабатываемая с целью замены существующих проводных соединений персональных офисной и бытовой техники с широким спектром переносных устройств, таких, как электронные записные книжки и мобильные телефоны, датчики сигнализации и телеметрии, и т.п.

Технология Bluetooth была разработана в 1998 году группой ведущих компаний в области телекоммуникаций. Bluetooth - это возможность объединять в локальные сети любую технику: от мобильного телефона и компьютера до холодильника. При этом, одни из немаловажных параметров технологии bluetooth - это низкая стоимость устройства связи, соответственно небольшие размеры и, что немаловажно, совместимость и простота встраивания в различные устройства. Эта технология использует небольшие приемопередатчики малого радиуса действия, либо непосредственно встроенные в устройство, либо подключаемые через свободный порт или PC-карту. Адаптеры

Bluetooth работают в радиусе 10 или 100 метров и, в отличие от IrDA (инфракрасный порт), не обязательно в зоне прямой видимости, то есть, между соединяемыми устройствами могут

быть различные препятствия, или стены. Bluetooth технология незаменима для оснащения мобильных телефонов различными внешними устройствами такими как handsfree, внешняя память или беспроводные модемы (PC-Card-модемы). Более того, bluetooth гарнитуры получили огромное распространение вследствие нескольких свойств: они обладают гораздо меньшей степенью излучения, чем сами мобильные телефоны, а также позволяют вести разговор по телефону без необходимости держать его в руке. Тем самым это bluetooth устройство практически незаменимо для использования в автомобиле, где требуется особое внимание и осторожность и любой разговор по телефону может привести к неприятным последствиям.

Bluetooth - название, данное новому стандарту современной технологии беспроводной передачи данных, использующему радиоволны на близком расстоянии, заменяющему кабель для соединения мобильных и/или установленных электронных устройств. Этот стандарт позволяет соединять друг с другом при минимальном пользовательском участии практически любые устройства: мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты и даже холодильники, микроволновые печи, кондиционеры. Соединить можно все, что соединяется, то есть имеет встроенный микрочип Bluetooth. Технология стандартизирована, следовательно, проблемы несовместимости устройств от конкурирующих фирм быть не должно. Технология также предлагает беспроводный доступ LAN, PSTN, сеть мобильных телефонов и Интернет для домашних приборов и портативных устройств.

Изначально технология Bluetooth создавалась лишь для радиосвязи, и никаких планов по созданию беспроводных локальных сетей на ее основе не было. Но такие проекты вскоре появились, и теперь существует понятие Bluetooth-сети.

Цель этого стандарта - обеспечить соединение любых устройств Bluetooth с другими устройствами Bluetooth, находящимися в непосредственной близости, независимо от торговой марки. Bluetooth допускает соединения электронных устройств и беспроводное сообщение через короткий диапазон, специальные сети, называемые piconet. Каждое устройство может соединяться максимально с семью устройствами в piconet. Также, каждое устройство может одновременно принадлежать нескольким сетям. Эти сети устанавливаются динамически и автоматически, поскольку устройства Bluetooth вступают в связь и покидают соединение с устройствами, находящимися поблизости. Потребность в устройствах Bluetooth возникает из-за двух факторов: развитие технологий и рыночная конкуренция. Способность размещать большего количества чипов на небольшой области позволила маленьким устройствам выполнять сложные протоколы. Теперь контроллеры в устройствах способны к программированию, управляемому и используемому в различных современных (smart) областях. Таким образом, теперь интеллектуальные устройства могут быть внедрены в работу пользователя и домашнее использование. Для подключения устройств к Интернет доступны различные методы, формируя так называемый "встроенный Интернет". Существенный прогресс был сделан в развитии маленьких и дешевых датчиков, которые могут получать нужные сигналы от пользовательской среды без участия пользователя или явной команды. Стали доступны новые виды электронных тэгов, позволяющие взаимодействие среди разнообразных устройств, JPNI и Piano. Это открыло возможности для создания "повсеместной компьютеризации" окружающей среды. В этой среде устройства контролируются комбинацией интеллектуальных систем и стратегически расположенных датчиков, которые работают без явной пользовательской поддержки. Средство для автоматизации сильно зависит от способности устройств к беспроводному соединению друг с другом, с более интеллектуальными центральными серверами, информационными складами, датчиками и реле. Bluetooth обеспечивает решение этого требования. Как было упомянуто ранее, непосредственная потребность в устройствах Bluetooth вызвана желанием соединить внешние устройства и устройства без кабелей. Доступная технология -IrDA OBEX - основана на инфракрасном излучении, которое ограничено видом подключения. IrDA обеспечивает связь лишь в зоне прямой видимости и только по принципу точка - точка. Bluetooth в будущем - это передвижной и беспроволочный доступ к LAN, Интернет по передвижным и другим существующим сетям, где сеть защищена, но интерфейс свободно передвигается. Это не только делает использование сети более легким, но и расширяет область её досягаемости. Bluetooth также может использоваться в приложениях домашней сети. С увеличением количества домашних PC, необходимость сетей, которые просто установить и легко обслуживать, растет. Основным направлением использования Bluetooth должно стать создание так называемых персональных сетей (PAN, или private area networks), включающих такие разноплановые устройства, как мобильные телефоны, PDA, MP3-плееры, компьютеры и даже микроволновые печи с холодильниками (вот уж что давно не подключали в сеть). Возможность передачи голоса позволяет встраивать интерфейс Bluetooth в беспроводные телефоны или, например, беспроводные гарнитуры для сотовых телефонов. Возможности применения Bluetooth на практике безграничны: помимо

синхронизации PDA с настольным компьютером или подсоединения относительно низкоскоростной периферии, типа клавиатур или мышей, интерфейс позволяет очень просто и с небольшими затратами организовать домашнюю сеть. Причем узлами этой сети могут быть любые устройства, имеющие потребность в информации либо обладающие необходимой информацией. Также существует коммерческая необходимость обеспечить "information push" способностям, которые являются важными для карманных компьютеров и других мобильных устройств, и это предусмотрено Bluetooth. Основная сила Bluetooth -способность одновременно обрабатывать данные и передачи голоса, позволяя такие инновационные решения как hands-free для голосовых звонков, печать факса, автоматическая синхронизация с PDA, ноутбук и приложения для записной книжки телефона. Все это говорит о том, что технология подобно Bluetooth чрезвычайно полезна и эффективна для развития пути приема информации.

Хотя технология Bluetooth изначально задумана для универсальных беспроводных соединений ноутбуков, PC и мобильных телефонов, сразу стало очевидно, что существует много других приложений для использования стандарта Bluetooth. Таким образом, стандарт Bluetooth не только пытается преодолеть ограничения проводных сетей, но также предлагает разнообразие другого сервиса, создает возможности для новых моделей использования.

Сейчас система Bluetooth получила даже большее признание, чем замененная кабельная технология. Различные модели использования открывают новые области для возможности применения Bluetooth. Соответственно, к технологии предъявляются всё новые требования, некоторые из них описаны ниже.

Наиболее важным требованием от беспроводных соединений является то, что должна быть универсальная структура, которая предлагает доступные и удобные средства доступа к информации набора различных устройств (PDA, ноутбуков, PC, мобильных телефонов, домашних приложений и т.п.). В практическом исполнении ожидается, что не все устройства будут отвечать ко всем функциональным возможностям, и пользователи могут ожидать, что знакомые им устройства выполнят свои основные функции обычным способом. Поэтому Bluetooth должен предложить средство для взаимодействия между устройствами, находящимися вблизи друг от друга, где каждое устройство обеспечивает свойственную ему функцию, основанную на форме, интерфейсе пользователя, стоимости и мощности, но дополнительный сервис появляется в результате взаимодействия. Стандарт должен дать возможность устройствам установить инициативное подключение. Устройства могут соединяться без специальной команды пользователя или действия, что позволяет использовать различные информационные ресурсы. Предусматривается поддержка передачи данных и голоса, поскольку это два наиболее важных вида информации, передаваемых сегодня по сетям. (Требования видео и мультимедиа также

налагаются на будущие версии Bluetooth). Стандарт должен уметь включать новые модели использования без требования какой-либо регистрации нового сервиса. Соединения должны предоставлять защиту данных, подобную защите при соединения через кабель. Выполнение этого стандарта должно быть простым, не громоздким и эффективным для легкого мобильного использования. Для быстрого развития системы и для наибольшей пользы Bluetooth необходимо на деле показать пользователям, что всё большее количество устройств подходит под стандарт Bluetooth. Эти устройства представляют собой весьма неоднородный набор, и, конечно, никакая отдельная компания не сможет производить все эти устройства. Поэтому немаловажным аспектом в развитии Bluetooth является тот факт, что эта технология не подлежит платному лицензированию и ее использование не требует выплаты каких-либо лицензионных отчислений (хотя и требует подписания бесплатного соглашения). Такая политика позволила многим компаниям энергично включиться в процесс разработки устройств с интерфейсом Bluetooth. Вышеупомянутые требования вносят большую техническую сложность не только в термины функциональных возможностей, которые будут обеспечены, но также и в термины по требованиям размера и мощности. Технология, разработанная для того, чтобы выполнить вышеупомянутые требования, должна столкнуться со следующими техническими требованиями:

Система должна использовать свободный от лицензирования диапазон для универсального использования, так как его используют не только системы научного эксперимента (ISM) и системы связи, но также и устройства типа микроволновых печей. Таким образом, для Bluetooth был выбран диапазон, который в некоторых странах называют Industrial, Scientific и Medical (ISM). Предпочтительно, чтобы каждый передатчик самостоятельно использовал бы необходимое минимальное количество мощности, чтобы не мешать другим пользователям.

Передатчики должны быстро приспосабливаться к меняющейся окружающей среде, так как обычно используются мобильные устройства. Должны быть решены всем известные проблемы беспроводных системах, установленные соединения и протоколы маршрутизации должны работать в окружающей

среде, где количество, разнообразие и разнообразие устройств Bluetooth будут динамически изменяться с соответствующей скоростью.

Размер исполнения должен быть маленький для легкой интеграции в карманные и мобильные устройства. Потребление мощности не должно превышать лишь маленькой доли от общего количества потребления мощности основным устройством, в котором будет представлен Bluetooth.

Технология должна быть приспосабливаемой к устройствам изменения вычислительной мощности и ресурсов памяти, чтобы количество устройств, совместимых с Bluetooth, увеличивалось.

Должно быть обеспечено автоматическое установление соединения. Количество и идентичность устройств меняется довольно часто, и будет неудобно каждый раз вручную устанавливать подключение.

Также должна быть достигнута синхронизация часов среди сообщающихся устройств. Так как у каждого устройства будут свои собственные свободно запущенные часы, то выполнение успешного соединения, особенно CDMA, - вызов сам по себе. Должны быть соблюдены требования безопасности. Устройства Bluetooth будут в личном использовании, будут содержать и сообщать конфиденциальную деловую информацию, информацию частного характера и другие данные, которые должны быть защищены. Помимо фокуса с частотными шаблонами и необходимости синхронизации приемопередачи в стандарте Bluetooth предусмотрено шифрование передаваемых данных с ключом эффективной длины от 8 до 128 бит и возможностью выбора односторонней или двусторонней аутентификации (конечно, можно обойтись вообще без аутентификации), что позволяет устанавливать стойкость результирующего шифрования в соответствии с законодательством каждой отдельной страны (в некоторых странах запрещено использование сильной криптографии). В дополнение к шифрованию на уровне протокола может быть применено шифрование на уровне приложений - здесь уже применение сколь угодно стойких алгоритмов никто не ограничивает.

У Bluetooth имеются конкуренты, IrDA OBEX и HomeRF. IrDA - технология инфракрасной (также беспроводной) связи. Спецификация HomeRF предназначена для связи бытовых аудио- и видеоустройств и построения домашних радиосетей. Передача данных также осуществляется на частоте 2.4 ЕГц, но со скачками 50 раз в секунду. Пропускная способность HomeRF больше, чем у Bluetooth. Правда, количество подключаемых устройств ограничено - 127. Радиус действия - до 50 метров. Поэтому Bluetooth должна обеспечить сервис и средства для серьезной конкуренции.

Безопасность Ajax-приложений

Князев А.Д., Стуров А.С.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
ank@ssau.ru

Safety of Ajax-appendices

Knyazev A.D., Sturov A.S.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
ank@ssau.ru

What is Ajax-application?

Owing to the technology of Ajax, the modern Web-application is head and shoulders above those applications not using the given technology. But in addition to new possibilities for user, the use of Ajax opens new types of attacks, earlier inaccessible. Therefore, the issue of safety of Web-application shall be given particular consideration.

Ajax is based on the technologies of Dynamic HTML (DHTML), which include:

- **JavaScript** – language of scenarios, used everywhere in Web-applications executable on the side of client.
- **Document Object Model (DOM)** – standard object model for representation of HTML- or XML-documents.
- **Cascading Style Sheets (CSS)** – language of style design, used for description of representation of HTML-documents.

In Ajax-application, JavaScript-code on the client side dynamically updates the appearance of a Web-page, while changing the objects' tree of DOM and table of styles. In addition, using the following technologies, one could update the data dynamically:

- **XMLHttpRequest** – this is API, enabling JavaScript-code on the side of client to connect via HTTP to remote servers and perform exchange of data, such as ordinary text, XML or JavaScript Serialized Object Notation (JSON).
- **JSON** – this is slimmed-down, language-independent format of data exchange. It defines a small set of rules for formatting, for the creation of transferable representation of structured data.

Ajax-applications operate according to the HTTP protocol.

HTTP protocol in Ajax-applications.

In Ajax-applications, the act of HTTP is used for both copying of client code, and for transmission of the client's queries to server. All methods of interaction which are mainly considered, — internal layers iFrame, HTML-forms and objects of XMLHttpRequest. Any Web-application, in that quantity and internal structure of Ajax, have a number of vulnerable locations, which could be used by trespassers, for example, an attack by means of interception of transmitted data at an intermediate node is called "a man in the middle". In order to seal up with putty the gap in protection of applications, one could use one of the following solutions:

- **HTTPS (Hypertext Transfer Protocol on the base of Secure Socket Layer)** The given protocol realises the envelope for HTTP. Coding of the data,

transmitted in both directions is performed by means of a pair of keys (open and closed). The "man in the middle" would still have access to the content of frames, however it is coded and it would be impossible to derive benefit from such information. In order that the HTTPS protocol could be used on the side of browser,

and on the side of server, a support of platform-oriented code would be required. Modern browsers contain built-in facilities for operation with HTTPS.

A number of arguments could be shown against the use of HTTPS. Firstly, a huge volume of computational resources would be required for encoding and decoding. On the server, additional loading is extremely undesirable. It is particularly important at large nodes. In classical Web-applications it is common practice to only transmit critically important data by means of HTTPS, whereas usual content, for example, images or descriptors are transmitted by means of HTTP protocol. Secondly, HTTPS only protects the process of data transmission itself, but it does not provide safety of the application as a whole. If one transmits the number of a charge card via protected channel, and then saves the number in a database, which protection system has drawbacks, the valuable information can well be stolen. Nevertheless, HTTPS is widely used for transfer of important data via network.

- **Algorithm of encoding**

Transmission of the most important data in encoded form, for example, with the use of one of the algorithms of encoding, suppose, the MD5. The algorithm of encoding transforms the input line into a sequence, in appearance resembling a chaotic set of symbols. The following scope of capabilities provided by this algorithm enables to use it for provision of safety. Firstly, as a result of transformation of the same fragment of data, the same results would be obtained. Secondly, the probability, that with transformation of two different fragments, the output data would be the same, is negligibly small. There is the third peculiarity. This consists in that there is no algorithm of inverse transformation. Therefore, MD5-digest can be transmitted via the network in an open form. In case if a trespasser intercepts this, he would not be able to restore initial form of the message.

Let us consider the main vulnerabilities of Ajax-applications.

Vulnerabilities Ajax-applications.

One of the problems consists in that the majority of Ajax-applications, while loading queries and responses use XML, and hence, the XML-traffic increases. In huge volumes, the Ajax-applications can stop data transmission in the network. Even more apprehensions are concerned with the fact that large volumes of traffic make Ajax-applications liable to vulnerabilities, typical for Web-applications. Should anybody make use of those vulnerabilities, the processing power of the systems and applications would be decreased. Let us consider four *examples of the vulnerabilities:*

- Exceeding of throughput
- Corrupted data
- Frequent small HTTP-queries
- Memory drain

1. **Exceeding of throughput.**

XML-messages in text format can increase by a factor of two, and higher, the volume of transmitted binary data. The higher is the throughput required for transmission of XML-messages, the lower is the amount of resources of the system, or application, for execution of other necessary tasks, for example, for execution of complicated algorithms. Exceeding of throughput can reduce the efficiency as a result of system overload.

2. **Corrupted data.**

Exceeding of throughput can result in generation, by the Ajax-applications, of corrupted data, because there would not be enough resources for creation of reliable data. It means that portals of Web-services, which composition includes Ajax-applications, can transmit corrupted data to other parts of the portal, as a result of which, poorly formed messages would appear. If such vulnerability is used by a trespasser, this could result in "falling" of the browser.

3. **Frequent small queries.**

One of the drawbacks of the Ajax consists in that it allows to perform many small queries instead of transmission of the whole page. Frequent small HTTP-queries can overload servers and firewalls, and this would result in exceeding of throughput, thus reducing the performance. Such queries may encounter limitations of the browser or slow network connection, and bottlenecks would appear in the network.

4. **Memory drain.**

Usually, in a Web-application, the Web-pages are frequently rebooted, and respectively, the memory of the same is deleted and filled anew. Using Ajax, it would be possible to avoid repeated loading of pages. Ajax allows to display a single-page application in the browser for a number of days, which gives rise to problems

associated with possible drain of memory or other resources. Large-scale drains of memory along with exceeding of throughput and small HTTP-queries can result in corrupted data of the Web-portal and increase the chance of success for hackers, who could make use of the system vulnerabilities through the Internet.

Special attention should be paid to *XSS vulnerabilities of* Ajax-applications.

Inter-site scenarios (XSS).

XSS – is a typical attack in which trespasser introduces a harmful code into a usual normal site. Two basic XSS-attacks include:

- *Reflected XSS*
- *Stored XSS*

Attack with reflected XSS uses vulnerable Web-applications, displaying input parameters back into the browser, without checking them for presence of active content. Usually a cracker seduces victims for passage via URL, using the following code:

http://trusted.com/search?keyword=<script>document.images[0].src="
http://evil.com/steal?cookie="+document.cookie;</script>

Let's assume that a function of search is located at trasted.com, which returns the results of search along with the entered key words. If the searching application does not filter special symbols in the URL [for example, the symbols less than (<) and more than (>)], the content of tag <script> would also be inserted in the user's Web-page, and as the result we would transmit cookies of the document to a remote server evil.com.

Stored XSS-attack becomes more important because of wide propagation of Web 2.0. The basis of Web 2.0 is combined access, interaction and combined operation, therefore potential trespassers have more chances to see the information entered by other users (by means of social network services – SNS), wiki or blogs.

Several typical attacks with the use of this vulnerability:

- **Theft of cookies or passwords.** Most direct profit for a trespasser is obtaining of important user information, such as passwords or cookies. Since the introduced scenarios can address any part of the tree of objects of DOM, they are in position, in addition, to steal passwords from text fields of registration forms.
- **Theft of the events of keyboard with the help of keyboard logger.** This allows a cracker to steal any data entered by a user; for example, if the user uses the service of Web-mail, the keyboard logger will read and transmit all the entered text to the cracker. He could then analyse the recorded data to extract confidential information (for example, passwords and confidential correspondence).
- **Theft of the events of keyboard with the help of mouse events sniffer.** Programmed keyboards become typical technical method for protection of important entered information against attacks with the help of keyboard logger, for example, PIN-code for interactive bank services. However, the mouse events sniffers can use technologies, similar to keyboard loggers. By stealing the coordinates X and Y of mouse events, one may determine, which keys were depressed.
- **Insertion of incorrect information.** Using DOM-interface, the cracker can change any information in the objects' tree of DOM. For example, while the user performs interactive money transfer, there is a possibility to change the number of account of the destination of payment, to the number of the cracker. As a result, the transferred money would be received at the account of the trespasser.

Recommended actions for protection against XSS.

Let us consider some techniques which could be used for improvement of immunity of the Ajax-applications.

1. **Addition of verification of the entered values.**

The majority of attacks, while implementing the various scenarios, use vulnerability on the server side. Hence, the verification for correctness of the entered information has been the first step for protection of Web-applications. Verification of entry and clearance screen all active or harmful content of insecure data.

Two types of verification of the entered data:

- **Blacklisting** (maintaining of black list): Under such an approach, all symbols listed in the black list would be screened out from the entered data. The most problematic in this approach is guaranteeing of availability of all harmful symbols in the black list. Since it is impossible to stipulate for all possible combinations of data, maintaining of black list frequently would not perform a correct verification.

- **Whitelisting** (maintaining of white list): In this alternative approach, all allowable symbols are listed, and all other symbols would be deleted from the entered data. The problem of such approach consists in how to achieve minimal length of the list, while ensuring at the same time, adequate flexibility for entering the data required for the Web-application.

Maintaining of black or white list shall not be considered as a reliable solution. However, maintaining of white list is deemed to be a more reliably protected variant. Hence, it is recommended to maintain white list for cleaning off potentially harmful data.

2. **Use of toolkit for verification of vulnerability.**

Many Web-applications are vulnerable because of similar errors of programming. Experts in protection have developed toolkit for detection of those unsafe methods of programming. Such means, called the means for verification of vulnerability, detect the possible vulnerabilities in advance. One of the most typical vulnerabilities detected by these toolkits is a situation, when programmers forget to call the procedure of clearing off potentially harmful entered data.

3. **Disuse of dynamic execution of code.**

In the JavaScript-programme, one may use several methods of dynamic generation of code. One of the most well-known functions is the function of eval(), which enables to execute arbitrary line as JavaScript-code. However, careless application of that function is very dangerous. Unfortunately, several widely used JavaScript-libraries internally use the function of eval().

4. **Safe use of JSON.**

Since JSON is based of the subset of JavaScript, it has been the content of scenario, which potentially can contain a harmful code. However, JSON – is a safe subset of JavaScript, in which assignments and activation are eliminated. Hence, many of the JavaScript-libraries use the function of eval() simply for transformation of JSON into JavaScript-object. Using this situation, crackers transmit invalid JSON-objects to these libraries for execution by the eval() function of its harmful code. For safe use of JSON, one could use a number of approaches. The first one of these is the use of regular expressions defined in RFC 4627, to guarantee absence of active fragments in JSON-data.

5. **Use of <iframe> while integrating suspicious content.**

One can use the policy of uniformity of origin to impede obtaining of access by the trespassers, to the entire tree of objects of DOM. When loading data from the various domains into <iframe>, it would be necessary to render to the data the own context of execution of JavaScript and the objects tree of DOM. This would prevent stealing by a cracker, of the information from the main page. It is a good practice to use <iframe>, as frequently as possible, for constraint of unreliable external content.

Что такое Ajax-приложение?

Благодаря технологии Ajax, современное Web-приложение стоит на голову выше приложений, не использующих данную технологию. Но помимо новых возможностей для пользователя, использование Ajax открывает и новые типы атак, недоступные ранее. Поэтому вопросу безопасности Web-приложения следует уделять особое внимание.

Ajax основан на технологиях Dynamic HTML (DHTML), которые включают в себя:

- **JavaScript** - язык сценариев, повсеместно используемый в выполняющихся на стороне клиента Web-приложениях.
- **Document Object Model (DOM)** - стандартная объектная модель для представления HTML- или XML-документов.
- **Cascading Style Sheets (CSS)** - язык стилевого оформления, используемый для описания представления HTML-документов.

В Ajax-приложении JavaScript-код на стороне клиента динамически обновляет вид Web-страницы, изменяя дерево объектов DOM и таблицу стилей. Помимо того, применяя следующие технологии, можно обновлять данные динамически:

- **XMLHttpRequest** - это API, позволяющий JavaScript-коду на стороне клиента подключаться по HTTP к удаленным серверам и обмениваться данными, такими как обычный текст, XML или JavaScript Serialized Object Notation (JSON).

- **JSON** - это облегченный, независимый от языка формат обмена данными. Он определяет небольшой набор правил форматирования для создания переносимого представления структурированных данных.

Ajax-приложения работают по протоколу HTTP.

HTTP протокол в Ajax-приложениях.

В Ajax-приложениях акт HTTP применяется как для копирования клиентского кода, так и для передачи запросов клиента серверу. Все способы взаимодействия, которые в основном рассматриваются, — внутренние слои iFrame, HTML-формы и объекты XMLHttpRequest. Любое Web-приложение, в том количестве и внутренняя структура Ajax, имеет ряд уязвимых мест, которыми могут воспользоваться злоумышленники, к примеру, атака путем перехвата передаваемых данных на промежуточном узле называется «человек посередине». Для того чтобы замазать брешь в защите приложений, можно использовать одно из следующих решений:

- **HTTPS (Hypertext Transfer Protocol на базе Secure Socket Layer)** Данный протокол реализует оболочку для HTTP. Кодирование данных,

передаваемых в обоих направлениях, осуществляется посредством пары ключей (открытого и закрытого). "Человеку посередине" по-прежнему доступно содержимое пакетов, но оно закодировано, и извлечь выгоду из данной информации невозможно. Для того чтобы протокол HTTPS можно было применить на стороне браузера и на стороне сервера, необходима поддержка платформенно-ориентированного кода. Современные браузеры содержат встроенные средства для работы с HTTPS.

Против использования HTTPS можно выдвинуть ряд аргументов. Во-первых, для кодирования и декодирования требуется большой объем вычислительных ресурсов. На сервере дополнительная нагрузка крайне нежелательна. В особенности это важно на больших узлах. В классических Web-приложениях принято передавать посредством HTTPS только критичные данные, а обычное содержимое, например изображения или дескрипторы, пересылается посредством протокола HTTP. Во-вторых, HTTPS защищает только сам процесс передачи данных, но не обеспечивает безопасность приложения в целом. Если передать по защищенному каналу номер платежной карточки, а затем поместить его в базу данных, в системе защиты которой имеются недостатки, ценная информация вполне может быть похищена. Тем не менее, HTTPS широко используется для передачи важных данных по сети.

- **Алгоритм шифрования**

Передача наиболее важных данных в закодированном виде, к примеру с использованием одного из алгоритмов шифрования, допустим MD5. Алгоритм шифрования преобразует входную строку в последовательность, с виду напоминающую беспорядочный набор знаков. Следующий ряд возможностей, обеспечиваемых данным алгоритмом, позволяет использовать его для обеспечения безопасности. Во-первых, в результате преобразования одного и того же фрагмента данных каждый раз будут получены одинаковые результаты. Во-вторых, вероятность того, что при преобразовании двух разных фрагментов будут получены одинаковые выходные данные, ничтожно мала. Есть и третья особенность. Она состоит в том, что алгоритма обратного преобразования не существует. Поэтому MD5-дайджест может передаваться по сети в открытом виде. В случае, если злоумышленник и перехватит его, он не сможет восстановить исходное сообщение.

Рассмотрим основные уязвимости Ajax-приложений.

Уязвимости Ajax-приложений.

Одна из проблем состоит в том, что в большинстве Ajax-приложений при загрузке запросов и ответов используется XML, следовательно, увеличивается объем XML-трафика. В больших объемах Ajax-приложения могут застопорить передачу данных в сети. Еще больше опасений вызывает то, что большие объемы трафика делают Ajax-приложения подверженными уязвимостям, типичным для Web-приложений. Если кто-либо воспользуется этими уязвимостями, производительность систем и приложений снизится. Рассмотрим четыре *примерауязвгтостей:*

- Превышение пропускной способности
- Испорченные данные
- Частые небольшие HTTP-запросы
- Утечки памяти

1. **Превышение пропускной способности.**

XML-сообщения в текстовом формате могут в два и более раз увеличить объём передаваемых двоичных данных. Чем большая пропускная способность требуется для передачи XML-сообщений, тем меньше ресурсов останется у системы или у приложения для выполнения других необходимых задач, например, для выполнения сложных алгоритмов. Превышение пропускной способности может снизить производительность в результате перегрузки системы.

2. **Испорченные данные.**

Превышение пропускной способности может привести к генерации Ajax-приложениями испорченных данных, потому что для создания достоверных данных будет недостаточно ресурсов. Это означает, что порталы Web-сервисов, в состав которых входят Ajax-приложения, могут передавать испорченные данные в другие части портала, в результате чего появятся плохо сформированные сообщения. Если этой уязвимостью воспользуется злоумышленник, это может привести к "падению" браузера.

3. **Частые небольшие запросы.**

Один из недостатков Ajax состоит в том, что он разрешает выполнять много небольших запросов вместо посылки страницы целиком. Частые небольшие HTTP-запросы могут перегружать серверы и брандмауэры, а это приведет к превышению пропускной способности, что снизит производительность. Такие запросы могут столкнуться с ограничениями браузера или медленным сетевым соединением, и в сети появятся узкие места.

4. **Утечки памяти.**

Обычно в Web-приложении Web-страницы часто перезагружаются, и, соответственно, память о них стирается и заполняется заново. При помощи Ajax можно избежать повторной загрузки страниц. Ajax позволяет отображать одностраничное приложение в браузере несколько дней, что увеличивает проблемы, связанные с возможной утечкой памяти или других ресурсов. Крупные утечки памяти, наряду с превышением пропускной способности и небольшими HTTP-запросами, могут привести к порче данных Web-портала и увеличить шансы на успех хакеров, которые могут воспользоваться уязвимостями системы через Интернет.

Особое внимание следует уделить *XSSуязвимости* Ajax-приложений.

Межсайтовые сценарии (XSS).

XSS - это типичная атака, в которой злоумышленник внедряет вредоносный код в обычный нормальный сайт. Двумя основными XSS-атаками являются:

- *Reflected XSS* (Отраженный XSS)
- *Stored XSS* (Сохраненный XSS)

Атака с отраженным XSS использует уязвимые Web-приложения, отображающие входные параметры обратно в браузер, не проверяя их на наличие активного содержимого. Обычно взломщик завлекает жертвы для перехода по URL, используя следующий код:

http://trusted.com/search?keyword=<script>document.images[0].src="
http://evil.com/steal?cookie="+document.cookie;</script>

Предположим, что на trasted.com размещена функция поиска, которая возвращает результаты поиска вместе с введенными ключевыми словами. Если поисковое приложение не фильтрует в URL специальные символы [например, символы меньше чем (<) и больше чем (>)], содержимое тега <script> будет также вставляться в Web-страницу пользователя, и в результате мы будем передавать куки документа удаленному серверу evil.com.

Сохраненная XSS-атака становится более важной в связи с широким распространением Web 2.0. Основой Web 2.0 является совместный доступ, взаимодействие и совместная работа, поэтому у потенциальных злоумышленников есть больше шансов увидеть вводимую другими пользователями (посредством публичных сетевых сервисов (social network services - SNS), wiki или блогов) информацию.

Некоторые типичные атаки с использованием данной уязвимости:

- **Кража куки или паролей.** Самой прямой выгодой для злоумышленника является получения важной пользовательской информации, такой как пароли или куки. Поскольку внедренные сценарии могут обращаться к любой части дерева объектов DOM, они в состоянии, помимо прочего, похищать пароли из текстовых полей форм регистрации.

- **Похищение событий клавиатуры с помощью клавиатурного регистратора.** Это позволяет взломщику похитить любые данные, введенные пользователем; например, если пользователь использует сервис Web-почты, клавиатурный регистратор будет записывать и передавать весь введенный текст взломщику. Он может затем проанализировать записанные данные для извлечения конфиденциальной информации (например, пароли и конфиденциальную переписку).
- **Похищение событий клавиатуры с помощью перехватчика событий мышки.** Программные клавиатуры становятся типичным техническим приемом для защиты важной вводимой информации от атак с использованием клавиатурного регистратора, например, PIN-кода для интерактивных банковских сервисов. Однако перехватчики (sniffers) событий мышки могут использовать технологии, аналогичные клавиатурным регистраторам. Похищая координаты X и Y событий мышки, можно определить, какие клавиши были нажаты.
- **Вставка неправильной информации.** Используя DOM-интерфейс, взломщик может изменить любую информацию в дереве объектов DOM. Например, при выполнении пользователем интерактивного перевода денег существует возможность изменить номер счета назначения платежа на принадлежащий взломщику. В результате переведенные деньги поступят на счет злоумышленника.

Рекомендуемые действия по защите от XSS.

Рассмотрим некоторые технические приемы, которые можно применить для улучшения защищенности Ajax-приложений.

1. **Добавление проверки вводимых значений.**

Большинство атак, внедряя вредные сценарии, использует уязвимости на стороне сервера. Следовательно, проверка на корректность вводимой информации является первым шагом для защиты Web-приложений. Проверка ввода и очистка отсеивают все активное или вредное содержимое ненадежных данных.

Два типа проверки введенных данных:

- **Blacklisting** (ведение черного списка): В этом подходе из введенных данных отфильтровываются все символы, перечисленные в черном списке. Самым проблематичным в данном подходе является гарантирование наличия в черном списке всех опасных символов. Поскольку невозможно предусмотреть всевозможные комбинации данных, ведение черного списка часто не выполняет проверку корректно.
- **Whitelisting** (ведение белого списка): В этом альтернативном подходе перечисляются все разрешенные символы и из вводимых данных удаляются все остальные. Проблема данного подхода состоит в том, как добиться минимальной длины списка, обеспечив в то же время достаточную гибкость для ввода необходимых Web-приложению данных.

Нельзя считать ведение черного или белого списков надежным решением. Однако ведение белого списка обычно считается более защищенным вариантом. Следовательно, рекомендуется использовать ведение белого списка для очистки потенциально опасных данных.

2. **Использование инструментальных средств проверки уязвимости**

Многие Web-приложения уязвимы из-за похожих ошибок программирования. Эксперты по защите разработали инструментальные средства для обнаружения этих небезопасных приемов программирования. Такие средства, называемые средствами проверки уязвимости, обнаруживают возможные уязвимости заблаговременно. Одной из наиболее типичных уязвимостей, обнаруживаемых этими инструментальными средствами, является ситуация, когда программисты забывают вызвать процедуру очистки потенциально опасных введенных данных.

3. **Неиспользование динамического выполнения кода.**

В JavaScript-программе можно использовать несколько способов динамического генерирования кода. Одной из самых известных функций является функция eval(), которая позволяет выполнять произвольную строку как JavaScript-код. Однако неосторожное применение этой функции очень опасно. К сожалению, некоторые широко распространенные JavaScript-библиотеки внутренне используют функцию eval().

4. **Безопасное использование JSON**

Поскольку JSON основан на подмножестве JavaScript, он является содержимым сценария, который потенциально может содержать опасный код. Однако JSON - это безопасное подмножество JavaScript, в котором исключены присвоения и активизация. Следовательно, многие JavaScript-библиотеки используют функцию eval() просто для преобразования JSON в JavaScript-объект. Используя данную ситуацию, взломщики передают в эти библиотеки искаженные JSON-объекты для выполнения функцией eval() своего опасного кода. Для безопасного использования JSON можно применить несколько подходов. Первым из них является применение регулярных выражений, определенных в RFC 4627, чтобы гарантировать отсутствие в JSON-данных активных фрагментов.

5. Использование <iframe> при интеграции подозрительного содержимого.

Можно воспользоваться политикой единства происхождения для затруднения получения злоумышленниками доступа ко всему дереву объектов DOM. При загрузке данных из различных доменов в <iframe> надо предоставить этим данным свой собственный контекст выполнения JavaScript и дерево объектов DOM. Это предотвратит похищение взломщиком информации с главной страницы. Хорошей практикой является как можно более частое использование <iframe> для ограничения ненадежного внешнего содержимого.

Ограничение привилегий неуправляемого кода в .NET Framework

Семенова Н.А.

Московский государственный институт Электроники и Математики
г. Москва, Россия
natasha_sem@inbox.ru

Enabling security restrictions for unmanaged code in .NET Framework

Semenova N.A.

Moscow State Institute of Electronics and Mathematics
Moscow, Russia
natasha_sem@inbox.ru

One of the most important security features of Microsoft .NET Framework is that it allows access to native libraries, because the execution of unmanaged native code is not restricted by the .NET security model. At the same time, it is impossible to completely exclude native code calls from .NET programs as this will lead to losing backward compatibility and legacy code support, in particular with Windows API, which contains thousands of routines that provide access to most aspects of the Windows operating system. This paper presents several methods for enabling security restrictions on native code execution, which provides a way to extend .NET security model to unmanaged code.

Одной из самых критичных, с точки зрения безопасности кода, особенностей .NET Framework является возможность обращения к коду из native-библиотек, так как на код, выполняющийся в результате таких вызовов, не распространяются ограничения безопасности модели .NET. В то же время, невозможно полностью отказаться от вызова native-кода, так как это приведет к потере совместимости со многими ранее написанными программами и библиотеками, в частности, с Windows API. В данной статье описано несколько способов введения ограничений на выполнение native-кода, позволяющих распространить на него контроль безопасности .NET.

Несколько лет назад компания Microsoft представила систему .NET Framework, которая позиционировалась, как безопасная для пользователей среда. Концепция .NET Framework обладает гранулированной моделью безопасности, позволяющей контролировать уровень доступа программ, построенных на базе .NET. Весь код, выполняющийся внутри «виртуальной машины» .NET, называется управляемым (managed), так как на него действуют все ограничения безопасности, определяемые системой полномочий .NET.

Для решения проблемы обратной совместимости, в частности, при вызове функций Windows API, в .NET была добавлена возможность обращения к native-библиотекам. Функции, вызываемые из native-библиотек, выполняются вне модели безопасности .NET, поэтому они называются неуправляемым (unmanaged) кодом. Следовательно, использование этой функциональности в приложениях .NET может позволить злоумышленнику обойти механизм безопасности системы, и выполнить произвольный код. Несмотря на серьезную угрозу безопасности, невозможно полностью отказаться от вызова native-кода из .NET программ, так как для этого придется отказаться от поддержки множества ранее написанных программ и переписывать все существующие приложения.

Для обратной совместимости с кодом, написанным вне .NET (например, Windows API), CLI использует интерфейс, называемый службой обращения к платформе (Platform Invoke Service, P/Invoke). Этот сервис позволяет обращаться к коду из native-библиотек. Так как код в native-библиотеках может изменять параметры безопасности пользовательского окружения, то в .NET привилегия вызова native-кода эквивалентна полному доверию. Более того, native-код, запущенный P/Invoke, выполняется в том же процессе, что и .NET CIL, и, как следствие, вредоносный native-код может изменить состояние самой среды выполнения .NET. Безопасность выполнения .NET программ можно повысить, если

распространить проверки CAS на неуправляемый (native) код. Тогда неуправляемый код будет выполняться с теми же ограничениями, что и управляемый .NET код.

Дублировать полномочия CAS для контроля полномочий неуправляемого кода можно несколькими способами, каждый из которых имеет свои достоинства и недостатки:

1. Использование встроенной модели безопасности ОС Windows.

При реализации данной схемы ограничения прав CAS .NET дублируются на уровне процесса, в котором запущено приложение, включая все его native-компоненты. При этом для ограничения привилегий этого процесса будет применяться уже механизм контроля доступа уровня ОС, дублирующий настройки CAS .NET. Недостатки метода: Хотя модель безопасности в Windows и является достаточно широкой, она все же отличается от модели CAS. Т.е., полномочия безопасности в Windows отличаются от полномочий в .NET, и с их помощью нельзя получить тот же уровень детализации привилегий. Контроль доступа в Windows основан на учетных записях пользователей и ролях, в то время как CAS основан на доказательствах, предоставленных для идентификации кода. В модели безопасности Windows не существует концепции, аналогичной доказательствам. Например, в Windows, невозможно ограничить права процесса, основываясь на URL, с которого была загружена запущенная в процессе программа.

2. Использование выделенного слоя безопасности.

Использование выделенного слоя безопасности позволяет несколько сгладить различия между моделью безопасности Microsoft Windows и CAS, что позволяет контролировать неуправляемый код с ограничениями, введенными на уровне .NET CAS. Этот слой безопасности будет отслеживать действия, выполняемые неуправляемым кодом и гарантировать, что действия native-кода не будут превышать полномочий, заданных CAS.

При этом к реализации слоя безопасности предъявляются следующие требования:

a. Прозрачность для выполняющихся приложений.
b. Полный доступ ко всем функциям, которые вызываются приложением, чтобы иметь достаточно информации для принятия решений о соответствии или несоответствии выполнения этой функции заданной политике безопасности.
c. Вредоносный код не должен иметь возможности преодоления уровня безопасности.

Основной вопрос, который необходимо решить при построении выделенного слоя безопасности – его размещение. Ниже приведены результаты построения трех схем дублирования полномочий CAS расположения слоя безопасности: пространство пользователя, пространство ядра и смешанное (распределенное).

2.1. Использование выделенного слоя безопасности на пользовательском уровне (над Windows API)

Описание метода:

В случае размещения слоя безопасности над Windows API, его задача - перехват обращений к функциям Windows API, отвечающим за безопасность, и оценка параметров вызова функции. Перехват управления осуществляется за счет перезаписи нескольких первых инструкций целевой функции на безусловный переход к созданной функции-обработчику. Таким образом, при каждом обращении к функциям безопасности Windows API вызываются функции-перехватчики, которые осуществляют проверку входных параметров исходной функции и создают соответствующие им объекты полномочий .NET. Эти полномочия затем проверяются на непротиворечивость множеству полномочий, доступных приложению. Если запрашиваемое действие, представленное полномочием безопасности, не разрешено CAS, то генерируется исключительная ситуация (security exception). Прошедший все проверки запрос передается на уровень Windows API, и запрашиваемая операция выполняется, как обычно.

Достоинства метода:

a. Простота реализации (Windows API хорошо документирован)
b. Полномочия безопасности .NET можно легко сопоставить параметрам вызовов Windows API. Это дает возможность оценивать параметры вызовов Windows API, создавая и проверяя соответствующие объекты полномочий .NET. Например, можно оценить параметры вызова API CreateFile, создав соответствующий объект

полномочий .NET, представляющий имя файла и запрашиваемое действие (создать или открыть). Затем этот объект полномочий может быть проверен на соответствие доступным разрешениям CAS, и по результатам проверки запретить, либо разрешить запрос.

c. Прозрачность механизма проверки для приложений.

Недостатки метода:

a. Злоумышленник, имеющий право обращения к native-коду, имеет множество возможностей, чтобы обойти данный уровень безопасности. Например, это можно сделать, вызывая функции из ntdll.dll, которая преобразует пользовательские вызовы в системные вызовы уровня ядра, или выполняя системные вызовы непосредственно из ассемблированного кода.

Следовательно, чтобы удовлетворять условию «вредоносный код не должен иметь возможности преодоления уровня безопасности», новый слой безопасности должен не только контролировать обращения к native-коду, но и обеспечивать защиту среды runtime .NET и предотвращать несанкционированные операции параллельно выполняющихся процессов над выделенной им памятью.

2.2. Использование выделенного уровня безопасности на уровне ядра

Описание метода: функциональность данного метода аналогична предыдущему, за исключением того, что перехватываются не вызовы Windows API, а native API. При этом следует учитывать, что существуют вызовы Windows API, соответствующие сразу нескольким системным вызовам native API. В таких случаях, корректный вызов native API можно определить только по параметрам функции Windows API.

Достоинства метода:

Так пользовательские процессы не могут модифицировать объекты, находящиеся в пространстве ядра, то вредоносный native-код не может обойти уровень безопасности, реализованный как драйвер ядра. Следовательно, можно использовать драйвер, как доверенное хранилище критичных данных, например, доверенной копии полномочий CAS.

Недостатки:

1. Сложность практической реализации из-за отсутствия опубликованной документация для native API, который может изменяться даже при установке новых сервис-паков для Windows.

2.3. Совместное использование двух слоев безопасности (на уровне ядра и пользовательском уровне)

Описание метода: В данном случае, слой безопасности на уровне ядра ОС служит дополнительным механизмом защиты от обращений к системным вызовам ОС в обход Windows API (а, следовательно, в обход функций-перехватчиков, реализованных на уровне Windows API). Являясь дополнением к первому слою безопасности (на уровне API), второй слой (на уровне ядра) перехватывает и анализирует обращения к ОС. Его основная задача - гарантировать, что каждое обращение к системному вызову будет проходить через первый слой безопасности в Windows API (который функционирует, как описано в 2.1).

Взаимодействие между двумя слоями безопасности осуществляется с помощью механизма «авторизации» системных вызовов. Для этого функции в Windows API модифицируются таким образом, чтобы при любом обращении к Windows API, сначала выполняется функция-перехватчик, которая сначала «авторизует» соответствующий системный вызов, к которому происходит обращение, а затем осуществляет проверку параметров вызова. В случае неуспешной проверки, авторизация отзывается, иначе – происходит вызов исходной функции API. Для выполнения авторизации и отзыва системных вызовов используются сообщения IOCTL.

Когда вредоносный код пытается полностью обойти проверки на первом уровне безопасности и обращается к системным вызовам напрямую, то драйвер на уровне ядра определяет, что эти вызовы неавторизированны, и может отменить операцию. Двухшаговый процесс авторизации гарантирует отклонение системного вызова, в случае если злоумышленник будет обращаться к системным вызовам через Windows API, но сделает попытку обойти оценку параметров вызова пользовательской функцией-перехватчиком, совершив безусловный переход к инструкциям, разрешающим (авторизующим) системный вызов.

Достоинства метода:

1. Простота реализации
2. Защита от обхода злоумышленником
3. Наличие доверенного хранилища данных

Описанный выше способ можно распространить и на многопоточные приложения, если корректно обрабатывать «условие гонки» в двухшаговом процессе авторизации.

Злоумышленник может смоделировать ситуацию, сделав обращение к запрещенному системному вызову в одном потоке, одновременно обратившись к тому же вызову в другом потоке между временем, когда он был авторизован в первый раз, но еще не был отозван. Эта проблема решается разрешением и отзывом авторизации системных вызовов для каждого потока в отдельности. Т.е., каждый раз, когда к драйверу ядра обращаются за авторизацией или отзывом полномочий на системный вызов, он проверяет идентификатор текущего потока вместо идентификатора процесса.

Таким образом, система безопасности, описанная в пункте 2.3, не содержит недостатков двух предыдущих систем, объединяя при этом их достоинства. Как показали испытания разработанных прототипов системы, ее внедрение на тестовом компьютере (ОС Windows XP SP 2, Intel Pentium 4 - 1.4 ГГц, 1 Гб) не приводит к значительным потерям производительности при выполнении .NET программ.

3 Секция

Криптография. Её актуальность в современном обществе

Cryptography and its relevance today

Симметричное и асимметричное шифрование

Гончаров Н.О.

Московский государственный технический университет им. Н.Э.Баумана
г. Москва, Россия
goncharovkolya@list.ru

Symmetric and asymmetric encryption

Goncharov N.O.

Bauman Moscow State Technical University
Moscow, Russia
goncharovkolya@list.ru

The purpose of project

Research of symmetric and asymmetric encryption which are urgent and cryptographically guaranteed methods of data security and also studying of methods of encryption and principles of operation. Software on realization of algorithms of symmetric and asymmetric encription is developed.

1. Theoretical part:

The purpose of work consists in research of symmetric and asymmetric encryption, which are topical and cryptographically guaranteed methods of information protection, and also examination of the methods of encryption and principles of operation. Software has been developed, for the realisation of algorithms of symmetric and asymmetric encryption. The work is continued, on the enhancement of the earlier developed software by the author, for realisation of the algorithm of encryption based on gamming, and the scheme of RSA (block diagrams and programmes in the language of object-oriented programming, Visual Basic-gammir2-version2 and RSA-demo, version 2). Further work on the project is planned.

2. Methods of carrying out the research:

For achievement of the goal of research, general scientific (theoretical and empirical) methods were used. Among the **theoretical** methods, the following were applied:

- analysis of the known data about methods of symmetric encryption (method of Shannon's classical encryption; block encoders – American encoder DES (Data Encryption Standard) and the

domestic standard GOST 28147-89, etc.); and methods of two-key cryptography (RSA cryptosystem);

- synthesis of the obtained data for obtaining of conception of the efficiency of the given methods;
- comparison of classical codes, methods of encryption with the help of symmetric and asymmetrical keys, revealing of the basic advantages and drawbacks, concrete definition of the general methods and schemes of symmetric encryption and asymmetric encryption, generalization of the obtained data.

Among **empirical** methods, the following were used: examination of symmetric encryption by the example of the works by Shannon et al., asymmetric encryption by the example of methods of two-key cryptography, research-experimental work on the development of software on realisation of algorithms of symmetric and asymmetric encryption, and enhancement of the earlier developed software on realisation of the algorithm of encryption, based on gamming and scheme of RSA (development of block diagrams and programs in Visual Basic language of object-oriented programming).

3. Literature:

1. А.В. Аграновский, Р.А. Хади. Практическая криптография (серия "Аспекты защиты"), М.: Солон-Пресс, 2002.
2. Т.Л. Партыка, И.И. Попов. Информационная безопасность. М.: Форум-Инфра-М, 2007.
3. Шеннон К., Теория связи в секретных системах, в кн.: Шеннон К. Э., Работы по теории информации и кибернетике, М.: ИЛ, 1963.
4. У.Диффи и М.Э.Хеллман. Новые направления в криптографии,1976 г
5. Брюс Шнайер.Прикладная криптография, 2е изд, изд.Триумф,2002г
6. О современной криптографии. В. М. Сидельников, д. ф.-м. н., профессор, академик Академии криптографии РФ, зав. Лабораторией МГУ по математическим проблемам криптографии. Опубликовано на сайте: Cryptography.Ru
7. Крис Сасаки. (перевод с англ. Ю.Суслов). Лучшие сверхсекретные шифры.М.: АСТ: Астрель, 2007.
8. С.В. Глушаков А.С.Сурядный. Программирование на Visual Basic 6.0 Х.: Фалио, 2004.
9. И.Сафонов. Visual Basic в задачах и примерах. С-П.: "БХВ", 2007.

4. Starting file: gammir1.exe (source code: gammir1.bas); gammir2.exe; and RSA-demo1.exe (source code-RSA-demo1.bas and RSA – key.bas); RSA-Demo2.exe; RSA-Demo3.exe

1.Теоретическая часть:

Цель работы - исследование симметричного и асимметричного шифрования, которые являются актуальными и криптографически гарантированными методами защиты информации, а также изучение методов шифрования и принципов работы. Разработано программное обеспечение по реализации алгоритмов симметричного и асимметричного шифрования. Продолжена работа по совершенствованию разработанного ранее автором программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании и схемы RSA (блок-схемы и программы на языке объектно-ориентированного программирования Visual Basic –gammir2-версия2 и RSA-demo,версия 2). Планируется дальнейшая работа над проектом.

2. Методы проведения исследования:

Для достижения цели исследования использовались общенаучные (теоретические и эмпирические) методы. Из **теоретических** методов применялись:

- анализ известных данных о методах симметричного шифрования (метод классического шифрования Шеннона; блочные шифраторы - американский шифратор DES (Data Encryption Standard) и отечественный стандарт ГОСТ 28147-89 и др.); и методов двухключевой криптографии (криптосистема RSA);
- синтез полученных данных для получения представлений об эффективности данных методов;
- сравнение классических шифров, методов шифрования с помощью симметричного и несимметричного ключей, выявление основных достоинств и недостатков, конкретизация

общих методов и схем симметричного шифрования и асимметричного шифрования, обобщение полученных данных.

Из **эмпирических** методов использовались: изучение симметричного шифрования на примере работ Шеннона и др, асимметричного шифрования на примере методов двухключевой криптографии, опытно-экспериментальная работа по разработке программного обеспечения по реализации алгоритмов симметричного и асимметричного шифрования и совершенствованию разработанного ранее программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании и схемы RSA (разработка блок-схем и программ на языке объектно-ориентированного программирования Visual Basic)

3. Литература:

10. А.В. Аграновский, Р.А. Хади. Практическая криптография (серия «Аспекты защиты»), М.: Солон-Пресс, 2002.
11. Т.Л. Партыка, И.И. Попов. Информационная безопасность. М.: Форум-Инфра-М, 2007.
12. Шеннон К., Теория связи в секретных системах, в кн.: Шеннон К. Э., Работы по теории информации и кибернетике, М.: ИЛ, 1963.
13. У.Диффи и М.Э.Хеллман. Новые направления в криптографии,1976 г
14. Брюс Шнайер.Прикладная криптография, 2е изд, изд.Триумф,2002г
15. О современной криптографии. В. М. Сидельников, д. ф.-м. н., профессор, академик Академии криптографии РФ, зав. Лабораторией МГУ по математическим проблемам криптографии. Опубликовано на сайте: Cryptography.Ru
16. Крис Сасаки.(перевод с англ.Ю.Суслов). Лучшие сверхсекретные шифры.М.: АСТ: Астрель, 2007.
17. С.В. Глушаков А.С.Сурядный. Программирование на Visual Basic 6.0 Х.: Фалио, 2004.
18. И.Сафонов. Visual Basic в задачах и примерах. С-П.: «БХВ», 2007.

4. Стартовый файл: gammir1.exe (исходный код : gammir1.bas) ; gammir2.exe; и RSA-demo1.exe (исходный код- RSA-demo1.bas и RSA--key.bas) ; RSA-Demo2.exe; RSA-Demo3.exe

Криптография. Ее актуальность в современном обществе

Егоров Г.В.

Московская финансово-промышленная академия
г. Москва, Россия
GEgorov@scarybox.ru

Cryptography and its relevance today

Egorov G.V.

Moscow University of Industry and Finance
Moscow, Russia
GEgorov@scarybox.ru

This work consists in the analysis existing crypto algorithms and revealing of the most widespread mistakes of their realization. And also spheres of application cryptography in a modern community.

В настоящее время информация становится одним из наиболее важных и ценных продуктов, создаваемым человеком. Именно поэтому большое значение придается ее защите от несанкционированного получения и использования.

Целью работы является определение дальнейших направлений развития криптографии и сфер ее применения. Для этого предстоит решить ряд задач, а именно изучение криптоалгоритмов и выявление основных уязвимостей в их реализации.

Исследование и анализ существующих алгоритмов, является одним из необходимых условий разработки безопасных систем. Перспективным направлением исследований в этой области является анализ успешно осуществленных атак или выявленных уязвимостей в криптосистемах с целью их классификации и выявления причин их появления и существования.

Опираясь на проведенные исследования и выявленные уязвимости можно разработать более стойкий криптоалгоритм, осуществляющий надежную защиту данных.

Кодирование информации на мобильных устройствах

Ершов Д.И.

Новосибирский государственный архитектурно-строительный университет
г. Новосибирск, Россия
d_ershov@ngs.ru

The coding of information on mobile devices

Ershov D.I.

Novosibirsk state architectural - building university
Novosibirsk, Russia
d_ershov@ngs.ru

Now there are a plenty various cryptographic algorithms [1, 2]. However high computing requirements to devices, for example small volume of memory, low frequency of the processor, bad loyalty to the multitask applications [3], determining the factor in choice of cryptographic algorithms. Thus, the simplification of computing realization of algorithms of coding of the information on mobile devices becomes here task, which on the complexity is commensurable with a problem of increase decoding-resistance of these algorithms.

The purpose of the submitted work is the development easy circuit of coding of the information for realization on the mobile device. For a basis was taken private key encryption. Important to understand, that the given circuit intended for coding the information stored on the mobile device, therefore at construction of the appropriate algorithms the emphasis is done on as it is possible more essential dependence output data from a key and initial message; however it does not mean, that it is necessary to create complex and hardly-computable functions.

For program realization I chose language Java, as most suitable for a fast spelling of the effective application, including applications working with the isolated memory.

As a result of the carried out researches was received variant of the circuit of coding of the information on the mobile device and created the simple algorithm realizing the similar circuit. The work of the application realizing the given algorithm is illustrated. Thus it is necessary to note, that the enciphering of the textual information is only one of examples of application of the described circuit of coding - it is possible as successfully to develop the application for enciphering the files which have been in file system of the mobile devices.

References

1. Gorbatov V.A., Gorbatov A.V, Gorbatova M.V. The discrete mathematics. M.: AST Astrel, 2006 (in Russia).
2. Novikov F.A. The discrete mathematics for the programmers. SPb: Piter, 2002 (in Russia).
3. Gornakov S.G. The programming of the mobile phones on Java 2 Micro Edition. M.: DMK Press, 2004 (in Russia).

В настоящее время существует большое количество разнообразных криптографических алгоритмов [1, 2], однако высокие вычислительные требования к устройствам – малый объём памяти, низкая частота процессора, малая лояльность к многозадачным приложениям [3] – зачастую являются определяющими фактором в выборе того или иного криптографического алгоритма для реализации его на мобильных платформах. Таким образом, упрощение вычислительной реализации алгоритмов кодирования информации на мобильных устройствах становится здесь задачей, которая по своей сложности соизмерима с проблемой повышения криптостойкости этих алгоритмов.

Целью представленной работы является разработка простой для реализации на мобильном устройстве схемы кодирования информации. За основу взята схема кодирования с закрытым ключом. Важно понимать, что данная схема предназначена именно для кодирования информации, хранящейся на устройстве, поэтому при построении соответствующих алгоритмов упор делается на как можно более существенную зависимость выходных данных от ключа и исходного сообщения; однако это ещё не означает, что нужно создавать сложные и трудновычислимые функции.

Для программной реализации мною был выбран язык Java, как наиболее подходящий для быстрого написания эффективных приложений, в том числе и приложений работающих с изолированной памятью.

В результате проведенных исследований был получен вариант схемы кодирования информации на мобильном устройстве и построен простой алгоритм, реализующий подобную схему. Проиллюстрирована работа приложения, реализующего данный алгоритм. При этом нужно отметить, что шифрование текстовой информации является лишь одним из примеров применения описанной схемы кодирования – можно так же успешно разработать приложение для шифрования файлов, записанных на мобильном устройстве.

Литература

1. Горбатов В.А., Горбатов А.В, Горбатова М.В. Дискретная математика. М.: АСТ Астрель, 2006.
2. Новиков Ф.А. Дискретная математика для программистов. СПб: Питер, 2002.
3. Горнаков С.Г. Программирование мобильных телефонов на Java 2 Micro Edition. М.: ДМК Пресс, 2004.

Алгоритм шифрования ГОСТ 28147-89

Крайнов Н.А.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
ank@ssau.ru

Algorithm of enciphering GOST 28147-89

Krainov N.A.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
ank@ssau.ru

То, что информация имеет ценность, люди осознали очень давно. Несколько десятилетий назад информация приобрела самостоятельную коммерческую ценность и стала широко распространенным, почти обычным товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит - воруют и подделывают - и, следовательно, ее необходимо защищать. Современное общество все в большей степени становится информационно-обусловленным, успех любого вида деятельности все сильней зависит от обладания определенными сведениями и от отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации с железной необходимостью привело к возникновению индустрии средств защиты информации.

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения. Образно говоря, криптографические методы строят барьер между защищаемой информацией и реальным или потенциальным злоумышленником из самой информации. Конечно, под криптографической защитой в первую очередь - так уж сложилось исторически - подразумевается шифрование данных. Раньше, когда эта операция выполнялось человеком вручную или с использованием различных приспособлений, и при посольствах содержались многолюдные отделы шифровальщиков, развитие криптографии сдерживалось проблемой реализации шифров, ведь придумать можно было все что угодно, но как это реализовать...

Почему же проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна? С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц. С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми

Разработка нового подхода к оценке эффективности криптографической защиты информации

Савельева А.А.

Государственный Университет – Высшая Школа Экономики
г. Москва, Россия
asavelieva@hse.ru

A new Approach to the problem of evaluating the efficiency of cryptographic systems

Savelieva A.A.

State University – Higher School of Economics
Moscow, Russia
asavelieva@hse.ru

We introduce a complex approach to evaluating cryptographic protection efficiency. Classically, the research has mostly focused on information system security as a whole, whereas cryptographic tools evaluation techniques have not received as much attention. The main thread of our work is the development of mathematical models of threats to analyze the security of cryptographic systems based on various types of attacks that the cryptographic system is exposed to. The second main thread is the development of software tools to facilitate the process of cryptosystem efficiency assessment by computer security specialists. The new approach allows to build an economic rationale for investments to cryptographic systems and to provide sound arguments for implementing an information security strategy.

Introduction

Bruce Schneier, a well-known cryptographer, declares in [15] that the term "security" does not have meaning unless you can answer such questions as "Secure from whom?" or "Secure for how long?". This statement applies to security systems in general as well as to their essential component – cryptographic systems. Furthermore, Ross Anderson, Professor in Security Engineering at the University of Cambridge Computer Laboratory and an industry consultant, concludes his well-known paper [1] stating that “the evaluator should not restrict herself to technical tools like cryptanalysis and information flow, but also apply economic tools”. Our paper aims at providing a formal way of analyzing cryptographic systems security.

The analysis of modern publications on security revealed a lack of methods designed to support the process of cryptographic protection efficiency. Formalized security risk analysis and management methodologies such as CRAMM [6], RiskWatch [13] and GRIF [7] are focused on information system security as a whole and do not consider the peculiarities of evaluating cryptographic systems. A mathematical model designed by V.P. Ivanov [8] applies the principles of the catastrophe theory and queuing theory to computing the indicators of a cryptographic system efficiency. Although the approach incorporates economic and technical perspective, its major restriction is that it can only apply to the so-called restricted use cryptographic systems [4] whose security depends on keeping both the encryption and decryption algorithms secret. The author reduces the problem of breaking a cipher to engineering analysis of the program that implements the encryption mechanism. This assumption is inadmissible for modern cryptographic systems because it contradicts Kerckhoffs’s fundamental principle [9] that encryption should not depend on the secrecy of the system - which sooner or later would be compromised - but should solely depend on the secrecy of the key. Finally, various tools for cryptographic protocols analysis [Bodei2003, Boreale2002, 5] focus only on the high-level, conceptual design of a protocol postulating that cryptographic algorithms satisfy perfect encryption assumptions, while the interaction between cryptosystems and cryptographic protocols still remains an open area of research.

Problem Statement

The purpose of our work is to develop an approach to analyzing the security of cryptographic systems based on various types of attacks that the cryptographic system is exposed to. In order to achieve the goal, we need to:

- formulate the steps of cryptographic systems evaluation process;
- design a mathematical model of security threats;
- develop software tools to facilitate the process of cryptosystem efficiency assessment by a computer security specialist;
- select appropriate economic indicators as a basis to build an economic rationale for investments to cryptographic systems and to provide sound arguments for implementing an information security strategy.

Cryptographic Systems Evaluation Process

The process of cryptosystem efficiency assessment can be described as a sequence of steps, each of them directed at answering a specific question:

- Step 1: What cryptosystem is the object of attack?
- Step 2: Who wants to attack the cryptosystem?
- Step 3: Which attack techniques are most likely to be used to break the cryptosystem?
- Step 4: Is the cryptosystem capable of withstanding such attacks?
- Step 5: Does the cryptosystem provide sufficient security in the given context?

The environment typically imposes restrictions on the attack scenarios that the cryptographic systems are exposed to, so Steps 1 to 3 imply modeling threats to a cryptographic system in a given context. Step 4 is about analyzing the cryptographic system resistance to the types of attacks defined at Steps 1 - 3. Finally, Step 5 involves using various risk analysis techniques and economic tools to evaluate the data obtained during Steps 1-4.

ABC-Model of Security Threats

We can assume that the adversary is most likely to choose the attack with the maximum benefit for a given cost, or choose the least costly attack that gives them a particular benefit [14]. Each cryptosystem has a set of attacks that is applicable to it and a set of attacks that is not. These statements perfectly fit into common risk-management methodologies and result in the following approach to evaluating security threats.

Each crypto attack has a value of risk assigned to it defined as the product of probability of the hazard and its potential impact:

$$Risk = Probability \cdot Impact$$

Impact refers to effect of an attack on a specific type of cryptographic system. Probability reflects the likelihood that an adversary will consider a specific type of attack appropriate in terms of available resources and target secret data. Thus, a formal model of the cryptosystem coupled with formal models of the adversaries will yield a set of the most hazardous attacks that the cryptosystem is exposed to. The model of security threats represented as a composition of 3 elements will be referred to as an *ABC-model* ('A' for **a**ttack, 'B' for code**b**reaker and 'C' for **c**ryptosystem). The following subsections describe the multiple-category divisions of cryptographic systems, adversaries and attacks we suggest using as a basis for modeling the components of a security threats.

Classification of Cryptosystems

There are various classification schemes of cryptosystems available in modern literature. For example, Ueli Maurer's idea is to distinguish cryptosystems by the number of keys used for data processing, i.e. unkeyed, single-keyed, and double-keyed cryptosystems [12]. Gilles Brassard's scheme [4] has to do with the secrecy of algorithm. However, neither of these classifications reflects all the properties necessary to identify a cryptosystem in practice. We propose a multiple-category classification scheme that includes the criteria mentioned above along with several new criteria:

- By secrecy of the algorithm
- By the number of keys
- By breakability
- By the means of implementation
- By certification
- By key medium

Classification of Code-Breakers

Types of attackers that you are defending against define the sensible type of security. Predicting most likely attackers and understanding them gives a clue to how they might attack the assets protected by the cryptosystem [14]. There is obviously an *m : n* relationship between the types of attackers and the types of attacks, i.e. a single attacker can undertake many different attacks, and a single type of attack can usually be launched by a number of different attackers. Being excellent for high-level analysis, Schneier's classification

[14] using motivation as a key parameter to identifying an adversary provides no clear mapping between the type of attacker and the attacks they can use. We designed a new scheme to give a more precise definition to the types of adversaries in terms of different model parameters:

- By equipment
- By final objective
- By access
- By expertise
- By initial knowledge on the cryptosystem
- By manpower

Classification of Attacks

The fundamental classification of attacks by access to plaintext and ciphertext introduced by Kerckhoffs [9] is no longer complete since it does not include a new powerful cryptanalysis technique called *Side-Channel attacks* [16]. We categorize the attacks as follows (the rationale of criteria choice is described in a survey of modern techniques of cryptanalysis [2]):

- By access to plaintext and ciphertext
- By control over the enciphering/deciphering process
- By the outcome
- By critical amount of resources
- By applicability to various ciphers
- By tools and techniques
- By consequences
- By parallelizing feasibility
- By level of automation

Software Tools for Cryptanalysis

The statistics on breaking cryptosystems are not always available and quickly become out-of-date with the advent of new attack techniques and computation power growth. Therefore, computer security specialists need a set of tools to support evaluation of cryptographic system capability to resist various types of attacks. The software tools CRYPTO [3] are designed as a means for conducting cryptanalysis of public-key cryptosystems. CRYPTO consist of two components: a dynamic-link library DESIGNER, and an application ANALYST. ANALYST provides a friendly graphical user interface to access functions of DESIGNER. DESIGNER is a high-performance, portable C++ library providing the necessary elements to design and evaluate modern techniques for cryptanalysis of ciphers based on factorization and discrete logarithm problems. The implementation makes use of NTL (a Library for doing Number Theory) written and maintained by Viktor Shoup [11].The rationale for the core library is its functionality, performance, and portability.

Economic perspective

We suggest that the *discounted cash flow (or DCF) approach* [10] should be used to provide economic rationale for investments to cryptographic systems. In finance, DCF is a method of valuing a project, company, or asset using the concepts of the time value of money. All future cash flows are estimated and discounted to give their present values. The discount rate used is generally the appropriate cost of capital and may incorporate judgments of the uncertainty (riskiness) of the future cash flows.

The cash flow R_t related to a cryptographic system can be described using the following formula:

$$R_t = -Cost_t + Profit_t \times (1 - R_t) - Loss_t \times R_t,$$

where $Cost_t$ is the cost of a implementation, deployment and support of the cryptographic system;

$Profit_t$ is the value of information assets being protected;

$Loss_t$ refers to the hazard in case of unauthorized access to the asset by an adversary;

R_t is the probability of an adversary to break the cryptographic system;

t is the time (e.g. in years) before the future cash flow occurs.

Results

The paper proposes a formalized methodology for analyzing the security of cryptosystems. Model-based analysis is a part of the five-step process designed to focus on the specific aspects of cryptographic systems security. The methodology is supported by software tools designed to evaluate the cryptographic system capability to resist various types of attacks. We expect that the proposed approach will be of value to security

professionals, application developers, software vendors or anyone else with an interest in information security.

One direction of our future work is the development a built-in expert knowledge base to aid in-house cryptographic systems expertise. This involves evaluating the dependency between the parameters of a cryptosystem model and the applicable attacks on the one hand, and the parameters of an attacker model and the types of attacks that they are likely to use, on the other hand.

Another direction of our work is the using of CRYPTO software tools to design new algorithms and improve present methods for factorization and computing discrete logarithms. We are also working on extending the library to include modern techniques to analyze the security hash-functions as well as asymmetric cryptosystems.

References

1. Anderson R. Why information security is hard - an economic perspective // Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC '01), 10-14 Dec 2001, New Orleans, Louisiana, USA, 2001.
2. Avdoshin S.M., Savelieva A.A. Cryptanalysis: current state and future trends// Information technologies. Moscow, 'Novye technologii', in Appendix to № 3, 2007, 35 p. (in Russian).
3. Avdoshin S.M., Savelieva A.A. Tools for asymmetric ciphers analysis: Industrial registration certificate No. 10193 dated 18.03.2008 (in Russian).
4. Brassard J. Modern Cryptology. Springer-Verlag, Berlin - Heidelberg, 1988. - 107 p.
5. Cheminod M., Cibrario Bertolotti I., Durante L., Sisto R., Valenzano A. Tools for cryptographic protocols analysis: A technical and experimental comparison // Computer Standards & Interfaces, 2008.
6. CRAMM V Official website // Siemens Enterprise Communications Limited 2006. Available at: www.cramm.com
7. Digital Security: GRIF //Available: http://www.dsec.ru/products/grif/
8. Ivanov V.P. Mathematical evaluation of information protection from unauthorized access // "Specialnaya tekhnika". 2004, N 1. –Pp. 58-64. (in Russian).
9. Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires, vol. IX. P. 5-38, Jan. 1883.
10. Kruschwitz L., Loeffler A. Discounted Cash Flow: A Theory of the Valuation of Firms (The Wiley Finance Series). Wiley, 2005. 178 p.
11. Library for doing Number Theory. Available at: http://www.shoup.net/ntl/ 06.02.2008
12. Oppliger R. Contemporary Cryptography. Artech House Publishers , 2005, 510 p.
13. RiskWatch Official website // RiskWatch, Inc. Available at: http://www.riskwatch.com/
14. Schneier B. Beyond Fear. Thinking Sensibly about Security in an Uncertain World. Copernicus Books (September 2003)
15. Schneier B. Modeling security threats // Dr. Dobb's Journal, December, 1999.
16. Zhou Y., Feng D. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing // Physical Security Testing Workshop (Hawaii, September 26-29, 2005. Available at: http://eprint.iacr.org/2005/388.pdf

В данной работе предлагается комплексный подход к оценке эффективности защиты информационных ресурсов предприятия, обеспечиваемой криптографическими средствами. Разработанный подход позволяет провести экономическое обоснование расходов организации на обеспечение информационной безопасности и сделать обоснованный выбор мер и средств криптографической защиты. В основе подхода лежит формализованный процесс анализа надежности криптосистемы в определенном контексте использования и математическая модель угроз безопасности защищаемых информационных ресурсов.

Актуальность работы

Разработка новых подходов к анализу защищенности информационных систем является важной задачей в области информационной безопасности. Росс Андерсон, ведущий эксперт в области информационной безопасности, в своей статье [1] подчеркивает, что при оценке уровня защищенности специалист должен принимать во внимание не только технические характеристики, получаемые путем криптоанализа и анализа информационных потоков, но использовать также и экономические инструменты. Это позволит при выборе необходимой степени защиты учитывать такие критерии, как уровень секретности информации, ее стоимость, время, в течение которого она должна оставаться в тайне и т.д. (см. [5])

Анализ публикаций в открытом доступе показал, что методики оценки эффективности средств криптографической защиты информации (СКЗИ) [13] с учетом перечисленных выше критериев до сих пор не разработаны. Так, в статье В.П.Иванова [10] эффективность СКЗИ предлагается оценивать с использованием математического аппарата теории массового обслуживания и теории катастроф на основе вероятностно-временной группы показателей. Выбор показателей эффективности представляет интерес, однако методика применима только для оценки криптосистем, стойкость которых основывается на сохранении в секрете алгоритмов зашифрования и расшифрования, что противоречит фундаментальному допущению Кирхгоффа [3]. В работе Н.Кукановой [11] описаны методы и инструменты анализа и контроля информационных рисков: CRAMM, RiskWatch и ГРИФ. Будучи полезными специалисту при проведении аудита систем обеспечения безопасности предприятия, перечисленные подходы, как показано в [8], не учитывают специфики СКЗИ. Автоматизированные средства анализа криптопротоколов [2] ограничиваются исследованием высокоуровневой схемы протокола и абстрагируются от деталей реализации, исходя из достаточно грубого допущения, что используемые методы шифрования идеальны и без знания ключа ни один злоумышленник не сможет их взломать.

Постановка задачи

Целью данной работы является разработка комплексного подхода к анализу эффективности СКЗИ с учетом того, каким угрозам защищаемая информация будет подвергаться со стороны злоумышленников. Для решения поставленной задачи необходимо:

разработать математическую модель угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств;

обеспечить криптоаналитика набором инструментальных средств, позволяющих оценить стойкость криптографических средств по отношению к идентифицированным угрозам;

выбрать финансово-экономические показатели для экономической оценки инвестиций в СКЗИ.

Поставленные цели согласуются с задачами, вошедшими в перечень основных направлений и приоритетных проблем научных исследований в области информационной безопасности Российской Федерации, который был разработан секцией по информационной безопасности Научного совета при Совете Безопасности Российской Федерации при активном участии ведущих ученых и специалистов научных учреждений и организаций РАН, вузов, федеральных органов исполнительной власти, работающих в различных областях, связанных с обеспечением национальной безопасности (см. [14], пп. 46, 47 и 56).

Математическая модель угроз безопасности информационных ресурсов

Оценку криптографической системы мы предлагаем проводить с использованием модели угроз безопасности информационных ресурсов из трех элементов – ABC-модели (“A” от англ. Attack – атака, “B” от англ. code-Breaker – взломщик шифра, “C” от англ. Cryptosystem – криптосистема). Очевидно, что между этими элементами, каждый из которых оказывает влияние на общую картину угроз, существует связь. Например, если исследуемый алгоритм шифрования реализован в аппаратном обеспечении, это повышает вероятность применения для взлома криптосистемы атак по побочным каналам [9], а наличие у предполагаемого взломщика доступа к распределенным вычислительным ресурсам повышает вероятность применения метода «грубой силы» и, вообще говоря, любой атаки, легко поддающейся распараллеливанию.

Для выделения важнейших параметров элементов ABC-модели нами были разработаны новые многокритериальные классификации криптосистем, атак и злоумышленников [8]. В соответствии с критериями разработанных классификаций параметрическая модель атаки задается в виде вектора $\vec{a} = A\{A_1, A_2, \ldots, A_9\}$ ($i = \overline{1,9}$) - множество значений i- го параметра модели атаки, определяющего тип атаки; модель злоумышленника - $\vec{b} = B\{B_1, B_2, \ldots, B_6\}$, B_j ($j = \overline{1,6}$) - множество значений j- го параметра модели злоумышленника; модель криптосистемы - $\vec{c} = C\{C_1, C_2, \ldots, C_6\}$, C_k ($k = \overline{1,6}$) - множество значений k- го параметра модели криптосистемы.

С каждой атакой связывается значение риска, вычисляемое по общеизвестной формуле на основе двух факторов – вероятности происшествия и тяжести возможных последствий: Риск = Влияние $\times$ Вероятность. Пусть $I: C \times A \to [0;1]$ - функция влияния (от англ. impact – влияние, воздействие: под влиянием мы будем понимать степень ущерба от применения атаки $\vec{a} = A$ к криптосистеме $\vec{c} = C$),

$R : B \times A \to [0; 1]$ - вероятность того, что злоумышленник $b \in B$ предпримет атаку $a \in A$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной. Обозначим через $B : A \times B \times C \to [0; 1]$ функцию, задающую уровень риска, связанного с атакой $a \in A$ в условиях, когда она может быть применена злоумышленником $b \in B$ для взлома криптосистемы $c \in C$. Тогда функция риска B выражается следующим образом:

$$B(a,b,c) = I(c,a) \cdot R(b,a)$$

Уровень взаимного влияния параметров элементов ABC-модели (криптосистемы и атаки - для вычисления функции I, злоумышленника и атаки - для вычисления функции R) определяется на основе экспертных оценок. Формулы для вычисления значений функций I и R приведены в [8].

Будем считать, что криптосистема $c \in C$ подвержена атаке $a \in A$ в условиях, когда ей угрожает злоумышленник $b \in B$, если $B(a,b,c) > q$, т.е. связанный с ней уровень риска превышает заданное пороговое значение q, где $q \in [0; 1]$. Допустимый уровень риска q является настраиваемым параметром ABC-модели угроз криптосистемы. Значение q задается с учетом критичности защищаемых данных и объема ресурсов, доступных специалисту, который осуществляет аудит системы.

В общем случае криптосистема может включать несколько подсистем (например, генератор ключей и симметричный шифратор), к каждой из которых применим свой набор атак, и на криптосистему может нападать несколько злоумышленников. Тогда множество атак, которым подвержена криптосистема, состоящая из подсистем $c \in C_{сў}$ ($C_{сўН}$ C), в условиях, когда ей угрожают злоумышленники $b \in B_{вў}$ ($B_{вўН}$ B), будем определять по формуле $L = \bigcup_{b \in B_{вў}} \bigcup_{c \in C_{сў}} I(b,c)$, где $I(b,c) = \{a \in A : B(a,b,c) > q\}$ при заданном уровне риска.

Оценка стойкости криптографических средств к идентифицированным угрозам

После того, как выделен набор атак, представляющих наибольшую угрозу для защищаемых данных, необходимо оценить способность криптосистемы противостоять этим атакам. Базой для получения таких оценок может служить статистика взлома и успешных атак на криптосистемы. Однако такая информация, во-первых, не всегда доступна, а, во-вторых, со временем теряет актуальность, т.к. повышение производительности вычислительной техники и появление новых видов атак на шифры ведет к понижению стойкости известных криптографических алгоритмов.

Для оценки стойкости криптосистем с открытым ключом нами был реализован программный комплекс «Инструментальные средства криптоанализа асимметричных шифров». Реализованный программный комплекс состоит из библиотеки КОНСТРУКТОР, включающей необходимые примитивы для конструирования современных методов криптоанализа асимметричных шифров, и приложения АНАЛИТИК, имеющего графический интерфейс пользователя для доступа к функциям факторизации и дискретного логарифмирования библиотеки КОНСТРУКТОР. Для выполнения операций с длинными числами использована библиотека NTL [4]. Выбор базовой библиотеки, обусловленный её функциональностью, скоростью, компактностью и переносимостью, позволил получить эффективные реализации перечисленных теоретико-числовых алгоритмов.

Расчет эффективности капитальных вложений в использование криптографических средств

В настоящее время нет единых стандартов, позволяющих оценить СКЗИ с экономических позиций. В таблице представлены результаты сравнительного анализа методов оценки эффективности инвестиций в средства обеспечения ИБ. На основании результатов был сделан вывод, что оптимальным является метод дисконтирования денежных потоков [12], позволяющий получить наиболее полное представление о целесообразности капитальных вложений, хотя и требующий много времени и усилий на расчет экономических показателей.

Определим денежные потоки, связанные с использованием СКЗИ, за период t (где t = 0, 1, 2…. T - периоды, T – горизонт расчета). Затраты $Cost_t$ на приобретение, установку и эксплуатацию СКЗИ

могут быть определены очень точно. С защищаемой информацией связаны значения дохода $Profit_t$ от ее использования и ущерба $Loss_t$ от НСД в течение указанного промежутка времени t. Пусть результаты оценки способности криптосистемы противостоять атакам показали, что в t-м периоде злоумышленник получит доступ к защищаемой информации с вероятностью R_t. Тогда математическое ожидание дохода R_t, связанного с использованием оцениваемой СКЗИ, вычисляется по формуле:

$$R_t = -Cost_t + Profit_t \times (1 - R_t) - Loss_t \times R_t$$

На основании этих данных о притоках и оттоках денежных средств вычисляются финансово-экономические показатели эффективности инвестиций в криптосистему и делаются выводы о ее соответствии потребностям организации.

Таблица 1. Сравнительный анализ методов оценки эффективности инвестиций в средства обеспечения ИБ

Методика оценки	Преимущества	Недостатки
Коэффициент возврата инвестиций	• Показатель, понятный финансистам	• Отсутствие достоверных методов расчета в области ИТ • «Статичный» показатель
Совокупная стоимость владения	• Позволяет оценить целесообразность реализации проекта на основании оценки только затрат • Предполагает оценку затрат на различных этапах всего жизненного цикла системы	• Не учитывает качество системы безопасности • «Статичный» показатель • Показатель, специфичный для ИТ
Дисконтированные показатели эффективности инвестиций	• Показатель, понятный финансистам • Учитывает зависимость потока денежных средств от времени • Учитывает все потоки денежных средств, связанные с реализацией проекта	• Сложность расчета

Основные результаты исследования

Выполнен анализ существующих методов и средств оценки криптосистем, выявлены их недостатки;

Разработана математическая модель угроз безопасности информационных ресурсов, защищенных с использованием СКЗИ;

Разработан программный комплекс «Инструментальные средства криптоанализа асимметричных шифров», получены авторские свидетельства Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (Роспатента) [7] и Отраслевого фонда алгоритмов и программ [6];

На основе анализа существующих методов обоснования инвестиций в средства обеспечения ИБ выделен набор финансово-экономических показателей для оценки эффективности СКЗИ с экономических позиций и предложена методика дисконтирования денежных потоков при оценке эффективности инвестиций в СКЗИ.

Использованная литература

1. Anderson R. Why information security is hard - an economic perspective // Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC '01), 10-14 Dec 2001, New Orleans, Louisiana, USA, 2001.

2. Cheminod M., Cibrario Bertolotti I., Durante L., Sisto R., Valenzano A. Tools for cryptographic protocols analysis: A technical and experimental comparison // Computer Standards & Interfaces, 2008.
3. Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires, vol. IX. P. 5-38, Jan. 1883.
4. NTL // Available at: http://www.shoup.net/ntl/ 06.02.2008
5. Schneier B. Modeling security threats // Dr. Dobb's Journal, December, 1999.
6. Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. - М.: ВНТИЦ, 2008. - №50200800603.
7. Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. Свидетельство о государственной регистрации в Реестре программ для ЭВМ № 2005612258 от 22.05.08.
8. Авдошин С.М., Савельева А.А. Оценка эффективности криптографической защиты информационных ресурсов в корпоративных системах // Труды международной конференции Software Engineering Conference (Russia) SEC(R) 2008, Москва. - С. 298 – 316. Опубликовано: http://www.secr.ru/ 25.12.2008
9. Жуков А.Е. Криптоанализ по побочным каналам (Side Channel Attacks). // Материалы конференции РусКрипто – 2006.
10. Иванов В.П. Математическая оценка защищенности информации от несанкционированного доступа // "Специальная техника", N 1, 2004. - С. 58-64.
11. Куканова Н. Методы и средства анализа рисков и управление ими в ИС // Byte/Россия,№12, 2005. С.69-73.
12. Старик Д.Э. Расчеты эффективности инвестиционных проектов. М.: Финстатинформ, 2001.
13. Руководящий документ Гостехкомиссии России "Защита от несанкционированного доступа к информации. Термины и определения". - М.: ГТК РФ, 1992. - 13 с.
14. Шерстюк В.П. МГУ: научные исследования в области информационной безопасности // Информационное общество. - М., 1989. С.48-53.

Метод защиты закрытого ключа при криптографической аутентификации в системах дистанционного обучения

Сергеева Е.Н.

Московский институт радиотехники, электроники и автоматики (технический университет)
г. Москва, Россия
camena@inbox.ru

Method of protecting a closed key with cryptographic authentication in systems of remote training

Sergeeva E.N.

Moscow state institute of electronics and mathematics (technical university)
Moscow, Russia
camena@inbox.ru

Increasing attention is given to a new direction in education – remote training. Remote education on the one hand opens new opportunities, as it allows to realize the process of training based on the use of modern information and telecommunication technologies for realisation of training at a distance, without direct, personal contact between the teacher and a student, on the other hand, it sets new problems. One of the basic problems is provision of protection in the system of monitoring and transfer of knowledge.

Important role in operation of the system of remote training is given to the software responsible for solving the task of identification and authentication of administrators and users possessed of expanded rights. In case of remote access, the methods resistant to passive and active methods of attack should be applied. One of such methods consists in application of bilateral cryptographic authentication, with the use of closed key K and random number x. Mechanism of open keys can be applied, for example, for additional protection in asymmetric encoding algorithms.

This work is devoted to actual problem associated with capabilities of restoration of closed key of asymmetric encoding algorithm, based on the information, intercepted in various channels of information leakage, because in that case, free unauthorized access would be possible, to the transmitted information. At that, there is a problem, consisting in that during reading/recording of closed key, weak electromagnetic signals would be generated, bearing the information about the key. Extraction of signals from noise by means of the method of accumulation, results in that after a certain number of addressing to the key, the resistance would be sharply reduced. Thus, a necessity arises, of the development of virtual algorithms for protection of closed key. One of such algorithms is the use of method of imposing, on the closed key, of randomized masks, as well as binary sequences, produced by random-number generator available with the subscriber who owns the key.

Все большее внимание уделяется новому направлению в образовании – дистанционному обучению. Дистанционное образование с одной стороны открывает новые возможности, так как позволяет реализовать процесс обучения, основанный на использовании современных информационных и телекоммуникационных технологий для осуществления обучения на расстоянии без непосредственного, личного контакта между преподавателем и учащимся, с другой стороны ставит новые задачи. Одной из основных таких задач является построение защиты в системе контроля и передачи знаний.

Важную роль в работе системы дистанционного обучения играет программное обеспечение, отвечающее за задачу идентификации и аутентификации администраторов и пользователей, обладающих расширенными правами. При удаленном доступе должны применяться методы устойчивые к пассивным и активным способам нападения. Одним из таких методов является применение двухсторонней криптографической аутентификации с использованием закрытого ключа K и случайного числа x. Для дополнительной защиты, к примеру, может применяться механизм открытых ключей в ассиметричных алгоритмах шифрования.

Данная работа посвящена актуальной задаче, связанной с возможностями восстановления закрытого ключа ассиметричного алгоритма шифрования по информации, перехваченной в различных каналах утечки информации, поскольку в этом случае возможен свободный несанкционированный доступ к передаваемой информации. При этом возникает проблема, заключающаяся в том, что при чтении/записи закрытого ключа возникают слабые электромагнитные сигналы, несущие информацию о ключе. Выделение сигналов из шума методом накопления приводит к тому, что после определенного числа обращений к ключу стойкость резко снижается. Таким образом, возникает необходимость в разработке виртуальных алгоритмов защиты закрытого ключа. Одним из таких алгоритмов является использование метода наложения на закрытый ключ случайных масок, двоичных последовательностей, выработанных генератором случайных чисел у абонента, владеющего ключом.

Разработка средств защиты программного продукта «Учет проживающих в сельской местности» для территориального органа Федеральной службы государственной статистики по Республике Башкортостан «Башкортостанстат»

Фатхинуров Айрат Ринатович

Башкирский государственный аграрный университет
г. Уфа, Россия
tanayr@mail.ru

Development of the protection software "The Accountant living in the countryside" for the Federal Service for State Statistics of the Republic of Bashkortostan (Bashkortostanstat)

Fathinurov A.R.

The Bashkir State Agrarian University
Ufa, Russia
tanayr@mail.ru

The given software product is developed for automation and ordering of the account living in a countryside of Republic Bashkortostan. For protection of a database are established the password by means of enciphering and a binding of a key of enciphering to serial number of a hard disk of a computer.

Как известно, во многих странах мира сбор статистической информации стал неотъемлемой чертой цивилизованной жизни. Статистическая работа состоит в том, чтобы собрать числовые данные о массовых явлениях, обработать их, представить в форме, удобной для анализа, проанализировать и интерпретировать полученные результаты.

В статистических данных отображаются сведения о развитии отдельных сторон жизни общества. Практическое применение полученной информации - это создание информационной базы для принятия управленческих решений.

В настоящее время перед статистической наукой встают актуальные проблемы дальнейшего совершенствования системы показателей, приемов и методов сбора, обработки, хранения и анализа статистической информации; развития и повышения эффективности автоматизированных систем управления, создания автоматизированных банков данных, распределительных банков данных и т.д.

С этой целью существуют специализированные органы государственной статистики. Одним из таких центров является Территориальный орган Федеральной службы государственной статистики по Республике Башкортостан - «Башкортостанстат».

Для целей автоматизации и систематизации учета информации со всех районов на предприятии существует отдел информационно–издательских услуг. Данный отдел ведет деятельность по разработке программного обеспечения, позволяющего достичь эти цели.

Отдел информационно – издательских услуг является структурным подразделением Территориального органа Федеральной службы государственной статистики по Республике Башкортостан, осуществляющим работу по разработке программного обеспечения и оказания информационно-статистических услуг. Отдел осуществляет свою деятельность под непосредственным руководством заместителя руководителя Башкортостанстата.

Основными задачами отдела являются:

- заключение договоров на разработку программного обеспечения и реализацию информационно-статистических материалов;
- проведение работ по распространению и сопровождению разработанных программ;
- осуществление взаимодействия с отделами Башкортостанстата в подготовке информационно-статистических материалов сторонним заказчикам;
- организация системного изучения материалов по вопросам методологии проектирования и программирования задач;
- использование средств автоматизации программирования и изучение достижений в области программирования и др.

Исходя из этого, можно отметить следующее. Отдел обеспечивает предоставление статистической информации сторонним заказчикам и осуществляет взаимодействия между отделами Башкортостанстата в подготовке этой информации. А также занимается разработкой и реализацией программного обеспечения для решения экономических и статистических задач (рисунок 1, рисунок 2).

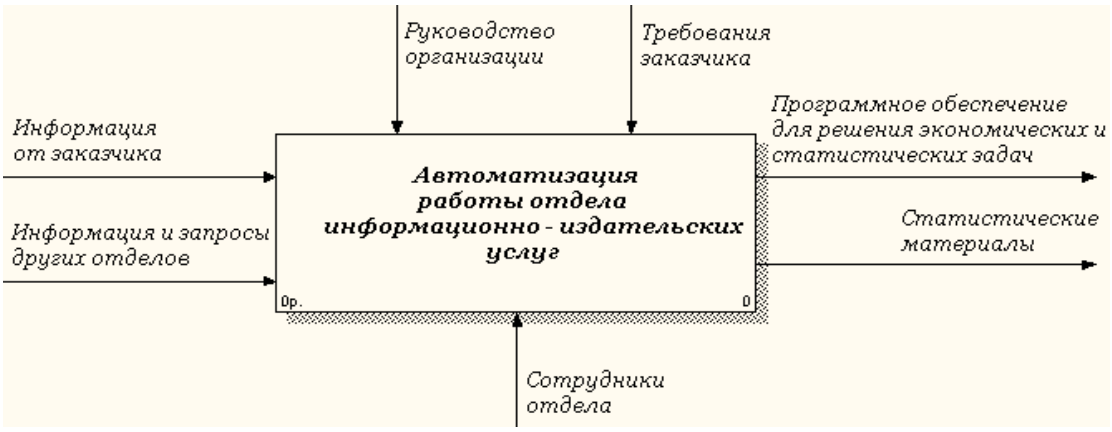


Рисунок 1 Функциональная модель работы отдела информационно – издательских услуг

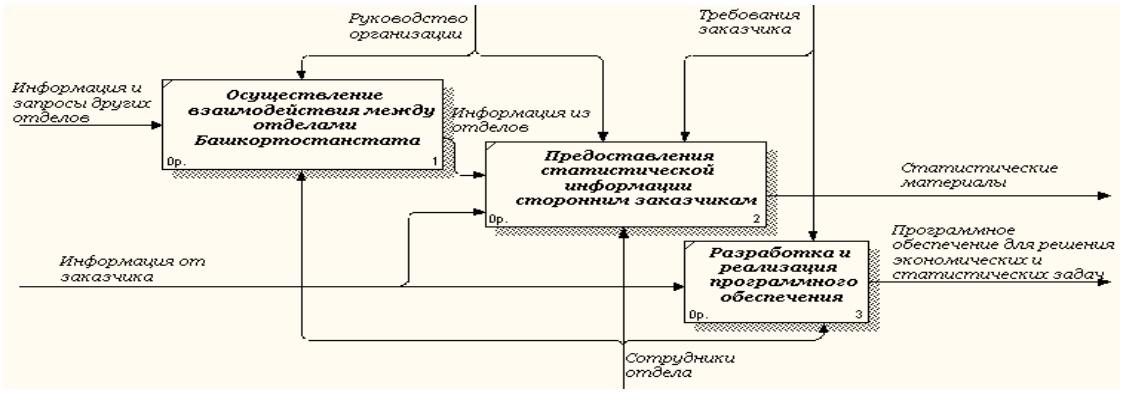


Рисунок 2 Декомпозиция блока «Автоматизация работы отдела информационно–издательских услуг»

В отделе информационно–издательских услуг используется программа «Похозяйственный учет». При разработке и внедрении предыдущей версии программы возникли следующие проблемы.

Данный программный продукт разрабатывался для массового внедрения и предназначался для хранения и анализа статистических данных хозяйствующих субъектов. Но одна из ключевых идей данного проекта была скопирована и реализована сторонними производителями, предоставившими подобный продукт по более низкой цене. Так же поступили жалобы со стороны клиентов, такие как:

- число установок ПО ограничены (при критических ошибках, при прерывании установки, аппаратных сбоев и т.д.);
- возможность копирования БД и просмотр её сторонними средствами.

Сегодня сложилась парадоксальная ситуация, когда в большинстве отечественных ПК в основном используется нелицензионное программное обеспечение.

В соответствии с международным правом труд автора программы приравнен к труду других творцов интеллектуальной собственности, таких как писатели, музыканты, художники, и подлежит защите. Однако в отличие от книги или картины массовое копирование программы не вызывает каких-либо технических трудностей и не требует специального дополнительного оборудования, если разумеется, не считать компьютер. В этом отношении программа намного беззащитнее, чем, скажем, скульптура или книга. Общий ущерб от нелегального копирования программ по оценкам западных специалистов составляет от 10 млрд. долларов в год.

Бурное развитие информационных технологий и использование их в самых различных областях человеческой деятельности привело к тому, что помимо задач передачи, хранения и обработки информации возникла не менее, а в ряде случаев и более важная задача защиты информации. Выделяют шесть направлений деятельности по защите информации:

1. Защита от несанкционированного доступа в автоматизированных информационных системах, имеющая как программную, так и аппаратную реализацию.
2. Защита информации при передаче по каналам связи и в средствах их коммутации (в том числе в локальных (ЛВС) и распределённых вычислительных сетях) .
3. Защита юридической значимости так называемых «электронных» документов (в системе электронной почты (e-mail) и др.).
4. Защита от утечки информации в виде побочных электромагнитных излучений и наводок (ПЭМИН).
5. Защита от программных средств скрытого информационного воздействия (частным случаем которых являются компьютерные вирусы).
6. Защита от несанкционированного копирования и распространения программ и баз данных.

Для разработчика программного обеспечения, как и для любого другого производителя основная задача состоит в том, чтобы окупить затраты на производство и получить прибыль. При этом возможны два крайних варианта: либо производитель находит заказчика, который оплачивает разработку, либо все затраты покрываются за счёт продаж.

Для противодействия попыткам несанкционированного копирования используются различные методы защиты программного обеспечения: организационные, юридические, программные и программно-аппаратные. Наиболее популярными являются технические, т.е. программные и программно-аппаратные методы, так как только они обеспечивают противодействие в момент несанкционированного копирования программного продукта, в отличие от остальных, где санкции за нелегальное использование либо отсутствуют, либо разнесены во времени с моментом эксплуатации нелегальной копии.

Мною была создана база данных, интерфейс к ней и средства защиты базы данных от несанкционированного копирования и использования. Разработанный программный продукт будет использоваться в Башкортостанстате и поставляться сторонним организациям для учета хозяйственной информации.

Разработка программы состояла из нескольких этапов.

На первом этапе разработки было предложено разработать базу данных для хранения и печати сведений о лицах, проживающих на территории администрации сельского поселения. Основным требованием к БД является простота и удобство хранения сведений.

После реализации данной БД по средствам MS Access, был разработан программный интерфейс для удобного взаимодействия между пользователями и БД. Программный продукт имеет формы для заполнения каждой таблицы. После заполнения всех данных пользователь может осуществлять необходимые действия на главной форме.

Так же было реализовано три отчета по учету лиц: проживающих на территории, с истекшим сроком прописки и истекающим.

Программа и отчеты были реализованы средствами Delphi.

База данных защищена паролем. Программный модуль обращается к БД, используя этот пароль. Пароль имеет длину более 10 символов.

После реализации БД и интерфейса пользователя к ней, переходим ко второму этапу проектирования. Были определены методы защиты информации.

В ходе второго этапа была реализована пробная версия программы для шифрования и дешифрования. Так же рассмотрены способы работы с ОС Windows XP посредством Delphi 7.0 и реализован модуль защиты программы при помощи возможностей ОС. Изучен принцип работы с буфером обмена Windows, защита от копирования.

При дальнейшей разработке происходит наложение пароля на БД, при помощи шифрования, а также привязка ключа шифрования к серийному номеру жесткого диска ПК. Объединив полученные модули, я получил конечную структуру программного продукта. Затем возникла необходимость в организации последовательного запуска каждого модуля программного продукта (рисунок 3).

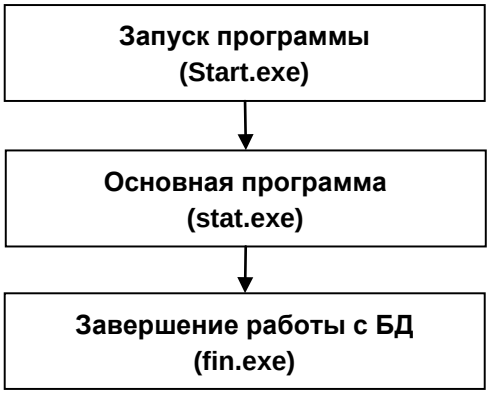


Рисунок 3 Схема последовательного запуска каждого модуля программного продукта

Также были внесены некоторые изменения в программный код каждого модуля. Все используемые файлы, кроме исполняемых, имеют атрибут «системный». В таблице 1 содержится информация о функциях каждого модуля программного продукта.

Таблица 1 Описание модулей программного продукта

Модуль	Основные функции
Start.exe	Реализация проверки пароля пользователя (пароль зашифрован и привязан к серийному номеру диска ПК, хранится в base.dat), дешифрование базы данных (БД хранится в stat_.exe), а также создание ключа по определенному алгоритму (динамично меняется в зависимости от даты) и сохранение его во временный файл base1.dat. Также имеется возможность для смены пароля пользователя. Запускает модуль Stat.exe.
Stat.exe	Основной модуль программного продукта, реализует работу с БД. При запуске проверяет ключ записанный в base1.dat. А также не позволяет пользователю по средствам Windows просмотреть содержание папки с программным продуктом и проверяет содержание буфера обмена. Также создает метку «My application». После завершения работы модуля, происходит запуск модуля fin.exe.
fin.exe	При запуске модуля проверяется существование метки «My application». При отсутствии метки программа завершается. Данный модуль запрашивает у пользователя разрешения на сохранение БД (т. е. шифрование БД). При отказе все изменения в БД не сохраняются, остается старая зашифрованная БД.

Данный принцип работы удобен, с точки зрения наличия резервной копии базы данных. В случае сбоя системы, можно восстановить БД.

Программный продукт отвечает заданным требованиям безопасности. При копировании папки с программой на сторонний ПК, она теряет работоспособность.

Следующий этап предполагает написание программы установки для созданного программного продукта. Была разработана программа упаковки всех модулей. А также программа для распаковки, запрашивающая ключ. Ключ генерируется по определенному алгоритму в зависимости от серийного номера диска ПК. Предполагается, что пользователь будет отсылать по электронной почте некоторые сведения о системе. После этой процедуры он получает уникальный ключ, который предполагает установку программы только на данный ПК.

4 Секция
Методы обнаружения и предотвращения компьютерных угроз

Methods used to detect and prevent computer threats

Методы обнаружения и предотвращения инсайдерских компьютерных угроз в локальных вычислительных сетях

Баринов А.Е.

Южно-уральский государственный университет
г. Челябинск, Россия
barinov_ae@bk.ru

Methods of detecting and preventing insider computer threats in local area networks (LAN)

Barinov A.E.

South Urals State University
Chelyabinsk, Russia
barinov_ae@bk.ru

Many organizations use the means of local area networks (LAN) to ensure the needs of data processing and transmission. Before using LAN the main part of data processing and exchange was centralized; information and its management were concentrated in one place and centralized. Nowadays LANs logically and physically distributed the data, computing power and message exchange service through the whole organization.

Security services responsible for data protection and means of data processing and transmission shall also be distributed through the whole LAN. It means that the main objectives of the company's IT-department in terms of LAN security are the following: to ensure confidentiality and integrity of the data during its storage, processing or transmission within the LAN; to ensure access to the data stored at LAN, and ensure possibility for their proper processing and transmission. And to guarantee identification of the sender and recipient of the messages.

Having classified informational security threats in terms of their integration into automated networks (AN), LAN in particular, we give a clear definition for internal (insider) threats for informational security (IS). According to the results of relevant researches, at the moment internal threats for international security comprise considerable part (18-35%) of the threats of large companies. The goal of this work is to study methods of detection and prevention of such threats.

The work deals with the internal threats both for single PC and LAN in general.

While analyzing IS threats for single PC we have studied the following types of the threats: indirect threats (data reading in the packages of other users, masking for registered user for the purposes of stealing passwords and other access data, using program trips, access to the protected data by means of series of allowed requests, using drawbacks of the programming languages and operating systems, willful entering of special blocks such as “Trojan horses” into the software libraries, malicious breaking down of the protection tools), direct (using intercepting devices, distant photos, electromagnetic pickup; stealing data medium and industrial wastes, copying data carriers, unauthorized usage of terminals, illegal connection to the equipment, malicious breaking down of the protection tools), and casual threats (software errors, breakdowns, negligence). Each of these types of the threats was analyzed in terms of the methods used for their detection and prevention. The work resulted in some recommendations given by the author.

While analyzing technical IS threats in LANs the following willful threats were given much attention: technical pickup devices, DoS and DDoS attacks, means for interception of the data transmitted in the network, malicious software aimed at the destructive network influence. We examined existing and offered new methods of detection and prevention of such threats as technical pickup devices, Dos and DDoS attacks, means for interception of the data transmitted in the network. Struggle against the malicious software aimed at the destructive network influence was considered on the levels implemented by means of anti-virus software (detection, evaluation of the threat of software, prevention, and specific features for detection and prevention of the software aimed at the destructive network influence were separated. The analysis of anti-virus means for struggle against this software resulted in recommendations for prevention of implementation and elimination of results of implementation of this software. Detection and prevention of casual threats in the LAN is represented in the same way as the one for the single PC taking into account the peculiarities of the LAN. To give a conclusion it should be mentioned that there are both general methods of detection of the software, and methods that are typical for destructive software in the LAN only, sometimes taking into account topology of the network.

This work resulted in 16 recommendations regarding protection of the LAN from the insider threats. In terms of their implementation these recommendations are given on the programming, mechanical and organizational level. Recommendations for struggling against technical threats are separated both for single PCs and LANs in general. Recommendations for the struggle against interception of the traffic were given on the physical level (detection and prevention from installation of the technical devices for pickup and interception of the data), channel level (protection from replacement of the network drivers), network level (usage of IPSec protocol in the tunnel mode), and session level (improvements for RPC protocol were declared).

The problems of adequacy for implementation of the given recommendations were considered separately. The general scheme for IS and LAN risk evaluation and elimination of detected LAN threats was offered.

The results of this work can be used for creation, maintenance, modification and audit of IS of the LAN.

Многие организации используют средства локальных вычислительных сетей (ЛВС) для обеспечения нужд обработки и передачи данных. До использования ЛВС основная часть обработки и обмена данными была централизована; информация и управление ею были сосредоточены в одном месте и централизованы. Сейчас ЛВС логически и физически рассредоточили данные, а также вычислительную мощность и службы обмена сообщениями по всей организации.

Службы безопасности, защищающие данные, а также средства по их обработке и передаче, также должны быть распределены по всей ЛВС. Следовательно, задачами ИТ-подразделений компаний по обеспечению безопасности ЛВС должны быть: обеспечение конфиденциальности и целостности данных в ходе их хранения, обработки или при передаче по ЛВС, доступности данных, хранимых в ЛВС, а также обеспечение возможности их своевременной обработки и передачи, гарантия идентификации отправителя и получателя сообщений.

Проклассифицировав угрозы ИБ по принципу их внедрения в АС, в частном случае ЛВС, мы чётко определяем понятие внутренних (инсайдерских) угроз ИБ. По данным сторонних исследований в настоящее время в крупных компаниях внутренние угрозы информационной безопасности в ЛВС составляют значительную долю (18-35%). Изучение методов обнаружения и предотвращения подобных угроз и стало целью данной работы.

В работе рассмотрены внутренние угрозы ИБ как для одиночного ПК, так и для ЛВС в целом.

При анализе угроз ИБ для одиночного ПК были проанализированы следующие типы угроз: косвенные угрозы (считывание данных в массивах других пользователей, маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа,

использование программных ловушек, получение защищаемых данных с помощью серии разрешенных запросов, использование недостатков языков программирования и операционных систем, преднамеренное включение в библиотеки программ специальных блоков типа “троянских коней”, злоумышленный вывод из строя механизмов защиты), прямые (применение подслушивающих устройств, дистанционное фотографирование, перехват электромагнитных излучений; хищение носителей информации и производственных отходов, копирование носителей информации, несанкционированное использование терминалов, незаконное подключение к аппаратуре, злоумышленный вывод из строя механизмов защиты), а также непреднамеренные угрозы (ошибки в ПО, сбои, халатность). По каждому из типов угроз проведен анализ существующих методов обнаружения и предотвращения. В результате были вынесены собственные авторские рекомендации.

При анализе технических угроз ИБ в ЛВС подробно были рассмотрены преднамеренные угрозы, такие как технические средства съёма, DoS и DDoS атаки, средства перехвата передаваемых по сети данных, вредоносное ПО, направленное на деструктивные сетевые воздействия. Были рассмотрены существующие и предложены новые методы обнаружения и предотвращения таких угроз, как технические средства съёма, DoS и DDoS атаки, средства перехвата передаваемых по сети данных. Борьба с вредоносным ПО, направленном на деструктивные сетевые воздействия была рассмотрена, как на уровнях, реализуемых средствами антивирусного ПО: обнаружение, оценка степени опасности ПО, предотвращение, а также были выделены особенности обнаружения и предотвращения ПО, направленного на деструктивные сетевые воздействия.. Итогом анализа антивирусных средств борьбы с данным ПО стало вынесение рекомендаций по разработке антивирусного ПО. Особенности обнаружения и предотвращения ПО направленного на деструктивные сетевые воздействия были выделены для каждого из четырёх классов подобного ПО (ПО использующее уязвимости MSTP протокола, атаки на маршрутизаторы, ПО направленное на подмену сетевых адресов, ПО направленное на создание в сети ложного сервера). Для каждого из данных классов были вынесены рекомендации по предотвращению внедрения и устранению последствий внедрения данного ПО. Обнаружение и предотвращение непреднамеренных угроз в ЛВС представлено по аналогии с одиночным ПК с поправками на особенности ЛВС. Подводя итоги, стоит отметить, что есть как наиболее общие методы детекции вредоносного ПО, так и методы характерные исключительно для деструктирующего ПО в ЛВС, иногда даже с поправкой на топологию сети.

Итогом данной работы стало вынесение 16 общих рекомендаций по защите ЛВС от инсайдерских угроз. Относительно реализации данные рекомендации вынесены на программном, аппаратном и организационном уровнях. Рекомендации по борьбе с техническими угрозами вынесены, как для одиночных ПК, так и для ЛВС в целом. Рекомендации по борьбе с угрозами перехвата передаваемого трафика вынесены на физическом уровне (обнаружение и предотвращение установки технических средств съема и перехвата данных), канальном уровне (защита от подмены сетевых драйверов), сетевом уровне (использование протокола IPSec в туннельном режиме), сеансовом уровне (предложены улучшения в протокол RPC).

Отдельно рассмотрены проблемы адекватности применения вынесенных рекомендаций. Предложена общая схема оценки рисков ИБ в ЛВС и устранения обнаруженных угроз в ЛВС.

Результаты данной работы могут быть применены при построении, обслуживании, модификации, а также аудите ИБ ЛВС.

Создание методики распознавания сетевых соединений вредоносных программ

Голованов С.Ю.

Московский инженерно-физический институт (государственный университет)
г. Москва, Россия
chudovisha@gmail.com

Creating a methodology for recognizing malware network connections

Golovanov S.Y.

Moscow Engineering Physics Institute (State University)
Moscow, Russia
chudovisha@gmail.com

Here is an analysis of existing systems to protect information from malicious software, and a method of finding the malicious activity on the basis of analysis of sources network activity.

Malicious software that uses networking technology to transfer of confidential data or receiving commands, have long been by the many numerical and popular among intruders. Their detection and identification of successfully performed using the signature and heuristic methods implemented in most software products and security systems. However, these approaches are clearly not enough because of the malicious use of protective methods, such as the encryption code did not allow a search for the signature, and obfuscation lack of both static and dynamic heuristic analysis. The success of hackers and virus writers using similar techniques, said the rapidly growing number of such malicious programs.

The aim of this work - to propose a new method for determining the presence of malware on the compromised system using inputs from the field of intrusion detection systems. The method is based on the representation of the network address of the attacker to use malicious software to a certain set of characteristics to work with statistical methods or apparatus of neural networks. This will prevent even more unknown malware using cryptographic protocols for network communication.

As a result of the proposed new method for detecting malicious activity, and presents the main characteristics of network addresses available for use in this model.

В работе произведён анализ существующих систем защиты информации от вредоносного ПО, предложен метод нахождения вредоносной активности на основе анализа источников сетевой активности.

Вредоносные программы, использующие сетевые технологии для например передачи конфиденциальных данных или получения команд, уже давно стали самими много численными и популярными среди злоумышленников. Их обнаружение и распознавание успешно производиться с помощью сигнатурных и эвристических методов, реализованных в большинстве программных продуктах и системах защиты информации. Однако данных подходов явно не хватает из-за использования злоумышленниками защитных методик, таких как шифрование кода, не позволяющее проведение сигнатурного поиска, и обфускация, препятствующая как статическому, так и динамическому эвристическому анализу. Об успешном использовании злоумышленниками подобных методик и говорит быстро растущее количество подобных вредоносных программ.

Цель данной работы - предложить новый метод определения наличия вредоносной программы на скомпрометированной системе с использованием наработок из области систем обнаружения вторжения.

Метод основан на представлении сетевого адреса злоумышленника, используемого вредоносной программой, в виде набора некоторых характеристик поддающихся обработки статистическими методами или аппаратом нейронных сетей. Это позволит предотвратить работу даже еще не известных вредоносных программ, использующих криптографические протоколы для работы с сетью.

В результате работы предложен новый метод детектирования вредоносной активности и представлены основные наборы характеристик сетевых адресов пригодных для использования в этой модели.

Разработка фильтра - анализатора сетевых пакетов с функцией контроля приложений

Ишемгулов Р.Ф.

Оренбургский Государственный Аграрный Университет
г. Оренбург, Россия
mr_dream@mail.ru

Filter dvelopment - analysing network packages with the control of appendices function

Ishemgulov R.F.

Orenburg State Agrarian University
Orenburg, Russia
mr_dream@mail.ru

В настоящее время особо актуальными в области информационных технологий становятся вопросы безопасности информации. Это связано с широкой информатизацией в отраслях производства, бизнеса, образования, государственных учреждениях и т.д., интеграцией автоматизированных систем в локальные и глобальные вычислительные сети.

Для наиболее эффективной защиты от сетевых атак, наряду с анализом и фильтрацией трафика необходимо также осуществлять контроль приложений, использующих доступ к сети. Актуальность этого обусловлена возможностью внедрения вредоносного кода в санкционированные приложения (исполняемые файлы или библиотеки), с целью сокрытия злоумышленных действий.

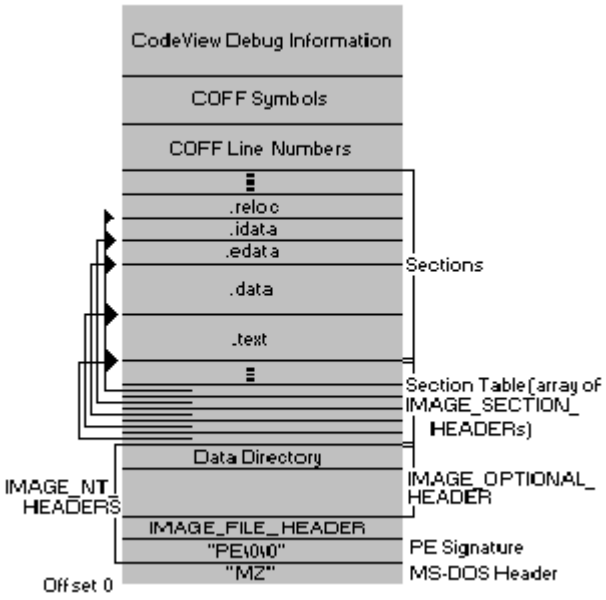
Учитывая актуальность рассмотренной задачи, целью нашей работы является разработка приложения, осуществляющего контроль сетевого трафика, путем просмотра содержания сетевых пакетов, и целостности приложений, за счет проверки содержимого исполняемого файла или библиотеки.

Архитектура программы представлена двумя компонентами:

- Контроль сетевых пакетов.
- Контроль приложения.

Для анализа пакетов нам необходимо работать непосредственно с сетевым адаптером и ядром системы. Анализ источников информации по выбранной теме позволил установить, что в наибольшей степени в качестве инструмента подходит набор средств (библиотека) PCAP.

Контроль приложения будет осуществляться путем просмотра PE-структуры исполняемых файлов.



В данной структуре представляет интерес таблица импорта. Таблица импорта содержит в себе адреса функций, которые импортируются из различных библиотек. **[5]** Просмотр этой секции исполняемого файла, по нашему мнению, достаточен для подтверждения целостности исполняемого файла.

Для проверки целостности был выбран алгоритм, основанный на проверке избыточности циклической суммы (CRC32). С точки зрения математики контрольная сумма (КС) является типом хеш-функции, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных, например сетевого пакета или блока компьютерного файла, применяемого для обнаружения ошибок при передаче или хранении информации.

Для подсчета CRC32 будет использована следующая функция:

```
unsigned long Crc32(unsigned char *buf, unsigned long len)
{
    unsigned long crc_table[256];
    unsigned long crc;

    for (int i = 0; i < 256; i++)
    {
        crc = i;
        for (int j = 0; j < 8; j++)
            crc = crc & 1 ? (crc >> 1) ^ 0xEDB88320UL : crc >> 1;

        crc_table[i] = crc;
    };

    crc = 0xFFFFFFFFUL;

    while (len--)
        crc = crc_table[(crc ^ *buf++) & 0xFF] ^ (crc >> 8);

    return crc ^ 0xFFFFFFFFUL;
};
```

В данной работе реализовано:

- Фильтрация сетевых пакетов
- Анализ PE-структуры исполняемых файлов
- Проверка целостности исполняемых файлов

XSS и Iframe. Зараженные сайты. Опасности. Методы защиты

Калинин А.В.

Пермский государственный университет
г. Пермь, Россия
antonu.kalininu@gmail.com

XSS and Iframe. Infected sites. Dangers. Protection methods

Kalinin A.V.

Perm state university
Perm, Russia
antonu.kalininu@gmail.com

Безопасный интернет – мечта каждого его пользователя. Однако в данный момент времени он представляется не таким уж безопасным.

В наши дни проблема атак через браузер очень актуальна. Ежедневно пользователи Интернета просматривают тысячи web-страниц, не задумываясь о безопасности своих данных, своего компьютера. Однако просматривая некоторые сайты, мы подвергаемся серьезному риску заразить свой компьютер каким-либо вредоносным кодом. Последствия заражения могут быть необратимы. Пользователь может потерять как пароли от критичных ресурсов (какой-либо сервер, e-mail, icq и т.д.), так и все данные на своем компьютере, сервере. Злоумышленник также может получить полный контроль над зараженной машиной.

Особое внимание необходимо уделить атакам через браузер. В настоящее время существует множество технологий атак: xss, атаки по средствам iframe, скрытые загрузки (drive-by downloads), атаки с использованием JavaScript, создание сайтов с внедренным в них вредоносным кодом и другие. Рассмотрим некоторые способы защиты сайтов и противостояния внедрению вредоносного кода.

Свыше трех миллионов веб-страниц на 180 тысячах сайтов при заходе автоматически пытаются установить на компьютер пользователя вредоносные программы, говорится в отчете, составленном специалистами по безопасности Google. Большая часть вредоносного ПО хранится на китайских веб-серверах. На некоторые из таких серверов Google обнаружил до 21 тысячи ссылок с других сайтов

В данной работе рассмотрены такие актуальные угрозы безопасности, встречающиеся на веб-страницах, как XSS и IFRAME. Также приведены описания некоторых сопутствующих опасностях.

Цеью дано работы быо выявление и частичное рассмотрение признаков, на основании которых можно создать фильтр, препятствующий атакам XSS и IFRAME. Также рассмотрены некоторые признаки, помогающие найти ответ на вопрос: содержит сайт вредоносный код, или нет.

Анализ руткит технологий под операционную систему Linux

Кожанов Е.А., Степина А.Н.

Саратовский Государственный Социально-Экономический Университет
г. Саратов, Россия
v01and.bj@gmail.com; friackazoid@gmail.com

Rootkit analysis technologies under Linux operating systems

Kojanov E.A.,Stepina A.N.

Saratov State Socio-Economic University
Saratov, Russia
v01and.bj@gmail.com; friackazoid@gmail.com

In this work we analyze the main types of existing Linux rootkits. We also describe methods of detection a rootkit and give the assumptions about the future development of these technologies.

Целью данной работы было анализ имеющихся технологий руткитов, выявления их сильных и слабых сторон с целью предсказать дальнейшее развитие самих руткитов и методик борьбы с ними.

На сегодняшний день очень остро стоит вопрос защиты конфиденциальной информации пользователей. За этой информацией охотятся множество злоумышленников, используя вредоносные и шпионские программы, распространяя их по средствам всемирной сети Интернет и съемных носителей. Безопасность основывается на возможностях операционной системы, а возможности системы зависят от её ядра.

До сих пор считается, что одной из самых безопасных операционных систем является Linux, и что она полностью защищена от вредоносного и шпионского программного обеспечения, благодаря архитектуре ядра. Но правильность этого суждения стремится к нулю, прямо пропорционально с числом людей в него верящих. Сейчас в любых антивирусных базах найдется приличное число сигнатур зловредных программ, которые работают под данной операционной системой.

Благодаря появлению множества дружелюбных к пользователю дистрибутивов Linux, технологии зловредительства и хищения данных под эту платформу перестают иметь только исследовательский характер.

В результате исследований был сделан анализ основных существующих руткит технологий под операционную систему Linux, выявлены их сильные и слабые стороны. Основываясь на этих исследованиях была разработана и проверена своя технология внедрения в ядро Linux. Также были выдвинуты предположения о дальнейшем развитии технологий борьбы с подобными руткитами.

Метод проактивного обнаружения сетевых аномалий на основе реконструкции математической модели сетевого трафика

Копыстко А.Л., Саварцов А.В.

Ставропольский государственный университет
г. Ставрополь, Россия
kopystko@stavsu.ru

Method of proactive anomaly detection using a reconstructed mathematical model of network traffic

Kopystko A.L., Savartsov A.V.

Stavropol State University
Stavropol, Russia
kopystko@stavsu.ru

No one of moderns methods for network anomaly detection can give satisfactory results in sophicated networks. The causes are highly rates of multimedia traffic in today's WAN's and LAN's, slowness of statistical methods widely used in anomaly detection systems and the stochastic nature of teletraffic. This study analyzes present methods of network anomaly detection and proves a new method based on network traffic mathematical model reconstruction which should solve the problems faced by statiscial methods for detecting anomalities

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы уже давно применяются как один из необходимых рубежей обороны информационных систем. Исследования в области обнаружения атак ведутся за рубежом уже больше четверти века. Исследуются признаки атак, разрабатываются и эксплуатируются методы и средства обнаружения попыток несанкционированного проникновения через системы защиты, как межсетевой, так и локальной — на логическом и даже на физическом уровнях. В настоящее время наблюдается тенденция многократного увеличения скоростей передачи информации в Интернет каналах связи. В связи с этим *становится актуальной задача проактивного обнаружения аномальной сетевой активности в высокоскоростных каналах связи*. Успешное решение этой задачи позволит создать детекторы, позволяющие освободить ресурсы защитных механизмов сети от постоянной обработки значительных объёмов сетевого трафика до того момента обнаружения признаков вторжения. В свою очередь это освободит существующие методы сигнатурного анализа от ограничений по ресурсам, так как они будут активироваться только в случае возникновения потенциальных угроз.

Исследования современных статистических методов обнаружения аномалий (анализ функций распределения, корреляционный анализ, кластерный анализ) и выявили следующие слабые стороны:

1) Статистические методы детектирования сетевых аномалий не обладают достаточной надёжностью и эффективностью. Приемлемые характеристики достигнуты только при детектировании DoS атак.

2) Детектирование сетевых аномалий на основе методов математической статистики требует значительных вычислительных затрат.

3) Обнаружение сетевых аномалий в реальном масштабе времени практически невозможно, так как статистический анализ эффективен только при использовании достаточно больших выборок экспериментальных данных.

4) Статистический анализ предусматривает предварительное преобразование и обработку исходных данных. Однако, при этом не учитывается возможное наличие сетевых аномалий или враждебных действий в обучающей выборке телетрафика. Как правило, система обнаружения аномалий, обученная на таких данных, не будет выявлять такие инциденты.

В соответствии с проведённым анализом была сформулирована *цель работы*, предусматривающая *обоснование и разработку нового метода детектирования сетевых аномалий, основанного на методике реконструкции математической модели сетевого трафика*.

Результаты исследований математической модели сетевого трафика выявили свойства фрактальности и детерминированности процессов, проходящих в информационных сетях. Это говорит о возможности применения методов реконструкции нелинейных динамических систем для проактивного обнаружения аномалий в широкополосных каналах передачи данных. Данные методы позволяют получить математическую модель стохастического процесса по временному ряду экспериментальных данных, порожденному этой динамической системой. Следовательно, если реконструкция проведена корректно, то параметры математической модели, восстановленной по наблюдаемым данным должны отражать текущее состояние динамической системы, в нашем случае, канала связи. Отсюда, изменение состояния канала связи повлечет за собой изменение параметров реконструкции по временному ряду показателей сетевого трафика. Следовательно, можно говорить о возможности применения данной методики для выявления аномалий, возникающих в сетевом трафике.

Задача выявления аномалий предложенным методом выполняется в три шага:

1) Выбор оптимальных параметров реконструкции для восстановления аттрактора системы и выполнение реконструкции.

2) Идентификация параметров системы дифференциальных уравнений, описывающих восстановленный аттрактор.

3) Мониторинг изменения параметров уравнений реконструированной модели.

На первом этапе необходимо решить задачу выбора оптимальных параметров реконструкции: временной задержки τ и размерности вложения m. Результат реконструкции полностью зависит от выбора обоих параметров. Оценка оптимальных $\{m_{opt}, \tau_{opt}\}$ выполняется с помощью показателя дифференциальной энтропии, так как этот метод, в отличие от альтернативных, позволяет получить оба параметра одновременно. После определения параметров проводится востановление векторов состояния математической модели по экспериментальному временному ряду.

На втором этапе определяется вид уравнений математической модели и реконструкция их параметров. На заключительном этапе производится мониторинг параметров уравнений и при резком их изменении делается вывод о наличии аномалий в наблюдаемом процессе.

Процесс обнаружения аномалий описанным методом представлен на рисунке 1, состоящем из трёх графиков. Временной промежуток для всех графиков составляет 90 секунд и представлен на оси абсцисс. За этот временной отрезок, была предпринята попытка подмены одного из IP адресов Интерента в адресном пространстве Университета. Подмена была совершена на 14-й секунде данного временного промежутка, а на 73-й секунде атака была завершена.

Верхний график представляет собой оценку оптимальной размерности пространства m для вложения реконструируемой модели. Как видно из графика для реконструкции модели достаточно вложения в пространство размерностью не меньше двух. На графике не представлены отсчеты с 51-го по 90-й так как график в этой части временного промежутка не изменяет своего поведения.

На среднем графике представлена оценка оптимального параметра временной задержки τ необходимого на первом шаге реконструкции математической модели сетевого трафика. Данный параметр используется для эффективного построения модели и представлен на данном рисунке для первой части временного промежутка с целью демонстрации его независимости от событий, происходящих на этом временном промежутке.

На нижнем графике представлено пространство параметров реконструированной модели сетевого трафика. Ось апликат – порядковый номер параметров системы уравнений, описывающих математическую модель (здесь 10-ый – 18-ый параметры – соответственно 1-ый – 9-ый параметры второго уравнения), а ось ординат – значения параметров. Как показано на представленном графике на начало атаки указывает всплеск параметров уравнений на четырнадцатой секунде. Второй значительный всплеск параметров на семидесятой секунде соответствует завершению атаки.

Возмущения в районе 30-й, 40-й могут быть отнесены как к изменению состояния канала связи, так и к ложному срабатыванию, что говорит о необходимости дальнейшего изучения состояния потока сетевого трафика и параметров описывающей математической модели.

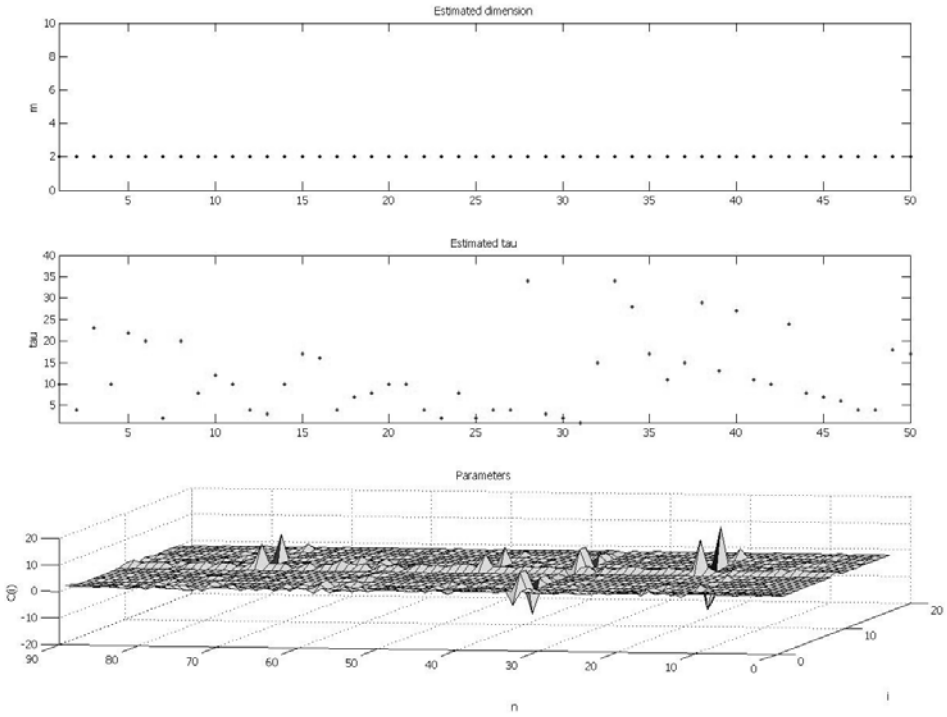


Рисунок 1 – Временная диаграмма параметров реконструированной модели атаки вида «подмена IP-адреса»

Таким образом, разработанный метод обнаружения сетевых аномалий позволяет выявлять атаки, возникающие в сетевом канале связи. Преимуществами изложенного подхода по сравнению с классическими статистическими методами являются:

1. Возможность обнаружения аномалий по коротким временным рядам параметров сетевого трафика. В соответствии с используемой методикой, для реконструкции состояния динамической системы необходимо всего около 5-6 отсчётов временного ряда параметров.
2. Отсутствие необходимости в предварительном преобразовании информации о сетевой активности. В качестве исходных данных достаточно использовать временной ряд, содержащий информацию о количестве пакетов, проходящих через магистральный канал в единицу времени.
3. Рассмотренный метод менее чувствителен к вычислительным затратам. Непрерывное вычисление параметров математической модели требует на много меньше системных ресурсов по сравнению с предварительной обработкой и статистическим анализом больших выборок данных.
4. Предложенный метод обнаружения сетевых аномалий по временным рядам одного из показателей состояния сети не требует наличия данных и времени для предварительного обучения системы обнаружения аномалий.

Учитывая сказанное выше, можно говорить о возможности использования разработанного метода в проактивном детекторе сетевых аномалий в магистральных каналах связи. Детектор может являться отдельным модулем системы обнаружения вторжений, позволяющим своевременно обнаруживать сетевые аномалии в канале связи. Такой элемент системы обнаружения вторжений может выполнять роль «тревожной кнопки», включающей, при обнаружении угрозы, дополнительные средства анализа сетевого трафика.

Литература

1. Лукацкий А.В. Обнаружение атак. – 2-е изд., перераб. и доп. СПб.:БХВ – Петербург, 2003. – 624 с.
2. Кенделл М. Временные ряды: Пер. с англ. и предисл. Ю.П. Лукашина. –М.: Финансы и статистика, 1981. – 199 с.
3. Гмурман В.Е. Теория вероятностей и математическая статистика. // Учеб. пособие для вузов. – Изд. 7-е, стер. – М.: Высш. Шк., 2001. – 480 с.
4. Орлов А.И. Прикладная статистика. Учебник. – М.: Экзамен, 2004. – 200 с.
5. Кузнецов С. П Динамический хаос (курс лекций). – М.: Физматлит, 2001. – 625 с.
6. Малинецкий Г.Г., Потапов А.Б. Современные проблемы нелинейной динамики. – М.: Едиториал УРСС, 2002. – 360 с.
7. Анищенко В.С. Знакомство с нелинейной динамикой. // Лекции соросовского профессора. – Саратов, 2000. – 144 с.
8. Безручко Б.П., Смирнов Д.А. Математическое моделирование и хаотические временные ряды. – ГосУНЦ «Колледж», Саратов, 2005. – 320 с.
9. Тезаурус уязвимостей. Common Vulnerabilities and Exposures. – http://www.cve.mittre.org
10. Нестеренко В.А. Статистические методы обнаружения безопасности в сети. // Информационные процессы. – 2006. том 6. №3. – С. 208 – 127.
11. S. Kim, S. Peker, B.Chan Detecting hackers(analyzing network traffic) by poison model measure. // Eighth PIMS-MITACS Industrial Problem Solving Workshop. – 2004. –P. 45-47.
12. Masaki Ishiguro, Hironobu Suzuki, Ichiro Measure Internet Threat Detection System Using Bayesian Estimation // Mitsubishi Research Institute. – 2004. – P. 12-17.
13. A. Wagner, B. Plattner. Entropy Based Worm and Anomaly Detection in Fast IP Networks // In Proceedings of IEEE International Workshop on Enabling Technologies, – 2005.
14. Chan P.K., Mahoney M., Arshad M.H. Learning Rules and Clusters for Anomaly Detection in Network Traffic // Managing Cyber Threats: Issues, Approaches and Challenges. – 2003.
15. Дружинин Е.Л. Разработка методов и программных средств выявления аномальных состояний компьютерной сети. // Диссертация на соискание учёной степени кандидата технических наук. – М., 2005.
16. Joshua McNull, Markus De Shon Correlation between quiescent ports in network flows // CERT Network Situational Awareness Group Carnegie Mellon University. – 2004.
17. Alexessander da Silva Couto Alves Internet Traffic Engineering An Artifactial Intellegence Approach : Disscrtation. – 2004.
18. Енюков И. Ретинская И., Скуратов А. Статистический анализ и мониторинг научно-образовательных Интернет-сетей. – М.: Финансы и статистика, 2004. – 467 с.
19. D. Marchette. A statistical method for profiling network traffic // In Proceedings of the Workshop on Intrusion Detection and Network Monitoring. –1999.
20. Лепёшкин О.М., Артамонов В.А. Обнаружение аномалий трафика канала связи по коротким временным рядам. – Научно-практический журнал «Противодействие угрозам терроризма»,№8, 2006 г. С.189-195.
21. Артамонов В.А., Лепешкин О.М. Подход к реализации сетевой системы обнаружения аномалий на основе реконструкции модели сетевого трафика. – Инфокоммуникационные технологии - Том 5, № 3, 2007, С. 145-147.

Обфускация

Коромысов С.Ю.

Самарский Государственный Аэрокосмический Университет
Самара, Россия
x_rash_x@list.ru

Obfuscation

Koromysov S.Y.

Samara State Space University
Samara, Russia
x_rash_x@list.ru

Быстрое развитие мультимедиа и Интернет технологий в последние годы вызывает потребность в защите такой интеллектуальной собственности, как программные продукты (ПП).

Разработка наиболее эффективного метода защиты для того или иного программного продукта, в нынешнее время, становиться одной из важных задач большинства программистов, которые занимаются разработкой специализированного, платного программного обеспечения (ПО), так как это позволяет им продавать свой интеллектуальный труд, и исключить возможности его нелегального использования среди потребителей, говоря иными словами, пользователь не сможет использовать оригинальную, лицензионную копию определенной программы предварительно не купив, не заплатив денег её разработчику.

Затраты производителей на создание эффективного метода защиты их программных продуктов окупаются и компенсируют потенциальный ущерб, наносимый нелегальным копированием и использованием программ.

Служба реагирования предприятия на инциденты компьютерной безопасности

Космачев А.В.

Томский государственный университет систем управления и радиоэлектроники
г. Томск, Россия
kosmachev@ms.tusur.ru

Enterprise response service to incidents of computer safety

Kosmachev A.V.

Tomsk state university of control systems and radio electronics
Tomsk, Russia
kosmachev@ms.tusur.ru

In process of increase of role ИТ the requirement for maintenance of corresponding level of service, maintenance of maximum availability ИТ grows in the company - services. The business user should have possibility to work at any time and to receive the decision of the problems if they have arisen, as soon as possible.

The purpose of the given work is consideration of existing techniques of construction of services of reaction to incidents of safety and realisation at the enterprise.

CSIRT (Computer Security Incident Response Team) - service which is responsible for reception, consideration, and reaction to messages on incidents of computer safety.

In process of increase of role ИТ the requirement for maintenance of corresponding level of service, maintenance of maximum availability ИТ grows in the company - services. The business user should have possibility to work at any time and to receive the decision of the problems if they have arisen, as soon as possible.

Possibility at occurrence of problems to address in corresponding service on the native language, especially for the user who is not the highly skilled expert, it can appear a situation of incident solving for the successful permission. Adding to it absence of expenses on the international telephone conversations, uniform time zone (so also uniform working hours), possibility in need of departure of group of experts on a place, uniform is standard-legal space and other factors, becomes clear, that the national Service of reaction to incidents possesses conclusive advantage before use of alternative services.

The purpose of the given work is consideration of existing techniques of construction of services of reaction to incidents of safety and realisation at the enterprise.

The problem of reaction to incidents of information safety (ИБ) and their investigations is today simultaneously and popular, and the most scrupulous. During investigation and reaction to incident are shown concrete vulnerability of information system, traces of attacks and intrusions are found out, work of protective mechanisms, quality of architecture of system IB and its management is checked.

In general, in Russia there is variety of serious problems in this area: there is no uniform centre of registration of incidents, the legislation lags behind, there are no open techniques and standards of the organisation of process of reaction and investigation of incidents ИБ. Where to address the company which have sustained losses as a result of ill-intentioned computer incident? How it is possible to be prepared for such events what preventive measures on prevention of incidents exist? Abroad already there are the standards describing process of reaction to computer incidents.

Despite consecutive structure of a statement of stages service creation, at acquaintance with sources arises not clear representation about stages of formation of services. Other technique of creation of a command of reaction to incidents of computer safety therefore is offered.

Incident - this certain event which is not standard operation which interrupts the normal functioning of the system fixed by automated systems of monitoring and control ИТ - infrastructures, compelling users to address in the centre of support of software developers.

Group CSIRT should:

- to carry out monitoring of systems for the purpose of revealing of infringements of safety;
- to serve as the centre of an information exchange, processing arriving reports on incidents in sphere of safety and dispatching to the major data about them to corresponding instances;
- to document and catalogue incidents in safety sphere;
- to raise level of knowledge of employees of the company about safety maintenance, thereby reducing probability of new incidents in the organizational environment;
- to make the analysis уязвимостей and check on penetration;
- to collect data about new уязвимостях and strategy of the attacks practised by malefactors;
- to study the newest corrections ON;
- to analyze and develop new techniques of minimisation of risks and уязвимостей safety systems;
- to render advisory services in safety issues;
- regularly to correct and update existing systems and procedures

CSIRT (Computer Security Incident Response Team) – служба, которая является ответственной за получение, рассмотрение, и реагирование на сообщения об инцидентах компьютерной безопасности.

По мере возрастания роли ИТ в компании растет потребность в обеспечении соответствующего уровня сервиса, обеспечении максимальной доступности ИТ - услуг. Бизнес-пользователь должен иметь возможность работать в любое время и получить решение своих проблем, если они возникли, как можно быстрее.

Возможность при возникновении проблем обратиться в соответствующую службу на родном языке, особенно для пользователя, не являющегося высококвалифицированным специалистом, может оказаться решающей для успешного разрешения ситуации инцидента. Добавляя к этому отсутствие расходов на международные телефонные переговоры, единый часовой пояс (а значит и единые рабочие часы), возможность при необходимости выезда группы специалистов на место, единое нормативно-правовое пространство и другие факторы, становится понятно, что национальная Служба реагирования на инциденты обладает неоспоримым преимуществом перед использованием альтернативных служб.

Целью данной работы является рассмотрение существующих методик построения служб реагирования на инциденты безопасности и реализация на предприятии.

Проблема реагирования на инциденты информационной безопасности (ИБ) и их расследования является сегодня одновременно и популярной, и самой щепетильной. Именно во время расследования и реагирования на инцидент проявляются конкретные уязвимости информационной системы, обнаруживаются следы атак и вторжений, проверяется работа защитных механизмов, качество архитектуры системы ИБ и ее управления.

Вообще, в России существует целый ряд серьезных проблем в этой области: нет единого центра регистрации инцидентов, отстает законодательство, нет открытых методик и стандартов организации процесса реагирования и расследования инцидентов ИБ. Куда обращаться компании, потерпевшей убытки в результате злоумышленного компьютерного инцидента? Как можно подготовиться к такого рода событиям, какие существуют превентивные меры по предотвращению инцидентов? За рубежом уже существуют стандарты, описывающие процесс реагирования на компьютерные инциденты.

Несмотря на последовательную структуру изложения этапов создание службы, при ознакомлении с источниками возникает не ясное представление о этапах формирования служб. Поэтому предлагается другая методика создания команды реагирования на инциденты компьютерной безопасности.

Инцидент- это некое событие, не являющееся стандартной операцией, которое прерывает нормальное функционирование системы, зафиксированное автоматизированными системами мониторинга и контроля ИТ - инфраструктуры, вынуждая пользователей обращаться в центр поддержки разработчиков программного обеспечения.

Группа CSIRT должна:

- проводить мониторинг систем с целью выявления нарушений безопасности;
- служить центром информационного обмена, обрабатывая поступающие отчеты о происшествиях в сфере безопасности и рассылая важнейшие данные о них соответствующим инстанциям;
- документировать и каталогизировать происшествия в сфере безопасности;
- повышать уровень знаний сотрудников компании об обеспечении безопасности, тем самым уменьшая вероятность новых происшествий в организационной среде;
- производить анализ уязвимостей и проверку на проникновение;
- собирать сведения о новых уязвимостях и стратегиях атак, практикуемых злоумышленниками;
- изучать новейшие исправления ПО;
- анализировать и разрабатывать новые методики минимизации рисков и уязвимостей системы безопасности;
- предоставлять консультативные услуги по вопросам безопасности;
- регулярно корректировать и обновлять существующие системы и процедуры.

Создание унифицированного средства защиты от угроз

Кукало И.А.

Томский государственный университет систем управления и радиоэлектроники
г. Томск, Россия
i@kukalo.ru

Creation of a unified threat management system

Kukalo I.A.

Tomsk state university of control systems and radioelectronics
Tomsk, Russia
i@kukalo.ru

Unified threat management (UTM) is used to describe network firewalls that have many features in one box, including e-mail spam filtering, anti-virus capability, an intrusion detection (or prevention) system (IDS or IPS), and World Wide Web content filtering, along with the traditional activities of a firewall. Main goal of this research is to create own open-source based UTM system, that has almost all capabilities as their commercial analogs.

Унификация захватывает самые различные области ИТ, и отрасль ИБ не является исключением. Многие эксперты предсказывают комплексным устройствам управления защитой от угроз большое будущее [1]. Главная цель данной работы создание системы UTM (унифицированного управления защитой от угроз), на базе свободного программного обеспечения (СПО) [2] с открытым исходным кодом, а также оценка и сравнение системы с ее коммерческими аналогами. Данное устройство ориентировано на потребителей из сегмента малого и среднего бизнеса, где особо важно использование устройств с минимальной стоимостью, простыми и гибкими механизмами внедрения и эксплуатации.

В настоящее время системы UTM включают следующие механизмы защиты [3]:

- МСЭ. Разграничивает доступ к внутренним и внешним ресурсам, участвует в аутентификации пользователей и аудите событий на контролируемом пространстве;
- Система обнаружения/предотвращения атак. Анализ сетевой активности и выявление аномалий;
- Средство построения VPN. Обеспечивает конфиденциальность данных, передаваемых по незащищенным каналам связи;
- Система контроля доступа к интернет-сайтам (фильтрация URL). Реализует политику безопасности доступа к ресурсам сети Интернет.
- Антивирус и подсистема защиты от шпионского ПО. Выявление вредоносного ПО в наиболее распространенных протоколах - HTTP, SMTP, FTP и POP3;
- В качестве дополнительных опций, в таких системах часто используются:
- Система контроля электронной почты. Позволяет отслеживать утечку по e-mail за пределы контролируемого периметра конфиденциальной информации;
- Антиспам. Предотвращает несанкционированные, массовые рассылки.

На начальном этапе разработки, особое внимание было уделено анализу рынка систем UTM, который позволил выявить следующее:

- Коммерческие производители систем UTM, повсеместно используют СПО, это и ОС Red Hat (продукция компании CheckPoint), и ОС FreeBSD (продукция компании Информзащита, Juniper Networks) и т. д.;
- На рынке СПО не существует успешных реализации систем UTM, сравнимых по функциональности с коммерческими аналогами, хотя стоит заметить наличие большого количества успешных реализаций отдельных составляющих систем UTM.;
- Высокая стоимость коммерческих реализаций систем UTM, затрудняет использование продукции в сфере малого и среднего бизнеса, которые обладают ограниченным бюджетом на ИБ;

Таким образом, было принято решение об использовании наиболее удачных реализаций продуктов СПО в собственной реализации системы UTM. Главными требованиями к используемому ПО были выдвинуты его стабильность, функциональность, а так же техническая поддержка. Реализованное комплексное устройство включает в себя лучшие наработки рынка СПО и является максимально совместимым с ПО сторонних производителей за счет использования стандартных протоколов IPSec, PPTP, ICAP, X.509, LDAP и т. д. Использование криптографических средств ограничено зарубежными, но наиболее распространенными алгоритмами шифрования - DES, 3DES, Blowfish, AES, алгоритмам хеширования - MD5, MD4, SHA-1, SHA-2, а так же алгоритмами реализации ЭЦП - RSA, DH, DSA. Использование российских криптографических алгоритмов присутствует на экспериментальном уровне и не является необходимым для целевой аудитории системы UTM.

Формальные требования по уровню защиты от НСД в соответствии с нормативной документацией: до 1Г, соответствие применяемого МСЭ требованиям четвертого класса защищенности, соответствие применяемых СВТ требованиям шестого класса защищенности.

Структурная схема СБ представленная на рисунке 1. ПО используемое в СБ, является бесплатным и свободно распространяемым и позволяет обеспечить следующую функциональность:

- Защита внутреннего периметра от вредоносного и шпионского трафика;
- Объединение филиальной сети территориально разрозненной организации в единую ЛВС;
- Защита внутреннего периметра от НСД со стороны злоумышленников;
- Контроль целостности системы UTM, расположенной удаленной территориально;
- Оптимизация и контроль использования ресурсов сети Интернет;
- Генерирование и обслуживание криптографических сертификатов.

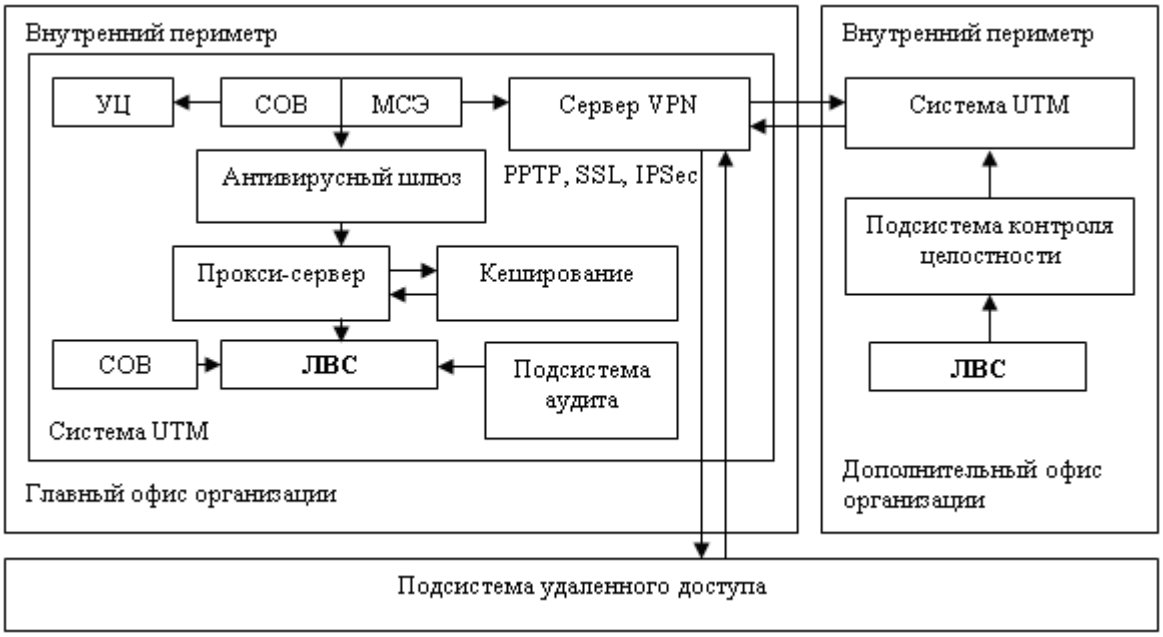


Рис. 1. Структурная схема СБ

В дальнейших планах интеграция в проект модуля по борьбе со спамом, а так же создание упрощенного интерфейса управления, для этого в состав СБ включена поддержка разработок на языке Java (ПО Apache+Tomcat).

Управление системой UTM осуществляется с помощью командной строки (по протоколу SSH) и большого количества документированных конфигурационных файлов, реализующие различные сценарии применения СБ (см. рисунок 2). Распространение ПО осуществляется по средствам использования мультиплатформенных загрузочных дистрибутивов, а так же по средствам установки дистрибутива на ОС FreeBSD. Предусмотрена сетевая версия установки системы.

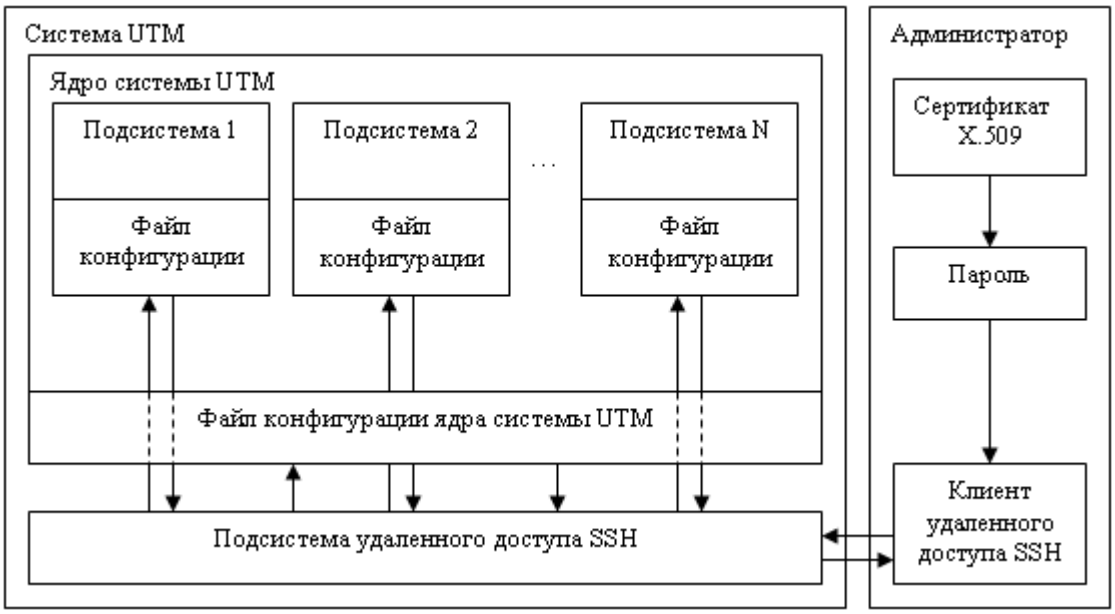


Рис. 2. Структурная схема управления системой UTM

Для оценки эффективности предложенной СБ было произведено категорирование информации подлежащей защите для типовой организации, и методом экспертной оценки [7] произведен анализ рисков до и после внедрения СБ. В процессе категорирования, были выделены следующие классы информации:

- открытая информация;
- конфиденциальная информация:

  – информация, составляющая коммерческую тайну – конфиденциальная информация, дающая преимущество предприятию в сфере его коммерческой деятельности в силу ее неизвестности третьим лицам и защищаемая предприятием;

  – информация для служебного пользования – сведения, разглашение которых может стать причиной нарушения режима безопасности или нанести ущерб предприятию, его сотрудникам или контрагентам, кроме сведений, охраняемых другими законами;

  – персональные данные – информация о сотрудниках, в том числе паспортные данные, адреса, семейное, социальное, имущественное положение, образование, профессия, другая информация.

Определение угроз безопасности проводилось в соответствии с ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» [8], согласно которому можно выделить два типа угроз безопасности:

- связанные с неконтролируемым распространением защищаемой информации – утечкой (разглашение, разведка, НСД);
- связанные с несанкционированным воздействием на информацию и ее носители (воздействие с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации).

В качестве экспертов привлекались начальник отдела ИТ, а так главный специалист службы безопасности филиала Газпромбанк (ОАО) в г. Томске.

Применение спроектированной системы защиты позволило снизить рассчитанные информационные риски до уровня приемлемых. В среднем снижение уровней высоких и средних рисков составило:

- Для информации составляющей коммерческую тайну 78 %;

- Для информации служебного пользования 69 %.

Более подробные результаты снижения рисков приведены в таблице 1.

Таблица 1 – Результаты снижения уровней высоких и средних рисков

Информация	Угроза	Снижение, %
Коммерческая тайна	НСД с последующей утечкой	66
	Модификация информации (уничтожение, искажение, блокирование)	88
	Модификация информации (подделка)	75
Информация для служебного пользования	НСД с последующей утечкой	50
	Модификация информации (уничтожение, искажение, блокирование)	83
	Дезорганизация функционирования АС	75

ЛИТЕРАТУРА

1.Орлов С. Один за всех / С.В. Орлов // LAN, журнал сетевых решений. – 2006. – № 7.
2.Концепция развития разработки и использования свободного программного обеспечения в Российской Федерации [Электронный ресурс]. – Электрон. дан.: Нормативные документы Министерства информационных технологий и связи – Режим доступа: http://www.minkomsvjaz.ru/upload/docs/20080314101749IP.rtf
3.Лукацкий А.В. Системы защиты «все в одном»: как объять необъятное/ А.В. Лукацкий // Connect! Мир связи. – 2006. – № 7.
4.Покровский П. Анализ рисков / П. Покровский // LAN, журнал сетевых решений. - 2004. – № 10.

Активная система обнаружения опасных серверов

Логинов В.В.

Московский инженерно-физический институт
г. Москва, Россия
passvvordoff@gmail.com

Active system for detecting dangerous servers

Loginov V.V.

Moscow Engineering Physics Institute
Moscow, Russia
passvvordoff@gmail.com

Objects:

Object of this research is a Client Honeypot (Active System of Detection Dangerous Servers, further ASDDS) programs.

Object is research and simulate work of ASDDS program.

In work process experimental research of auditing was executed in OS Windows XP. Changes in registry and file system was observed in case work in Internet, for goal of determine processes which are infects computer and further observation active of malicious program.

This area not researched fully by reason of new theme, also there not found any publication on Russian language, therefore work had made have scientist and practice value.

Results:

In course of work test of program model is successful executed on the study mold, which was created beforehand. Also in course of research infected web-site was found. System had revealed it efficiency in that case. Every result was saved and analyzed.

Structure and classification of ASDDS program was made out, also was explored specification for architecture of program and it's work.

Classification of system based on type and level of interaction, was submitted. Architecture and working of program made out. Advantages and disadvantages of different functions and variants of realizing and applying of system are considered for different kind of system. Demands for developing are revealed. Approach for rating was offered. Algorithm of work was simulated.

Applicability:

Programs of this type may be applied in area of analysis of dangerous in network, and also determining of dangerous servers and malicious software. Results of work system can be applied for further develop defense and in time notice users about danger. In creation of ASDDS interested antivirus companies and big servers, like hosting, e-mail servers, internet providers etc.

Цели:

Объектом данного исследования являются Client Honeypot (Активная Система Обнаружения Опасных Серверов, в дальнейшем АСООС) программы.

Целью является изучить и смоделировать работу АСООС программы.

В процессе работы проводились экспериментальные исследования ведения аудита в ОС Windows XP. Наблюдались изменения в реестре и в файловой системе в ключе работы в сети Интернет, с целью обнаружить процесс заражения и дальнейшие действия вредоносных программ.

Данная область на сегодняшний день исследована не полностью по причине новизны темы, к тому же не было найдено ни одной публикации на русском языке на тему подобного рода, поэтому проведенная работа имеет научную и практическую ценность.

Результаты:

В ходе работы были проведены успешные испытания модели программы на учебном муляже созданном заранее. Так же в ходе исследований был обнаружен реальный рабочий вариант зараженной веб-страницы. Система также проявила эффективность в ходе ее испытания в таких условиях. Все результаты работы были сохранены и проанализированы.

Детально разобрана структура АСООС программы, и их классификация выявлен ряд требований к архитектуре программы и ее работе.

Представлена классификация систем по типам и уровню взаимодействия. Детально разобрана архитектура и функционирование АСООС. Рассмотрены преимущества и недостатки различных функций и вариантов реализации, а также области применения различных видов системы. Выявлен ряд требований к разработке АСООС. Определен подход к оценке качества системы. Смоделирован алгоритм работы.

Применимость:

Программы описанного типа применимы в сфере исследований опасности работы в сети, а также обнаружения опасных серверов и вредоносных программ. Результаты работы системы подобного рода применимы для последующей разработки защиты, а также своевременного предупреждения пользователей о потенциальной опасности. Созданием АСООС заинтересованы, в основном, антивирусные компании и крупные сервера, в том числе различные хостинги, почтовые серверы, провайдеры итп.

Автоматизированная система защиты сайта, разработанного на языке программирования PHP с использованием сервера баз данных MySQL, от атак типа SQL-инъекция, PHP-инъекция и межсайтовый скриптинг лужба реагирования предприятия на инциденты компьютерной безопасности

Приходько М.А.

Институт Государственного Управления, Права и Инновационных Технологий
г. Москва, Россия
spex19@mail.ru

An automated security system for a web-site developed using PHP and MySQL, protecting against SQL-injection, PHP-injection and Cross Site Scripting

Prihodko M.A.

Institute of Public Administration, Law and Innovation Technologies
Moscow, Russia
spex19@mail.ru

Annotation: This work describes the mechanism of the automated security system of the web-site developed with the usage of PHP and MySQL, protecting from SQL-injection, PHP-injection and Cross Site Scripting. The weak spots of “black-list” filter are discussed and the solutions for these problems are given.

Язык web-программирования PHP и сервер баз данных MySQL – чаще всего используемая на сегодня «связка» технологий для разработки web-сайтов. Как и в любой другой сфере, у такой распространенности есть обратная сторона – web-сайты, разработанные по схеме PHP+MySQL, привлекают наибольшее внимание злоумышленников, а методы их взлома совершенствуются каждый день.

Web-сайты, разработанные на языке PHP с использованием СУБД MySQL, уязвимы для атак типа **SQL-инъекция**, **PHP-инъекция** и **межсайтовый скриптинг**. Эти атаки затрагивают **все** аспекты работы с web-сайтом – сервер СУБД, файловый сервер, на котором выполняется интерпретатор PHP, и даже клиентскую машину, на которой выполняются Javascript-скрипты. **Децентрализованная** проверка переменных в условиях бурно развивающегося или просто очень крупного проекта неизбежно приводит к возникновению «дыр» в коде, которые незамедлительно атакуются. Поэтому необходима проверка переменных **не в каждом конкретном случае**, а **в самом начале каждой PHP-страницы**, причем проверка автоматизированная и унифицированная. Эта проверка должна осуществляться специальной системой безопасности, которая будет не только обнаруживать и блокировать атаки, но и уведомлять о них администратора web-сайта, а также протоколировать все несанкционированные действия посетителей web-сайта.

Система безопасности **geneGuard** построена на основе интеллектуального механизма фильтрации по принципу «черного списка», когда запрещается использование определенного набора слов. При формировании HTML-текста страницы модуль безопасности производит проверку переменных, передаваемых методами **GET** и **POST** – в тексте значения переменной ведется поиск одного из запрещенных слов. Если атака не была обнаружена, используется оригинальное значение переменной. **Если атака была обнаружена, переменная аннулируется**, а вся информация об атакующем и самой атаке протоколируется в базе данных.

Для борьбы с *PHP-инъекцией* **в начале параметра** (первые 4 символа) выявляется наличие слова *http*, которое трактуется как **подозрение** на выполнение *PHP-инъекции*. В этом случае в начало

значения автоматически добавляется слово "*ссылка:* ", а администратор получает предупреждение о **возможной** попытке атаки типа PHP-инъекция.

Добавляемое слово "*ссылка:* " позволяет, во-первых, в случае **реальной атаки** ее нейтрализовать, а во-вторых, в случае **корректной** (а значит безопасной) ссылки ее сохранить, не нарушив при этом смыслового содержания значения параметра.

Фильтрация атак типа **межсайтовый скриптинг** производится по словам <script> и </script>.

Фильтрация атак типа **SQL-инъекция** производится по целому перечню запрещенных слов, состав которого зависит от конкретного защищаемого сервера СУБД (в нашем случае – MySQL). Для обработки «пограничных» ситуаций (значений вида "**select***ion*", часть которых является командой языка SQL) после обнаружения запрещенного слова проверяются предыдущий и следующий за словом символы. Окончательное блокирование происходит в случае подтверждения обнаружения «отдельно стоящего» слова, окруженного специальными символами (пробел, скобка, * и другие). Список таких «сигнальных» символов для каждого запрещенного слова может отличаться и хранится в настройках системы безопасности. В тех случаях, когда это возможно, дополнительно производится анализ на наличие целой «структуры» SQL-запроса, например за словом *select* должно следовать слово *from*.

Для борьбы с наиболее распространенными методами «обхода» фильтров перед анализом производится унификация значений переменных. Во-первых, *значение параметра предварительно анализируется на наличие hex-кодов, которые преобразуются в кодировку ascii*. Во-вторых, *перед сравнением значение параметра и запрещенного слова принудительно переводятся в один и тот же регистр* (верхний или нижний).

Еще один способ «изменить» код атаки заключается во внедрении **комментария**, который позволит скрыть запрещенное слово от фильтра, одновременно выполнив атаку (например, ***s/*comment*/elect***). Для борьбы с ним «начало» и «конец» комментария могут быть внесены в список в качестве запрещенных слов. Вторым способом борьбы с подобными действиями может быть модификация механизма унификации значений переменных, в который добавляется этап «вырезания» подобных «комментариев».

Система безопасности geneGuard внедрена на четырех web-сайтах различной тематики:

- электронный журнал www.elenoize.com;
- сайт научного фонда и научной конференции www.ikf2008.ru;
- сайт музыкального лейбла www.elenoize-records.com;
- сайт Автоматизированной системы интерактивного контроля знаний «Аргус-М») www.argusm.com.

Анализ работы системы на этих сайтах позволяет сделать следующие выводы:

- *система безопасности с фильтрацией по принципу «черного списка»* **не приводит** *к излишне «жесткой» фильтрации в условиях использования ее на русскоязычном сайте и может быть использована без изменений для защиты сайтов различной тематики*;
- *существующие методики обхода систем безопасности, построенных по принципу «черного списка», естественным образом предлагают механизмы защиты, которые встраиваются в единую технологию путем добавления специального вида запрещенных слов, используемых для сокрытия атак.*

Система geneGuard функционирует с мая 2008 года по настоящее время (март 2009 года). За этот период выявлено более 80000 (84909!) различных действий, которые были расценены как несанкционированные. Из них около 2000 приходится непосредственно на атаки типа SQL- и PHP-инъекция (остальные являются результатом работы различных «ботов»). Это еще раз подтверждает актуальность проблемы и явным образом указывает на ее важность.

Система безопасности geneGuard распространяется **свободно** и **бесплатно**. Подробнее познакомиться с системой, а также скачать базовые исходные коды можно на сайте автора: http://www.argusm.com/article.php?id=158

Проактивные методы защиты

Рашевский Р.

МОУ СОШ №146
г. Пермь, Россия
virus-bulletin@yandex.ru

Proactive methods of protection

Rashevsky R.

School №146
Perm, Russia
virus-bulletin@yandex.ru

История компьютерных вирусов насчитывает уже более 25 лет. Неразрывно с вирусами развивались и средства противодействия вирусам – антивирусы. Исторически сложилось так, что лидерство на рынке антивирусных технологий заняли системы сигнатурного поиска, иначе называемые реактивными. Данные системы, несмотря на кажущуюся простоту реализации и надежность, имеют ряд существенных недостатков, а именно:

- Слабая эффективность против угроз типа 0-day[1], так как эффективность напрямую связана с базой сигнатур вредоносного ПО, в которую внесены сигнатуры только известного, на данный момент, вредоносного ПО;
- Необходимость постоянного обновления базы сигнатур вирусов для эффективной защиты от нового вредоносного ПО;
- Для определения вредоносного ПО необходима процедура сканирования, которая отнимает достаточно много времени и системных ресурсов.

Данные причины и послужили толчком к развитию т.н. проактивных систем защиты, о которых и пойдет речь в данной работе.

[1] Угроза 0-day – только что созданная угроза.

Защита программных продуктов: методы обфускации и деобфускации программного кода. Деобфускация вредоносного кода, написанного на JavaScript

Рой К.С.

Пермский Государственный Университет
г. Пермь, Россия
kostyanroy@mail.ru

Protection of software products: methods of obfuscating and deobfuscating a program code. Debfuscation of harmful code written on JavaScript

Roy K.S.

Perm state university
Perm, Russia
kostyanroy@mail.ru

This article is about modern methods obfuskation and deobfuskation in programs. Scientific work involves the development of techniques deobfuskatstion malicious code which written on javascript-language.

At present, there is a pressing problem of intellectual protection of the products, arisen before the companies engaged in production and sale of software for personal computers. Even more pressing problem is arisen, in case of protection of those programmes, which are not compiled in an executable file, but delivered the end users as a code interpreted during execution of the programme.

Various techniques of code "entanglement" are applied for such purpose. *Obfuscation* (from the English obfuscation – literally means "entanglement") is a name given to a group of techniques and the means targeted at impediment of the analysis of program code [1]. In this work, the analysis of various types of obfuscators is carried out:

- obfuscators, entangling the code written in interpreted languages, such as Perl or PHP. Techniques are considered, starting from the simplest, such as removal of comments and replacing the names of variables with senseless ones, to complex, such as encryption of line constants, introduction of semantically insignificant constructions, and considerable increase of the body of the programme, with numerous transitions.
- obfuscators, analysing and transforming byte-code of virtual machines Java and .NET.

It is self-evident, that as a result of entangling, the programme can appear to be slower during execution, and also frequently it can become larger in terms of volume. For the purpose of evaluation of the operation of the programme-obfuscator, the value is introduced, such as cost. *The cost of* transformation [3] is a metrics, which allows to evaluate, to what extent more resources would be required (memory, processor time) for execution of the entangled programme, than for execution of the source programme. The cost is determined using the following scale:

- free-of-charge transformation – increases expenses of resources of the entangled function by O(1),
- cheap transformation – increases expenses of resources by O(m), where m is the size of entangled function,
- moderate cost transformation – increases expenses of resources of the entangled function by O(mp), where $p > 1$,
- expensive transformation – exponentially increases expenses of resources of the entangled function in comparison with the initial one.

According to [3], it is possible to mark four basic types of entangling transformations:

1. *transformations of formatting* which only change appearance of the programme. Transformations deleting comments, indents in the text of the programme, or renaming identifiers, are related to this group;

2. *transformations of structures of the data*, changing structures of data with which the programme operates. This group includes, for example, transformation changing hierarchy of inheritance of classes in the programme, or transformation uniting scalar variables of one type into an array;

3. *transformations of control flow of the programme,* which change the structure of its graph of control flow, such as development of cycles, allocation of fragments of the code into procedures, and other similar actions;

4. *preventive transformations* aimed against certain methods of decompiling of programmes, or using errors in certain tools of decompiling.

When we speak about the process of obfuscation, a question arises: whether there is a process reverse to it, which would allow trespasser to return the most similar initial code of the programme, that is the code existed before the obfuscation? It is difficult to give unequivocal answer to this question, but such process exists and it has the name of de-obfuscation. But another, not less important question, is how can it be realised [2].

In the first and the second parts of this work, it is examined, what are these two mutually opposite (but not mutually convertible) processes – obfuscation and de-obfuscation. The analysis of stability of entangling algorithms is given, in relation to the various methods of disentangling, and possibility or impossibility of automation of untangling transformations is also shown.

In the third part of the work, the variants of distribution and concealment of harmful code in HTML-pages are analysed, and development has been started, of theoretical basis and practical realisation for creation of a tool for de-obfuscation of harmful code, latent in the scenarios of HTML-page, since with the help of obfuscation, the trespassers very frequently try, if not to make impossible, then to complicate as much as possible, parsing of their virus. As the language, JavaScript was chosen, since according to the data from *viruslist.com* [4], the amount of nocuous code in JavaScript has increased by 48%, which is the biggest growth among all interpretable languages. Accordingly, the given language is also the one, most subject to the various methods of obfuscation.

Based on the results of the accomplished work, composition of the tool includes:

1. *module for parsing of HTML-page.* This module is responsible for parsing of HTML-page received at the input, into a frame network of tags. The decision about creation of a separate module (instead of using of ready toolkit) was made because of some specificity of representation of the page, associated with de-obfuscation of the very Web-page. In future, probably, it will be decided to use a third-party parser, and the essence of the given module will consist in converting the results into the required form;

2. *module for collecting the entire JavaScript-code into common base.* The given module is necessary for extraction of JavaScript-code necessary for us, from parsed HTML-code;

3. *module for loading of missing JavaScript-code.* For creation of a full picture, presence of the entire code is necessary;

4. *module for parsing of JavaScript-code.* For presentation of all variables, constants, functions and other construction of the language in the form of dynamic structure. Use of ready JavaScript-parsers is possible;

5. *module for de-obfuscation.* Directly the module for de-obfuscation of JavaScript-code, the development of which, as a matter of fact, is also one of the basic purposes;

6. *module for de-obfuscation.* As a necessity for testing, and also as desirable collateral action, code entanglement module will be written.

7. *module for general logging.* Each module will leave the own logs, the purpose of the given module is drawing up general report about the work done. Further, it is planned to start creation of module whose purpose will be auto-signing of the actions of the programme (that goes without saying, as it was already said earlier, the task of recognising of the semantics of the programme based on its syntax is algorithmically insoluble; the prospective module will perform this task only in part).

It is possible to relate indirectly to the process of de-obfuscation, the process of optimisation of programme code, since both of them, to some extent, are opposite to the process of obfuscation. During the process of obfuscation, addition of superfluous operations into programme code is frequently made; they usually do not influence at all the results of execution of the programme, and are intended to confuse and complicate the process of examination of code of the programme by third parties. In turn, the process of optimisation of the programme code is targeted at elimination of superfluous operations; therefore in special cases it can represent itself as a quintessence of the process of de-obfuscation [2].

Let us consider classification of methods of the process of de-obfuscation (according to [2]):

- Finding and evaluation of non-transparent constructions (predicates), static analysis of which is very complicated.
- Comparison against the sample. It is carried out by various ways; two of them are most commonly used.
- The first one, is when a number of same programmes is taken, which have passed the process of obfuscation (since the process of obfuscation in most cases is unique, then their code would also be different, though they would still carry out identical actions) and comparison of fragments of their code is made, for revealing of superfluous code inserted during realisation of obfuscation, which code is simply removed afterwards.
- The second way of comparison against the sample is carried out by means of search, in the code of the programme, of the most widespread constructions, used in the process of obfuscation. Such constructions can, for example, be stored and updated in the corresponding database, or be obtained by means of examination of the operation of the obfuscator itself.
- Allocation of fragments of code in the programme, which fragments are in no way associated with the primary goals, which the programme should fulfil, that is detection of unnecessary (superfluous) sectors of the code.
- Statistical analysis, consists in dynamic analysis of the code of the programme. For example, finding of non-transparent predicates can be carried out by allocation and further examination, in the analysed code of the programme, of those predicates, which during execution of analysis, always return the same value. Statistical analysis can also be used for evaluation of correctness of the implemented process of de-obfuscation, for that purpose, the programme "A" and the programme obtained as a result of de-obfuscation of "A`" are started in parallel, these are given equivalent input data, and a comparison is made, of the output data. If the output data is identical, it is possible to assume, that the process of de-obfuscation has been carried out correctly.
- The dataflow analysis is based on studying of how during the work of the programme, the data is changed in it (variables, arrays).

Since the theory of obfuscation very actively develops at present, and all the time, new, more advanced methods of entanglement are being invented, I believe, that the created tool for analysis and disentangling of code would appear tom be very useful for disentangling these new methods. In the given work, JavaScript was proposed as the language, but the theory stated above can well be transposed to some other interpretive programming language, with several rare exceptions (it is supposed to use the features of JavaScript considered above, for the process of de-obfuscation in individual single instances).

At present in the modern open literature there are very few works seriously engaged in the process of de-obfuscation, partly because of the fact, that this process could only poorly be automated, and only those who either "crack" software that belongs to others, or try to penetrate into essence of code, are engaged in the said process. Therefore the problem of de-obfuscation is topical. And if one could manage to use the obtained results for the good, as for example, the author has tried to, then the task becomes claimed.

LITERATURE

5. Koller "Процесс обфускация, его алгоритмы, процесс деобфускации" [статья на форуме], http://rootaccess.info/index.php?showtopic=2029&pid=10132&mode=threaded&start= (ссылка действительна на 1 января 2009).

6. LynX "Обфускация и защита программных продуктов" [электронный документ], http://www.citforum.ru/security/articles/obfus/ (ссылка действительна на 1 января 2009).

7. Чернов А. В. "Анализ запутывающих преобразований программ" [электронный документ], http://www.citforum.ru/security/articles/analysis/ (ссылка действительна на 1 января 2009).

Kaspersky Security Bulletin 2008. Развитие угроз в первом полугодии 2008 года [электронный документ] http://www.viruslist.com/ru/analysis?pubid=204007623 (ссылка действительна на 1 января 2009).

В настоящее время перед компаниями, занимающимися производством и продажей софта для персональных компьютеров очень остро стоит проблема интеллектуальной защиты своих продуктов. Еще более остро это проблема возникает для защиты программ, которые не компилируются в исполняемый файл, а поставляется конечным пользователям в виде кода, интерпретируемого во время выполнения программы.

Для этих целей применяются различные методики «запутывания» кода. *Обфускацией* (от английского obfuscation — буквально «запутывание») называется совокупность методик и средств, направленных на затруднение анализа программного кода [1]. В работе проведен анализ различных типов обфускаторов:

- обфускаторов, запутывающих код, написанный на интерпретируемых языках, таких как Perl или PHP. Рассмотрены методики, от самых простых, таких как удаление комментариев и изменении имен переменных на бессмысленные, до сложных, таких как шифрование строковых констант, введении семантически незначимых конструкций и значительном увеличении тела программы с многочисленными переходами.
- обфускаторов, анализирующих и преобразующих байт-код виртуальных машин Java и .NET.

Само собой разумеется, что в результате запутывания программа может оказаться более медленной во время исполнения, а также зачастую может быть более большой по объему. Для оценки действий программы-обфускатора вводится такая величина, как стоимость. *Стоимость* (*cost*) преобразования [3] - это метрика, которая позволяет оценить, насколько больше требуется ресурсов (памяти, процессорного времени) для выполнения запутанной программы, чем для выполнения исходной программы. Стоимость определяется по следующей шкале:

- бесплатное преобразование – увеличивает затраты ресурсов запутанной функции на O(1),
- дешевое преобразование – увеличивает затраты ресурсов на O(m), где m - размер запутанной функции,
- умеренное по стоимости преобразование – увеличивает затраты ресурсов запутанной функции на O(mp), где p > 1.
- дорогое преобразование – экспоненциально увеличивает затраты ресурсов запутанной функции по сравнению с исходной.

Согласно [3], можно выделить четыре основных типа запутывающих преобразований:

8. *преобразования форматирования*, которые изменяют только внешний вид программы. К этой группе относятся преобразования, удаляющие комментарии, отступы в тексте программы или переименовывающие идентификаторы;

9. *преобразования структур данных*, изменяющие структуры данных, с которыми работает программа. К этой группе относятся, например, преобразование, изменяющее иерархию наследования классов в программе, или преобразование, объединяющее скалярные переменные одного типа в массив;

10. *преобразования потока управления программы*, которые изменяют структуру её графа потока управления, такие как развёртка циклов, выделение фрагментов кода в процедуры, и другие подобные действия;

11. *превентивные преобразования*, нацеленные против определённых методов декомпиляции программ или использующие ошибки в определённых инструментальных средствах декомпиляции.

Когда мы говорим о процессе обфускации, появляется вопрос: есть ли процесс обратный ему, который позволил бы злоумышленнику вернуть наиболее похожий первоначальный код программы, то есть код до обфускации? На этот вопрос трудно дать однозначный ответ, но такой процесс существует и носит он название деобфускация. Но другой не менее важный вопрос, это как его можно реализовать [2].

В первой и второй частях данной работы рассматривается, что же собой представляют эти два взаимно противоположных (но не взаимно обратимых) процесса – обфускация и деобфускация. Приводится анализ устойчивости запутывающих алгоритмов по отношению к различным методам распутывания, а также показана возможность или невозможность автоматизации распутывающих преобразований.

В третьей части работы проанализированы варианты распространения и скрытия вредоносного кода в HTML-страницах и начаты разработки теоретического базиса и практической реализации для создания инструментального средства для деобфускации вредоносного кода, скрытого в сценариях HTML-страницы, так как именно при помощи обфускации злоумышленники очень часто пытаются если не сделать невозможным, то хотя бы максимально затруднить разбор своего вируса. В качестве языка был выбран JavaScript, так как по данным *viruslist.com* [4], количество вредоносного кода на JavaScript возросло на 48%, что является самым большим ростом из всех интерпретируемых языков. Соответственно, данный язык и является наиболее подверженным различным методам обфускации.

По итогам проделанной работы в состав инструментального средства входят:

8. *модуль парсинга HTML-страницы.* Данный модуль отвечает за разбор полученной на входе HTML-страницы во фреймовую сеть тегов. Решение о создании отдельного модуля (а не использовании готового инструментария) было вынесено из-за некоторой специфичности представления страницы, связанном с деобфускацией самой Web-страницы. В дальнейшем, возможно, будет решено использовать сторонний парсер, а суть данного модуля будет заключаться в конвертировании результатов в нужную форму;

9. *модуль сбора всего JavaScript-кода в общую базу.* Данный модуль необходим для извлечения из пропарсенного HTML-кода необходимого нам JavaScript-кода;

10. *модуль загрузки недостающего JavaScript-кода.* Для создания полной картины необходимо наличие всего кода;

11. *модуль парсинга JavaScript-кода.* Для представления всех переменных, констант, функций и прочих конструкций языка в виду динамической структуры. Возможно использование готовых JavaScript-парсеров;

12. *модуль деобфускации.* Непосредственно сам модуль деобфускации JavaScript-кода, разработка которого, по сути, и является одной из основных целей;

13. *модуль обфускации.* Как необходимость для тестирования, а также как желательное побочное действие будет написан модуль запутывания кода.

14. *модуль общего логирования.* Каждый модуль будет оставлять свои собственные логи, цель данного модуля – составление общего отчета о проделанной работе. В дальнейшем планируется начать создание модуля, целью которого будет являться автоподписание действий программы (само собой, как уже говорилось ранее, задача распознования семантики программы по ее синтаксису является алгоритмически неразрешимой; предполагаемый модуль будет выполнять эту задачу лишь частично).

К процессу деобфускации можно косвенно отнести процесс оптимизации программного кода, так как они оба, в той или иной степени, противоположны процессу обфускации. В процессе обфускации в программный код часто производиться добавление лишних операций, они обычно никоим образом не влияют на результаты работы самой программы, и предназначены для сбивания с толку и усложнения процесса изучения кода программы сторонними лицами. В свою очередь процесс оптимизации программного кода направлен на ликвидацию лишних операций, поэтому в частных случаях он может выступать в качестве квинтэссенции процесса деобфускации [2].

Рассмотрим классификацию методов процесса деобфускации (согласно [2]):

- нахождение и оценка непрозрачных конструкций (предикатов), статический анализ, которых очень сложен.
- сопоставление с образцом. Осуществляется различными способами, наиболее распространенны два из них.
- Первый, это когда берется несколько одних и тех же программ, прошедших процесс обфускации (так как процесс обфускации в большинстве случаев уникален, то их код также будет разный, хотя они и будут выполнять идентичные действия), и производиться сравнение фрагментов их кода, для выявления вставленного в процессе осуществления обфускации лишнего кода, который в последствии просто убирается.
- Второй способ сопоставления с образцом, осуществляется путем поиска в коде программы наиболее распространенных конструкций, применяемых в процессе обфускации. Такие конструкции могут, например, храниться и обновляться в соответствующей базе данных, или быть получены путем изучения работы самого обфускатора.

- выделение в программе фрагментов кода, которые никоим образом не связанны с основными задачами, которые должна выполнять программа, то есть обнаружение ненужных (лишних) участков кода.
- статистический анализ, заключается в динамическом анализе кода программы. Например, нахождение непрозрачных предикатов может осуществляться путем выделения и дальнейшего изучения в анализируемом коде программы тех предикатов, которые в процессе его выполнения возвращают всегда одно и тоже значение. Статистический анализ также может быть использован для оценки корректности осуществленного процесса деобфускации, для этого параллельно запускается программа "A" и программа, полученная в результате деобфускации "A`", им передаются эквивалентные входные данные, и происходит сравнение выходных. Если выходные данные одинаковы, то можно предположить, что процесс деобфускации был осуществлен правильно.
- анализ потока данных, основывается на изучении того, как в процессе работы программы изменяются в ней данные (переменные, массивы).

Так как теория обфускации очень активно развивается в настоящее время, и придумываются все новые, более усовершенствованные методы запутывания, то считаю, что создаваемое инструментальное средство для анализа и распутывания кода окажется весьма кстати для распутывания этих новых методов. В данной работе в качестве языка был предложен JavaScript, но теория, изложенная выше, вполне может быть переложена на некоторый другой интерпретируемый язык программирования, за некоторыми редкими исключениями (предполагается использовать особенности JavaScript, рассмотренные выше, при процессе деобфускации в частных единичных случаях).

На данный момент в современной открытой литературе очень мало работ, серьезно занимающихся именно процессом деобфускации, отчасти потому, что это процесс малоавтоматизируемый, да и занимаются им либо те, кто «ломают» чужое программное обеспечение, либо те, кто пытаются вникнуть в суть кода. Поэтому проблема деобфускации является актуальной. А если полученные результаты удается применить на благо, как например, попытался сделать автор, то задача становится востребованной.

ЛИТЕРАТУРА

12. Koller «Процесс обфускация, его алгоритмы, процесс деобфускации» [статья на форуме], http://rootaccess.info/index.php?showtopic=2029&pid=10132&mode=threaded&start= (ссылка действительна на 1 января 2009).

13. LynX «Обфускация и защита программных продуктов» [электронный документ], http://www.citforum.ru/security/articles/obfus/ (ссылка действительна на 1 января 2009).

14. Чернов А. В. «Анализ запутывающих преобразований программ» [электронный документ], http://www.citforum.ru/security/articles/analysis/ (ссылка действительна на 1 января 2009).

15. Kaspersky Security Bulletin 2008. Развитие угроз в первом полугодии 2008 года [электронный документ] http://www.viruslist.com/ru/analysis?pubid=204007623 (ссылка действительна на 1 января 2009).

Применения искусственных иммунных сетей в задачах детектирования вредоносного кода

Снегурский А.В.

Харьковский национальный университет радиоэлектроники
Харьков, Украина
alexandr.snigurskiy@dnt-lab.com

Application of artificial immune networks in problems of detecting of malware code

Snegursky A.V.

Kharkov National University of Radio electronics
Kharkov, Ukraine
alexandr.snigurskiy@dnt-lab.com

It was considered the possibility of application of artificial immune network model in the capacity of base for the development of effective heuristic analysis algorithm for detection of malware code.

Стремительное развитие алгоритмов упаковки и шифрования исполняемого кода обуславливает все большую актуальность проблемы разработки эффективных алгоритмов эвристического анализа. Одним из современных подходов к решению данной проблемы является использование искусственной иммунной сети, как фундаментальной парадигмы для решения задач классификации и кластеризации.

Цель работы состоит в разработке модели эффективного анализатора для распознавания схожих модификаций упакованных/зашифрованных вредоносных объектов.

Анализатор состоит из следующих частей:

- Блок мониторинга. Функцией данного блока является мониторинг поведения вредоносных и не вредоносных объектов с целью получения протокола их работы (последовательностей вызова API функций и переданных им аргументов).
- Блок сравнения. Данный блок принимает протоколы работы нескольких образцов от блока мониторинга и сравнивает их. Результатом работы данного блока будет множество одинаковых фрагментов в протоколах разных образцов одного семейства(далее «признаков»).
- Библиотека признаков. Данный блок хранит в себе все признаки выявленные блоком сравнения и ведет статистику их встречаемости. На основе данной статистики каждому признаку присваивается рейтинг характеризующий встречаемость данного признака, т.е. фрагмент, который был найден в протоколах всех образцов будет иметь наибольший рейтинг а фрагмент который найден в наименьшем количестве образов - наименьший.
- Блок принятия решений. Основной компонент анализатора. Функция данного компонента – принятие решения о принадлежности/непринадлежности рассматриваемого образца к некоторому семейству вредоносных программ.

Анализатор работает в двух режимах: обучение и распознавание.

В режиме обучения происходит настройка анализатора на распознавание поведений вредоносных объектов, при этом выполняются следующие действия:

1. Множество исполняемых файлов вирусов, сходных по функционалу и принадлежащих к одному семейству исследуется с помощью эмуляции и составляется подробные карты их действий (протоколы).

2. После этого протоколы сравниваются между собой, для того что бы выявить общие закономерности в поведении объектов.

3. Найденные закономерности представляются в виде фрагментов протоколов и сохраняются в библиотеке. Далее подсчитывается рейтинг встречаемости для каждого найденного фрагмента. Этот рейтинг показывает, в каком количестве объектов из всего множества представленных, был найден данный фрагмент. Происходит формирование выборки с рейтингами признаков вредоносных программ, для обучения нейронной сети на положительные вердикты.

4. Выборка не вредоносных программ исследуется с помощью эмуляции аналогичным образом как в пункте 1. После этого в протоколах работы не вредоносных программ производится поиск фрагментов поведения вредоносных программ, предварительно

сохраненных в библиотеке. Для всех не вредоносных программ так же формируется выборка с рейтингами признаков вредоносных программ, которая будет использована для обучения нейронной сети на отрицательные вердикты.

5. Производится создание иммунной сети и ее обучение на ранее подготовленных наборах рейтингов встречаемости.

В режиме распознавания перед иммунной сетью ставится задача кластеризации входного набора исполняемых кодов программ (представленных множеством рейтингов признаков), и выделения среди них подмножества вредоносных программ.

В качестве модели искусственной иммунной сети использовалась модель aiNet, предложенная Leandro N. de Castro и Fernando J. Von Zuben. Такая сеть может быть формально представлена в виде графа, состоящего из множества вершин, соответствующих антителам, и множества взвешенных ребер, обозначающих связи между клетками сети. Значение веса ребра соответствует аффинности связи. Кластерами сети aiNet служат внутренние образы (*internal images*), ответственные за отображение кластеров, существующих во множестве входных данных, в кластерах искусственной иммунной сети. В основе алгоритма обучения сети лежат механизмы клонального отбора и сжатия сети за счет удаления самораспознающих антител (*Ab-Ab recognition*).

В качестве популяции антигенов иммунной сети выступает множество входных данных, представленное в виде векторов из *p*-элементов. Каждый элемент вектора характеризует степень встречаемости (рейтинг) определенного характерного признака в исследуемом исполняемом коде.

Множество данных, используемых при обучении искусственной иммунной сети, формируется в результате выявления общих последовательностей вызовов API-функций у определенного количества вредоносных программ, взятых из одного семейства. Анализируемые последовательности вызовов API-функций получаются в ходе поведенческого анализа вредоносных программ с использованием эмулятора (технология ”Sandboxing”) либо API-монитора.

Дальнейшее развитие рассмотренного подхода позволит в значительной мере повысить эффективность антивирусного программного обеспечения при работе с полиморфным кодом вследствие отказа от сигнатурного анализа в пользу эвристического.

Способы борьбы со скрытыми каналами

Халитова К.И.

Самарский Государственный Аэрокосмический Университет
Самара, Россия

balabolka13@mail.ru

Ways of combating hidden channels

Khalitova K.I.

Samara State Space University
Samara, Russia

balabolka13@mail.ru

В любом наборе информации, будь то исполняемая программа, графическое изображение или сетевой протокол есть пути переноса дополнительных «скрытых» данных. Широко известны инструменты туннелирования, использующие служебные заголовки протоколов сетевого уровня TCP/UDP. Однако практическое применение таких туннелей ограничено из-за их низкой пропускной способности. Более широкие перспективы для построения скрытых коммуникационных каналов основываются на использовании прикладных протоколов. Здесь есть возможность быстрой передачи

больших объемов произвольной информации в качестве полезной нагрузки самого протокола, а не кода внутри его служебных заголовков.

Под скрытым каналом понимается способ организации несанкционированной передачи информации за счет избыточности протоколов межсетевого и внутрисистемного взаимодействия. При этом для организации передачи могут использоваться атрибуты, не предназначенные для передачи данных: задержки между регистрируемыми событиями, порядок следования сообщений, длины передаваемых блоков данных.

Впервые понятие скрытого канала было введено в работе Лэмпсона "A Note of the Confinement Problem" в 1973 году. Канал является скрытым, если он не проектировался, не предполагался для передачи информации в электронной системе обработки данных. Иными словами, это некий способ скрытой (замаскированной) несанкционированной передачи информации стороннему лицу, нарушающий системную политику безопасности.

Для организации “скрытых каналов” используется как штатное программное обеспечение, так и специально созданное вредоносное ПО.

Находясь внутри системы, программа-шпион способна скрытым способом установить связь со своим автором и передавать ему требуемые сведения. Атаки с использованием скрытых каналов всегда приводят к нарушениям конфиденциальности информации и в крайне редких случаях кто-либо пойдет на этот шаг ради удовлетворения личных амбиций. Чаще всего, это заказные адресные и тщательно подготовленные мероприятия.

Используя скрытые каналы передачи данных, "удаленный" злоумышленник может преследовать цель организовать управление информационной сетью извне, превратив её в бот.

На сегодняшний день подобные технологии наносят серьёзный ущерб компаниям и отдельным лицам, зачастую не подозревающим о том, что данные, хранящиеся и обрабатываемые на их компьютерах, уже давно являются не только их личным достояние.

Известны множество способов организации побочных каналов утечки информации, связанных с электромагнитным излучением, которое может содержать информацию об обрабатываемых на компьютере данных. Работа с побочными электромагнитными излучениями и наводками, привела к развитию технологии Soft Tempest, обеспечивающей скрытую передачу данных по каналу побочных электромагнитных излучений (ПЭМИН) с помощью программных средств.

По сути Soft Tempest атака, позволяет с использованием специальной программы-закладки, внедряемой на компьютер жертвы с помощью вредоносного ПО (трояны, сетевые черви и др.) отсортировывать необходимую информацию и передавать ее путем модуляции изображения монитора. Принимая побочные излучения монитора, можно выделить полезный сигнал и передать содержащиеся в нём приватные или корпоративные данные заинтересованной стороне.

Фактически, работа злоумышленника в этом случае сводится к трём основным задачам: установить шпиона, доставить перехваченную информацию условному заказчику и скрыть следы преступления, то есть сам факт того, что на компьютере жертвы была (или присутствует) какая-либо активность, помимо тех процессов, что запущены самим хозяином ПК.

В настоящее время как никогда актуальна проблема обеспечения высокого уровня информационной безопасности вычислительных сетей и средств.

Не смотря на пугающие масштабы современных угроз и постоянно расширяющийся инструментарий злоумышленников бороться с вредоносным ПО и кражей приватных данных можно и нужно. Создание скрытых информационных потоков является строгим нарушением политики ИБ, в связи с чем необходимо проводить регулярный анализ всей сетевой активности. Инспектирование должно предполагать решение следующих задач:

- выявление скрытых каналов;
- оценка пропускной способности скрытых каналов
- оценка рисков, связанных с функционированием скрытых каналов;
- выделение сигнала и типа информации, передаваемой по скрытым каналам;
- противодействие реализации скрытого канала вплоть до его уничтожения.

Грамотно организованная архитектура сети, защита которой построена на принципе эшелонирования – это серьёзный барьер для злоумышленника. Лучшей практикой является построение

эшелонированной централизованной системы антивирусной защиты, предусматривающей использование технологий защиты от вредоносного ПО и нежелательной корреспонденции на уровнях:

- входа в корпоративную сеть (gateway);
- сервера корпоративной сети;
- конечного устройства пользователя.

Самым сложным в этой и любой другой градации по уровням является организация защиты на уровне шлюза. Использование надёжных гибко настроенных фильтров, блокирующих "шпионов" на сетевом шлюзе и позволяющих оперативно закрывать все возможные уязвимости в сети, даже до выпуска официальных патчей от вендоров – это задача не из лёгких. И самым важным вопрос здесь как всегда является вопрос о том, какое решение позволит это сделать. Ведь между всем известными spy ware и ad ware есть множество разных других более сложно организованных кодов, селективно закрыть которые совсем не так просто. Не зря многие антивирусные вендоры опускают руки, если речь заходит о инспектировании графического контента или полной проверки кода HTML.

Для иллюстрации принципа эшелонирования рассмотрим следующий гипотетический пример. Банк, информационная система которого имеет соединение с Интернет, защищенное межсетевым экраном, приобрел за рубежом автоматизированную банковскую систему (АБС). Изучение регистрационной информации экрана показало, что время от времени за рубеж отправляются IP-пакеты, содержащие какие-то непонятные данные. Стали разбираться, куда же пакеты направляются, и оказалось, что идут они в форму-разработчик АБС. Возникло подозрение, что в АБС встроены "троянская" программа и скрытый канал, чтобы получать информацию о деятельности банка. Связались с фирмой и в конце концов выяснили, что один из программистов не убрал из поставленного в банк варианта отладочную выдачу, которая была организована сетевым образом (как передача IP-пакетов специфического вида, с явно заданным IP-адресом рабочего места этого программиста). Если бы не межсетевой экран, канал оставался бы скрытым, а конфиденциальная информация о платежах свободно гуляла по сетям.

Еще один практически важный в данном контексте архитектурный принцип — разнесение доменов выполнения для приложений с разным уровнем доверия на разные узлы сети. Если такие приложения будут функционировать в распределенной среде клиент/сервер, ограничить их взаимное влияние (и, следовательно, заблокировать скрытые каналы) будет существенно проще, чем в случае единых многопользовательских систем.

Основные критерии, которым должна удовлетворять система контентной фильтрации на уровне шлюза, следующие:

- блокирование уязвимостей в программном обеспечении (эксплойтов) и атак, направленных на клиентские приложения;
- инспектирование 100% HTTP/FTP трафика в реальном времени;
- прозрачное блокирование для всех Web-страниц (HTML) уязвимостей и атак ‘drive by’;
- многоуровневая защита от всех известных и неизвестных видов spyware, ad ware, троянов, руткитов, перехватчиков нажатий на клавиши, вирусов и червей;
- предотвращение фишинговых атак как с известных и неизвестных фишинговых сайтов, так и с инфицированных хакерами доверенных сайтов;
- URL фильтрация / родительский контроль с использованием постоянно обновляемой базы каталогизированных Интернет-сайтов;
- прозрачное инспектирование POP3 and SMTP почтовых протоколов на наличие злонамеренных кодов и спама;
- неограниченная масштабируемость системы (с учётом роста компании);
- детализированные отчеты для каждого пользователя.

Естественно, обеспечить такую защиту в домашних условиях фактически невозможно. Не стоит забывать и о том, что злонамеренный код постоянно прогрессирует и становится всё более "умным". Его создатели прекрасно понимают, что на данный момент в мире фактически нет компьютеров, на которых не установлен антивирус. Соответственно, вредоносное ПО должно сначала заблокировать

антивирус, чтобы проникнуть на ПК и затем реализовать любую активность, начиная от сбора ценных сведений и заканчивая выведением из строя сети.

Наиболее адекватным выходом для защиты домашних компьютеров является использование их хозяевами провайдинг-сервиса доставки "чистого" контента, прошедшего фильтрацию на узле провайдера и, следовательно, освобожденного от 99% вредоносного кода и спама. Подобные услуги достаточно широко распространены на Западе, и в России отдельные прогрессивные xSP-провайдеры уже начинают оценивать подобные сервисы в качестве новой рыночной нишы. Общая же масса относительно таких проектов пока настроена скептически. Ещё бы, ведь помегобайтная система оплаты трафика не предполагает выявления вредного контента – пользователь платит за общий объём, независимо от того, сколько "мусора" в итоге осело на его машине. Однако виросписатели не дремлют, и кто знает, оправдает ли себя такой реактивный подход или уже пора задуматься о превентивной защите.

Только программными средствами проблем информационной безопасности не решить. В настоящее время наметилась тенденция к расширению аппаратной поддержки защитных средств. Когда подобная поддержка обретет реальные очертания — вопрос не одного года. Чтобы он получил реальное решение, нужны экономические и правовые предпосылки, а не только устрашающая статистика злоумышленной активности и оценки потерь от нее.

Первопричину проблем информационной безопасности следует искать в сложности современных систем. Бороться со сложностью — значит делать системы более безопасными. К сожалению, стремление опередить конкурентов, предложить систему с более богатой функциональностью заставляют производителей двигаться в противоположном направлении. В настоящее время не видно причин, способных эту тенденцию изменить. Системным интеграторам и потребителям остается надеяться только на себя, на свое умение выбирать максимально простую, продуманную архитектуру и поддерживать производственные системы в безопасном состоянии техническими и организационными мерами, тратя силы и средства на отражение реальных, а не надуманных угроз.

Analysing the Kerberos timed authentication protocol using CSP-RANK functions

Yoney Kirsal and Orhan Gemikonakli

School of Engineering and Information Sciences, Middlesex University,
The Burroughs, Hendon, London NW4 4BT, UK
y.kirsal@mdx.ac.uk; o.gemikonakli@mdx.ac.uk

Abstract: Despite advances in network security, malicious attacks have shown a significant increase in recent times. Authentication mechanisms coupled with strong encryption techniques are used for security purposes; however, given sufficient time, well-equipped intruders succeed in breaking encryptions and compromising system security. The protocols often fail when they are analysed critically. Formal approaches have emerged to analyse protocol failures. Communicating Sequential Processes (CSP) is an abstract language designed especially for the description of communication patterns. A notion of rank functions is introduced for analysing purposes as well. This paper presents an application of this formal approach to a newly designed authentication protocol that combines delaying the decryption process with timed authentication while keys are dynamically renewed under pseudo-secure situations. The analysis and verification of authentication properties and results of the designed protocol are presented and discussed

1. Introduction:

Owing to the growing popularity and the use of computers and network-based electronic devices, providing privacy and data integrity has become more crucial; effective mechanisms are necessary to prevent network-based attacks and unauthorised access. For the purposes of attack prevention, authentication and access control play a vital role (Abadi, 1996). In order to meet increasing demands in secure computer communications, various security protocols have been developed.

Kerberos is one of these commonly used mechanisms. It is based on Needham-Schroeder Authentication Protocol (Needham, 1978). It utilises symmetric key cryptography to provide authentication for client-server applications. The Kerberos architecture is divided into two core elements, Key Distribution Centre (KDC) and Ticket Granting Service (TGS). The KDC stores authentication information while TGS holds digital tickets for clients and servers of networks for identifying themselves.

A new protocol description is designed (Kirsal, 2006) as the initial steps of developing a specific authentication protocol that provides authentication following a previously proposed framework (Kirsal, 2005). This protocol has properties of Kerberos and Key-Exchange protocols together with a powerful intruder model. Although the intruder has been given power to attack, the protocol is successful in preventing replay attacks.

Despite the design and proposal of authentication approaches for improving security of networks, threats of penetration and various other forms of attacks have continued to evolve.

In order to prevent intruder access to a network, increasing the decryption time of messages for an attacker is another way of attack prevention. Especially, security protocols on distributed systems are time-sensitive. In the analysis of delayed decryption systems, timestamps play an important role.

A new approach has been proposed to shut down external access to an enterprise network for a period of time to enable the distribution of randomly generated keys to users in a relatively secure way (Kirsal, 2007). This approach is based on the assumption that, the main threat is from external sources, internal sources can be controlled better. Renewing keys at various intervals while potential intruders are blocked out would inevitably work against intruders. Although the intruders may have the power to attack, the protocol is successful in preventing replay attacks (Kirsal, 2008).

Cryptographic protocols are necessary for secure key distribution in order to provide suitable keys for authenticated communication. However, it has also been reported that, the protocols often fail when they are analysed critically (Lowe, 1996). At this point, formal methods emerged for verification of security protocols. One of the most preferred methods is general purpose verification tools. The CSP is one of these tools. It is an abstract language designed especially for the description of communication patterns of concurrent system components that interact through message passing. The aim of the CSP approach is to reduce questions about security protocols and ensure that CSP processes satisfy particular specifications (Schneider, 1997).

CSP is particularly suitable for describing protocols close to the level we think of them. Schneider introduces the notion of rank functions to analyse the protocols by using the process algebra CSP.

In this paper, a new protocol based on the use of timestamps to delay decryption (Kirsal, 2008) is presented as an application of Rank-functions. The proposed model is based on secure key distributions at various intervals. During key distribution, external access to the network of servers is not allowed. The access restriction happens for short intervals. The proposed protocol is the initial steps for implementing a previously proposed framework (Kirsal, 2005). To prevent intrusion, it is proposed that external link(s) are shut down for short intervals to ensure secure key distribution and then links are re-instated. This will considerably restrict time for intruders to break encryptions.

In order to deal with the above protocol verification, Schneider's CSP process algebra is used along with the central rank function theorem. The evaluation and results are presented.

2. Related Work:

In recent years, various security protocols have been developed. Most of these protocols agreed upon a cryptographic key or achieved authentication specifications (Lowe, 1995, Abadi and Needham, 1996). These studies indicate that cryptographic protocols are prone to various forms of attacks.

Kerberos Authentication Protocol is designed as part of project Athena, provides secret key cryptography for secure communications. It uses key distribution. Clients and servers use digital tickets to identify themselves to the network and secret cryptographic keys for secure communications. The success of password guessing and replay attacks against Kerberos and weaknesses as a result of Kerberos' requirement of a trusted path have been clearly identified as limitations of Kerberos (Bellovin, 1991).

Furthermore, Kerberos' operation is system and application independent. Kerberos provides a mutual authentication between a client and a server. The Kerberos protocol assumes that initial transactions take place on an open network where clients and servers may not be physically secure and packets travelling on the network can be monitored and even possibly modified. The proposed framework (Kirsal, 2007a) and protocol script (Kirsal, 2007b), (Kirsal 2008) provide a design of security solution for wireless local area networks. Since the Kerberos Authentication Protocol is a trusted third party authentication protocol, its paradigms and entities are finalised for the proposed framework (Kirsal, 2007a). It is a timed model security protocol; that uses timestamps to delay decryption of messages by intruders. An approach has been proposed to shut down external access to an enterprise network (or part of it) for a period of time to enable the distribution of randomly generated keys to users. Renewing keys at various intervals while potential intruders are blocked out would inevitably work against intruders (Kirsal, 2007a). This study is based on the idea that the main threat is from outsiders and it is relatively easier to control internal sources since the internal sources are known. Keys are renewed at various intervals while external access to the system is disabled. Since, delay decryption mechanism was not used in that study, another protocol has been developed with the combination of Kerberos Authentication Protocol and Encrypted Key Exchange Protocol (Kirsal, 2006) with the addition of "delay decryption" property of the Kerberos Authentication Protocol (Kirsal, 2007b), (Kirsal, 2008).

In order to model protocols, the participants in the protocols are modelled as well (Eneh, 2006). As stated here, to present the model of the attacker in CSP, initial steps involve determining the extent of information that could be available to an attacker with formerly mentioned potentials (Eneh and Gemikonakli, 2005).

In a simple protocol, it is assumed that there are two communicating principals, A and B, and an adversary who is the attacker. The attacker is modelled as having capacity to intercept messages in all directions, modify messages, inject new messages and transmit messages (Schneider, 1997).

The attacker on network is represented as follows in (Schneider, 1997):

a. with unknown number of clients:

$NET = (|||_{j \in USER} USER_j) \mid [trans, rec] \mid ATTACKER$

b. with only two participants (client/agent):

$NET = (USER_A |||USER_B) \mid [trans, rec] \mid ATTACKER$

Also, in Schneider (1997) valid theorems are presented and the description of the attacker as follows:

$ATTACKER \text{ sat } (INIT \cup (tr \Downarrow trans)) \vdash tr \Downarrow rec$

This theorem is used here to explain that the sets of all the messages that pass through the rec channel are a function of the initial knowledge of the attacker and the sets of the messages input on the trans channel. Additionally, the description of the attacker is represented as follows in (Schneider, 1997):

ATTACKER(S) = trans? i? j?m → ATTACKER (S U {m}) □ i, j ∈USER, S ├ m rec.i!j!m → ATTACKER (S)

Apart from these, with the use of the inference rule to analyse a typical Kerberos protocol in the presence of the TGS reveals that the protocol is subject to a TGS masquerade attack. As discussed in the study of Eneh and Gemikonakli (2005), authentication in Kerberos requires a client, C, to send a request to the authentication server, AS, requesting credentials for a given application server, V. The AS responds with the requested credentials consisting of a ticket and a session key encrypted with the client's key. Kerberos exchanges may also be in the presence of a TGS. The CSP model of inference is as follows:

1. $C \rightarrow AS : Options \| ID_c \| Realm \| ID_{tgs} \| Times \| Nonce_1$
2. $AS \rightarrow C : Realm \| ID_c \| Ticket_{tgs} \| E_{kc}[K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}]$
3. $C \rightarrow TGS : Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c^b$
4. $TGS \rightarrow C : Realm_c \| ID_c \| Ticket_v \| E_{kc,tgs}[K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v]$
5. $C \rightarrow V : Options \| Ticket_v \| Authenticator_c^c$
6. $V \rightarrow C : E_{kc,v}[TS_2 \| Subkey \| Seq\#]$

Nevertheless, the same study shows that, in distributed systems where the intruder has reasonable communication and computational power belonging to the same administrative domain, Kerberos may be compromised. In other words, the chance of impersonating a principal by an intruder is higher where AS and TGS are on the same broadcast network.

Additionally, Trace Semantics are used by Schneider (1997) to specify security properties for protocols as trace specifications. This is done with the following definitions:

P **sat S** $\Leftrightarrow \forall$ ***tr*** $\in$ traces (P) • *S(tr)*

where P is a process and *S* is a predicate. P satisfies S, if S(tr) holds for every trace *tr* of P.

In terms of occurrence of events in its traces, the following definition is used for some sets of events R and T:

P **sat** R **precedes** T $\Leftrightarrow \forall$ ***tr*** $\in$ traces (P) • $(tr \uparrow R \neq \langle\rangle \Rightarrow tr \uparrow T \neq \langle\rangle)$

where a process *P* satisfies the predicate R **precedes** *T* if any occurrences of an event from T is preceded by an occurrence of an event from R in every trace *tr* of P.

As mentioned before, in the same study of Schneider (1997), a set of rules is introduced and defined as well to verify the specifications. According to this study, set of rules defined as **atom A,** in this, another three sets are considered which are known as the set of participant identities on the network to be **U,** the set of nonces used by the participants in protocol run as **N** and the set of encryption keys used as **K** Altogether, the atoms are defined as $\mathbf{A = U \cup N \cup K.}$ A message space **M** contains all the messages and signals that appear during the protocol's run in a way that $m \in \mathbf{A} \Rightarrow m \in \mathbf{M.}$ A rank function ρ is defined in order to map events and messages to integers, ρ**: M→Z.** This space is divided into two parts for characterising those messages that the intruder might get hold of (Schneider, 1997):

$M_P^- = \{m \in M \mid \rho \leq 0\}$ $\quad$ $M_P^+ = \{m \in M \mid \rho > 0\}$

where M_P^- is defined as a non positive rank, for those messages that the enemy should never get hold of, where M_P^+ is assigned for positive rank of, without compromising the protocol.

A general rank function theorem is presented in order to ensure that a protocol will be verified to be correct with regard to its security properties, if all the steps of the theorem are proven (Schneider, 1997).

1. For the sets *R* and *T,* there is a rank function ρ**: M→Z:** $\forall m \in \mathbf{IK} \bullet \rho(m) > 0$
2. $\forall \mathbf{S} \subseteq M, m \in M \bullet ((\forall m' \in \mathbf{S} \bullet \rho(m') > 0) \wedge \mathbf{S} \vdash m) \Rightarrow \rho(m) > 0$
3. $\forall t \in \mathbf{T} \bullet \rho(t) \leq 0$
4. $\forall i \in \mathbf{U} \bullet User_i \| Stop$ **maintains** ρ

R
then NET **sat** *R* **precedes T**

3. Work in Progress:

Despite the multiplicity of authentication approaches for improving network security, different types of attacks continue to evolve.

The proposed framework (Kirsal, 2005) has been designed for providing a trusted third party authentication for wireless networks that require a high level of security. Furthermore, the proposed protocol script is a combination of Kerberos and Encrypted Key Exchange Protocol (Kirsal, 2006). Since th**e** proposed protocol is a timed model security protocol, it uses timestamps to delay decryption of messages by intruders. In the previous study (Kirsal, 2007a), the proposed approach was shutting-down external access to a network for a period of time (e.g. 140 seconds), to enable the distribution of randomly generated keys to users in a relatively secure way. Another protocol has been developed with combination of Kerberos Authentication Protocol and Encrypted Key Exchange Protocol (Kirsal, 2006) with addition of the “delay decryption” property of the Kerberos Authentication Protocol (Kirsal, 2007b). It is shown that, due to the strong encryption assignments and authentication specifications there were no attacks found, even when new options “Guessable” and “Crackable” are added to “#Intruder Information” section (Kirsal, 2008). The protocol proposed in this paper is a version of the protocol reported in (Kirsal, 2008) within the designed framework of (Kirsal, 2007a). Fig.1 shows the proposed system.

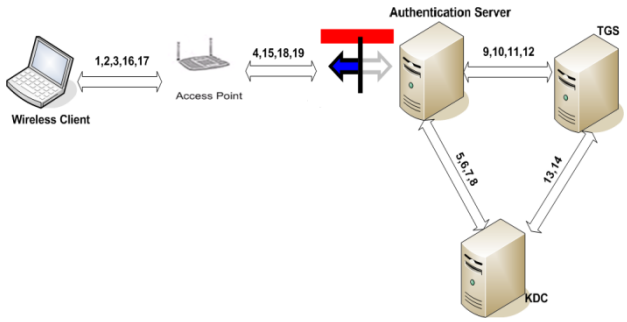


Fig.1. The Proposed Framework

The following script is the part of the proposed protocol script:

#Processes

INITIATOR(A,S,na) knows SK(A), SKey(A), PK(A), passwd(A,B)

RESPONDER(B,S,nb) knows SK(B), SKey(B), passwd(A,B)

SERVER(S,kab) knows PK, SKey, passwd

#Protocol description

0. -> A : B

[A != B]

1. A -> S : {B}{SKey(A)}

2. S -> A : {S,A,ts,{kab}{PK(A)},PK(B)%pkb}{passwd(A,B)}

3. A -> B : {A, ts, na, {kab}{pkb % PK(B)}}{passwd(A,B)} % v

[A != B]

4. B -> S : {A}{SKey(B)}

5. S -> B : {S, B, PK(A) % pka}{passwd(A,B)}

[decryptable(v,pka) and nth(decrypt(v,pka),1)==A \

and nth(decrypt(v,pka), 2) == now \

and decryptable(nth(decrypt(v,pka), 3), passwd(A,B)) \

and decryptable(nth(decrypt(v,pka), 4), SK(B))]

<na := nth (decrypt (nth(decrypt(v,pka), 3))) ; \

kab := nth (decrypt (nth(decrypt(v,pka), 4), SK(B)), 1)>
6. B -> A : {nb,na,tb}{kab}
7. A -> B : {nb,ta}{kab}
#Specification
TimedAgreement(A,B,2,[kab])
#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, Sam, Nm, PK, SPK, SK(Mallory), SKey(Mallory)}
Guessable = SessionKey
Crackable = SessionKey
Crackable = ServerKey

Crackable = Password

In the "#Processes" section, the first parameter of each process (here A, B and S) should represent agent identities used in the "#Protocol description" section Names are given to the roles played by the different agents. In this protocol, INITIATOR, RESPONDER, and SERVER are chosen as it was used in the protocol of (Kirsal, 2007b, Kirsal, 2008).

In the "#Protocol description" section, the protocol itself is defined by listing the steps in order. Message 0 is used to start the protocol off and tells A, the identity of the agent with whom he should run the protocol. Since the above protocol is timed protocol, timestamps *ta*, *tb* and *ts* are used as variables in the messages. The messages are encrypted with the password that is created by A and B and also are distributed by the server. This increases the time it takes for the intruder to decrypt the message. Additionally, in the "#Intruder Information" section, the intruder's identity and the set of data values that he knows are initially mentioned (Kirsal, 2008), (Lowe, 1998). The "Intruder knowledge" section holds the identifiers and functions of the protocol that he knows and he can apply any other value to those identifiers and functions.

3.1 The CSP Model of the Proposed Protocol:

In this section the CSP representation of the above proposed protocol is modelled as a network and specified the authentication property for this network as a trace specification.

While modelling the different processes of a protocol, advantage of the extensibility of CSP gives the opportunity to add additional elements to the processes.

The following scripts are representations of three participants of the proposed protocol.

INITIATOR(A, S, na) =

[] B : Agent @ A != B &env_I.A.(Env0, B,<>) ->

output.A.S.(Msg1, Encrypt.(SKey(A), <B>),<>) ->

[] kab : SessionKey @ [] ts : TS @ [] pkb : addGarbage_(PublicKey) @

input.S.A.(Msg2, Encrypt.(passwd(A, B), <S, A, Timestamp.ts, Encrypt.(PK(A), <kab>), pkb>),<>) ->

output.A.B.(Msg3, Encrypt.(passwd(A, B), <A, Timestamp.ts, na, Encrypt.(pkb, <kab>)>),<>) ->

[] nb : Nonce @ [] tb : TS @

input.B.A.(Msg6, Encrypt.(inverse(kab), <nb, na, Timestamp.tb>),<>) ->

[] ta : TS @

output.A.B.(Msg7, Encrypt.(kab, <nb, Timestamp.ta>),<nb>) ->

close.A.INITIATOR_role -> STOP

```
RESPONDER(B, S, nb) =
  [] A : Agent @
  [] v : addGarbage_({Encrypt.(passwd(A, B), <A, Timestamp.ts, na, Encrypt.(pkb,
<kab>)>) | A <- Agent, B <- Agent, kab <- SessionKey, na <- Nonce, ts <- TS, pkb <-
addGarbage_(PublicKey)}) @
    A != B & input.A.B.(Msg3, v,<>) ->
  output.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->
  [] pka : addGarbage_(PublicKey) @ [] now : TS @
    decryptable(v, pka) and nth(decrypt(v,pka), 1) == A  and nth(decrypt(v,pka), 2) == now  and
decryptable(nth(decrypt(v,pka), 3), passwd(A,B))  and decryptable(nth(decrypt(v,pka), 4), SK(B)) &
    input.S.B.(Msg5, Encrypt.(passwd(A, B), <S, B, pka>),<Timestamp.now>) ->
  RESPONDER'(B, S, nb, A, v, pka, nth(decrypt(nth(decrypt(v,pka),3))))


RESPONDER'(B, S, nb, A, v, pka, na) =
 RESPONDER''(B, S, nb, A, v, pka, na, nth(decrypt(nth(decrypt(v,pka),4),SK(B)),1))


RESPONDER''(B, S, nb, A, v, pka, na, kab) =
  [] tb : TS @
    output.B.A.(Msg6, Encrypt.(kab, <nb, na, Timestamp.tb>),<nb>) ->
  [] ta : TS @
    input.A.B.(Msg7, Encrypt.(inverse(kab), <nb, Timestamp.ta>),<nb>) ->
  close.B.RESPONDER_role -> STOP


SERVER(S, kab) =
  [] A : Agent @ [] B : Agent @
    input.A.S.(Msg1, Encrypt.(SKey(A),<B>),<>) ->
  [] ts : TS @
    output.S.A.(Msg2, Encrypt.(passwd(A, B), <S, A, Timestamp.ts, Encrypt.(PK(A), <kab>), PK(B)>),<>) ->
  input.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->
  output.S.B.(Msg5, Encrypt.(passwd(A, B), <S, B, PK(A)>),<>) ->
  close.S.SERVER_role -> STOP
```

In the model above, keywords *input* and *output* are used to define receive and send application respectively, where *trans* and *rec* keywords are the general definition for this purpose in Schneider's CSP definitions. Also, instead of key words $USER_A$, $USER_B$, INITIATOR and RESPONDER are used.

The CSP representations of each process (known as agents) show that the entities of the messages are encrypted with their own public keys.

The INITIATOR, A creates and sends a message, Msg3, but the receiver, B stores this message in variable *v*, without trying to interpret it. That is to say, RESPONDER, B decrypts this message and performs the appropriate checks only after receiving message in the future steps, which is defined as Msg5. Message 3 was encrypted with the inverse of the key received in message 5. Since the inverse of the password received is itself, B expects the common password. This is done in the following part:

```
A != B & input.A.B.(Msg3, v,<>) ->
output.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->
```

[] pka : addGarbage_(PublicKey) @ [] now : TS

In the test of message 5 “decryptable”, “decrypt” and “nth(_, n)” functions that are used for delaying decryption purposes.

Due to the use of delay decryption, B cannot automatically extract any fields from message 3, so more assignments are needed in the delay decryption model. The added assignments are defined as:

RESPONDER'(B, S, nb, A, v, pka, nth(decrypt(nth(decrypt(v,pka),3))))

RESPONDER'(B, S, nb, A, v, pka, na) =

RESPONDER''(B, S, nb, A, v, pka, na, nth(decrypt(nth(decrypt(v,pka),4),SK(B)),1))

The first assignment, RESPONDER', assigns the nonce *na* as the third field of message 3, but the message itself, is encrypted with the password of A – B, has to be decrypted using the inverse of this key which is itself.

The second assignment, RESPONDER'(B, S, nb, A, v, pka, na) = RESPONDER''(B,.) assigns the session key *kab* as the fourth component of message 3 but the first field of the message is encrypted with B’s public key and decryption has to be done by using the inverse of this key which is secret key of B.

Since the proposed protocol is time sensitive, introduction of any delay will prevent the intruder’s attempt to launch an attack. Because of this, the delay decryption technique that is used in here is to delay the intruder.

In the “#Specification” section of the proposed protocol, RESPONDER, B has completed a protocol run with A. This is verified with the following CSP process that implies that A was running the protocol with B within the last 2 time units and there is mutual agreement between them. This mutual agreement depends on the value of session key chosen:

```
AuthenticateINITIATORToRESPONDERTime
dAgreenent_
kab(A)                                    =
signal.Running1.INITIATOR_role.A?B?nb ->
signal.Commit1.RESPONDER_role.B.A.nb   ->
STOP


AlphaAuthenticateINITIATORToRESPONDER
TimedAgreement_kab(A) =
   {|signal.Running1.INITIATOR_role.A.B,
     signal.Commit1.RESPONDER_role.B.A |
       B <- inter(Agent, HONEST)|}
```

The intruder can try to make the first attempt to attack in step 3 when A sends nonce *na* to B. Due to protocol time agreement specification, an agent’s chance to attempt to connect will be timed-out by the server because of unsuccessful connection attempts thus preventing the attack.

In addition to the timestamps, nonces are also being used for authentication between the agents A and B.

Additionally, in the “#Intruder Information” section, the intruder’s identity and the set of data values that he knows are initially stated. The “Intruder knowledge” section holds the identifiers and functions of the protocol that he knows and he can apply any other value to those identifiers and functions.

The following CSP definition is Intruder’s initial knowledge with definitions:

```
IK0_init = union({Alice, Bob, Mallory, Sam, Nm, SK(Mallory), SKey(Mallory),
passwd(Mallory, Alice), passwd(Mallory, Bob),        passwd(Alice, Mallory),
passwd(Bob, Mallory),
```

```
passwd(Mallory, Mallory), Garbage}, TimeStamp)

INTRUDER_1 =
   (chase(INTRUDER_0)
   [[ hear.m_ <- send.A_.B_.(l_,m_,se_) |
         (l_,m_,se_,re_) <- DIRECT_MSG,
 A_ <- diff(SenderType(l_),{Mallory}), B_ <- ReceiverType(l_) ]]
    [|{| hear |}|] STOP)
 [[ say.m_ <- receive.A_.B_.(l_,m_,re_) |
     (l_,m_,se_,re_) <- DIRECT_MSG,
 A_ <- SenderType(l_), B_<- ReceiverType(l_)]]
```

The job of Intruder is defined in the above code together with its relevance to the initial knowledge.

The initially known facts that are added under the following section, the key words such as *leak, hear, say,* are used to signal that a possible secret has been learnt, to represent hearing and saying a message during the authentication and transfer of a message across a network.

```
SAY_KNOWN_0 =
   (inter(IK1, ALL_SECRETS_DI) != {} & dummy_leak -> SAY_KNOWN_0)
   [] dummy_send -> SAY_KNOWN_0
   [] dummy_receive -> SAY_KNOWN_0
 SAY_KNOWN =
   SAY_KNOWN_0
     [[ dummy_leak <- leak.f_ | f_ <- inter(IK1, ALL_SECRETS_DI) ]]
     [[ dummy_send <- send.A_.B_.(l_,m_,se_) |
         (l_,m_,se_,re_) <- DIRECT_MSG, components_(m_) <= IK1,
         A_ <- diff(SenderType(l_),{Mallory}), B_ <- ReceiverType(l_) ]]
     [[ dummy_receive <- receive.A_.B_.(l_,m_,re_) |
         (l_,m_,se_,re_) <- DIRECT_MSG, components_(m_) <= IK1,
         A_ <- SenderType(l_), B_ <- ReceiverType(l_) ]]
STOP_SET = {| send.Mallory |}

 INTRUDER =
(INTRUDER_1 [| STOP_SET |] STOP) ||| SAY_KNOWN

IntruderInterface = Union({{| send, receive |}, {|crack|}})

AlphaSystem = {|env, send, receive, close, tock|}
SystemManagerInterface = inter(AlphaSystem,CRACKING_M::AlphaManager)
SYSTEM = (SYSTEM_M::TSYSTEM_1 [|SystemManagerInterface|] CRACKING_M::Manager)
```

[|IntruderInterface|] INTRUDER_M::INTRUDER

It is proven that, in terms of attack prevention, the designed protocol is successful, despite of highly specified Intruder connection attempts.

4. Discussions:

This paper presents an approach to improve the security aspects of the Kerberos Authentication Protocol together with the CSP representation of the proposed approach.

The proposed protocol that has improvements over Kerberos authentication is designed to improve security and minimise the threat of possible attacks (Kirsal, 2007a, b and 2008).

As discussed in the previous section, the previous study (Kirsal, 2007b) was about shutting-down external access to a network for a period of time, to enable the distribution of randomly generated keys to users in a relatively secure way. Due to the Kerberos' delay decryption properties and being a timed authentication protocol, it is proven that in terms of attack prevention this protocol is successful despite of strong intruder connection attempts. This is investigated with an approach that is developed by Schneider in order to identify flaws in protocol design.

Throughout the process, it is managed to define and investigate attacks discussed earlier.

5. Conclusions:

This paper is presents the CSP codes of a new protocol proposed for improving security of the Kerberos Authentication Protocol. A new protocol is derived from a designed and tested protocol (Kirsal, 2007a, 2007b) to increase the time for an intruder to break an encryption and hence improve the security.

The Schneider's CSP Processes are applied to expose any flaws in the design and managed to identify attacks. It is based on increasing the time needed to break the encryption, and hence improve security.

In addition to delayed description, this paper proposes further improvement to network security by restricting externals' access to the system temporarily.

Further work will be carried out on the performance analysis of the proposed approach, in order to choose parameters for acceptable levels of security and performance.

6. References:

1. M. Abadi and R. Needham**,** "Prudent Engineering for Cryptographic Protocols**.**" *IEEE Transactions on Software Engineering*, vol. 22(1): pp. 6-15, 1996.
2. S.M. Bellovin, and M. Merritt**,** "Limitations of the Kerberos Authentication System"**.** *USENIX winter 1991,* pp.253-268. 1991.
3. A.H. Eneh., O. Gemikonakli and R. Comley, "Security of Electronic Commerce Authentication Protocols in Economically Deprived Communities", The Fifth Security Conference 2006, Las Vegas, Nevada, April 2006, ISBN: 0-9772107-2-3.
4. A.Harbitter and D. A. Menascé, "A Methodology for Analyzing the Performance of Authentication Protocols"**.** *ACM Transactions on Information and System Security,* vol. 5(4): pp. 458-491, 2002.
5. C.A. Hoare, "Communication Sequence Process". *Prentice- Hall*, International Englewood Cliffs. New Jersey. 1985.
6. Y. Kirsal, A. Eneh and O. Gemikonakli, "A Solution to the Problem of Trusted Third Party for IEEE 802.11b Networks", *PGNET2005*, Liverpool UK, pp.333-339, 2005.
7. Y. Kirsal and O. Gemikonakli, "An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols", *CISSE 2006,* 2006.
8. Y. Kirsal and O. Gemikonakli, "Frequent Key Renewal under Pseudo-Secure Conditions for Increased Security in Kerberos Authentication and Its Impact On System Performability", *3rd International Conference on Global E-Security,* University of East London (UeL), Docklands, UK, 2007a.
9. Y.Kirsal and O.Gemikonakli, "Further Improvements to the Kerberos Timed Autentication Protocol", *CISSE 2007*, 2007b.

10. Y.Kirsal and O. Gemikonakli, “Improving Kerberos Security through the Combined Use of the Timed Authentication Protocol and Frequent Key Renewal**”,** 6th IEEE International Conference on Cybernetic Systems 2008, Middlesex University, London, UK

11. G. Lowe**,** “An Attack on the Needham-Schroeder Public-key Authentication Protocol**.**” *Information Processing Letters***.** vol: 56(3), pp. 131-133, 1995.

12. G. Lowe, “Some New Attacks upon Security Protocols”, *Proceedings of 9th IEEE Computer Security Workshops*, pp. 162 – 170, 1996.

13. G. Lowe, “CASPER: A Compiler for the Analysis of Security Protocols”. *Proceedings of the 10th Computer Security Foundation Workshop.* pp.18-30., 1998

A. Mishra and W. A. Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard”, *White paper*, UMIACS-TR-2002-10, February 2002.

14. M. R. Needham and M.D. Schroeder, “Using Encryption for Authentication in Large Networks of Computers.” *Communication ACM* (21) pp.993–999, 1978.

A. W. Roscoe “CSP and Determinism in Security Modelling”. *IEEE Symposium on Security and Privacy.* pp. 115-127, 1995.

15. S. Schneider. “Verifying authentication protocols with CSP” *10th Computer Security Foundations Workshop,* IEEE. pp. 741-758, 1997.

16. “Security White Paper Evolution, Requirements, and Options”

Available: http://wifiplanet.com/tutorials/articles.php/965471
[Accessed: 27 April 2005]
[Last Accessed: 13 September 2007]

Анализ протокола аутентификации Керберос, построенного с помощью "штампа времени", с использованием функций CSP-RANK

Йони Кирсал, Орхан Гемиконакли

Школа техники и информатики, Университет Миддлсекс, Бэрроуз, Хендон, Лондон NW4 4BT, Великобритания

Аннотация: Несмотря на успехи, достигнутые в области обеспечения информационной безопасности при работе в сети, количество вирусных и хакерских атак существенно выросло за последнее время. Для обеспечения безопасности применяются механизмы аутентификации в сочетании с надежными методами шифрования; однако, имея в своем распоряжении достаточное время, хорошо вооруженным соответствующими средствами хакерам удается взламывать зашифрованную информацию и ставить под угрозу безопасность системы. Зачастую протоколы прекращают выполнять свои функции, если они подвергаются анализу на критическом уровне. Для анализа отказов работы протоколов были разработаны формальные подходы. Алгебра взаимодействия последовательных процессов (CSP) представляет собой абстрактный язык, специально предназначенный для описания моделей взаимодействия. Кроме того, для проведения анализа применяется понятие ранговых функций. В настоящей работе осуществляется применение этого формального подхода к новому предлагаемому протоколу аутентификации, в котором сочетается задержка процесса дешифрования с аутентификацией на основании "штампа времени" в то время, как производится динамическое обновление ключей с использованием механизмов псевдобезопасности. Проводятся анализ и проверка свойств аутентификации, а также обсуждаются результаты применения предлагаемого протокола.

1. Введение:

В связи с ростом распространения и использования компьютеров и сетевых электронных устройств проблема обеспечения конфиденциальности и целостности данных становится все более важной; необходимо обеспечить наличие эффективных механизмов для предотвращения сетевых атак и несанкционированного доступа. Жизненно важную роль для предотвращения сетевых атак играют процессы аутентификации и обеспечения доступа (Абади, 1996). Для удовлетворения растущего

спроса на обеспечение безопасности при взаимодействии компьютеров были разработаны различные протоколы системы защиты.

Керберос является одним из таких наиболее распространенных механизмов защиты. Он основан на использовании протокола аутентификации Нидхэма-Шредера (Нидхэм, 1978). В этом протоколе для обеспечения аутентификации в приложениях "клиент-сервер" применяется симметричная криптография с ключом. Архитектуру протокола Керберос можно разделить на два ключевых элемента: Центр распределения ключей (KDC) и Служба предоставления билетов (TGS). В KDC хранится информация об аутентификации, а в TGS находятся цифровые билеты, предназначенные для того, чтобы клиенты и серверы сетей могли себя идентифицировать в сети.

В качестве начальных шагов при разработке конкретного протокола аутентификации строится новое описание протокола (Кирсал, 2006), которое обеспечивает аутентификацию на основании предложенной ранее схемы (Кирсал, 2005). Этот протокол обладает свойствами протокола Керберос и протокола обмена ключами, а также содержит эффективную модель защиты от взломщиков. Хотя в данном случае взломщику предоставляется возможность осуществлять атаку, этот протокол успешно предотвращает атаки путем повторов.

Несмотря на создание и разработку подходов к осуществлению аутентификации, повышающих уровень безопасности работы в сети, угрозы проникновения и иные различные формы атак продолжают появляться.

Для того, чтобы не допустить доступа взломщика к сети, применяется другой подход к предотвращению атак, заключающийся в увеличении для злоумышленника времени, необходимого для дешифрования сообщений. Особенно чувствительными к времени являются протоколы обеспечения безопасности в распределенных системах. При анализе систем с задержкой дешифрования важную роль играют "штампы времени".

Был предложен новый подход, предусматривающий закрытие внешнего доступа к сети предприятия на некоторый период времени с тем, чтобы можно было относительно безопасным способом распределить среди пользователей случайным образом сгенерированные ключи (Кирсал, 2007). Этот подход основан на предположении о том, что основная угроза исходит от внешних источников, а управление внутренними источниками находится на более высоком уровне безопасности. Обновление ключей через разные интервалы времени в то время, когда доступ потенциальных взломщиков блокирован, должно очевидным образом затруднить работу взломщиков. И хотя в данном случае взломщикам предоставляется возможность осуществлять атаку, этот протокол успешно предотвращает атаки путем повторов (Кирсал, 2008).

Криптографические протоколы нужны для обеспечения надежного распределения ключей с тем, чтобы в случаях связи с взаимной аутентификацией партнеров выдавались надлежащие ключи. Однако сообщалось также о том, что часто происходят сбои и отказы протоколов аутентификации в том случае, если они подвергаются критическому анализу (Лоэв, 1996). На этой стадии появились формальные методы проверки протоколов защиты. При этом наиболее предпочтительными методами являются универсальные средства верификации. Одним из таких средств является CSP. Это абстрактный язык, предназначенный специально для описания моделей взаимодействия одновременных компонентов системы, которые взаимодействуют путем передачи сообщений. Цель подхода CSP состоит в том, чтобы сократить число вопросов о протоколах защиты и обеспечить выполнение процессами CSP конкретных спецификаций (Шнайдер, 1997). Процесс CSP особенно подходит для описания протоколов, близких к тому уровню, как мы их себе представляем. Шнайдер вводит понятие ранговых функций для анализа протоколов с помощью процессной алгебры CSP.

В настоящей работе в качестве приложения ранговых функций предлагается новый протокол, основанный на использовании "штампов времени" для задержки процесса дешифрования (Кирсал, 2008). Предложенная модель основана на распределении стойких к криптографическому анализу ключей через различные интервалы времени. Во время распределения ключей внешний доступ к сети серверов запрещен. Такое ограничение доступа происходит в течение коротких промежутков времени. Предлагаемый протокол представляет собой первые шаги реализации ранее предложенной схемы (Кирсал, 2005). Для предотвращения вторжения предлагается закрыть внешние ссылки на короткие промежутки времени для того, чтобы осуществить распределение стойких к криптографическому анализу ключей, а затем восстановить ссылки. Это должно существенным образом ограничить время, которое взломщик может использовать для расшифровки.

Для того, чтобы осуществить указанную выше верификацию протокола, применяется предложенная Шнайдером процессная алгебра CSP вместе с центральной теоремой о ранговых функциях. Производится оценка процесса и приводятся полученные результаты.

2. Родственные работы в данной предметной области:

В последние годы было разработано много различных протоколов защиты. В большинстве этих протоколов признавалась необходимость использования криптографического ключа или обеспечивалось выполнение условий аутентификации (Лоэв, 1995, Абади и Нидхэм, 1996). Эти исследования показывают, что криптографические протоколы восприимчивы к воздействию различных видов атак.

Протокол аутентификации Керберос создан как часть проекта "Афина" и обеспечивает криптографию с секретным ключом для осуществления взаимодействий, стойких к криптографическому анализу. В этом протоколе используется процесс распределения ключей. Клиенты и серверы пользуются цифровыми билетами для того, чтобы идентифицировать себя в сети, и секретные криптографические ключи для обеспечения безопасного взаимодействия. Успешное угадывание паролей и применение атак против протокола Керберос путем повторов, а также недостатки, связанные с содержащимся в протоколе Керберос требованием наличия доверенного пути, однозначно были квалифицированы как ограничения протокола Керберос (Белловин, 1991).

Кроме того, протокол Керберос работает независимо от системы и приложения. Протокол Керберос обеспечивает взаимную аутентификацию между клиентом и сервером. Использование протокола Керберос предполагает, что исходные транзакции осуществляются в открытой сети, в которой клиенты и серверы физически не могут находиться в безопасных условиях, а пакеты, передающиеся по сети, можно отслеживать и даже, возможно, модифицировать. Предлагаемая схема (Кирсал, 2007а) и сценарий протокола (Кирсал, 2007б), (Кирсал 2008) обеспечивают построение системы защиты для беспроводных локальных вычислительных сетей. Так как протокол аутентификации Керберос представляет собой протокол аутентификации доверенной третьей стороной, то его парадигмы и объекты окончательно определяются для предлагаемой схемы (Кирсал, 2007а). Это протокол защиты, основанный на временной модели, в которой используются "штампы времени" для задержки дешифрования сообщений взломщиками. Был предложен подход, предусматривающий закрытие внешнего доступа к сети предприятия (или к ее части) на некоторый промежуток времени для того, чтобы можно было распределить среди пользователей случайным образом сгенерированные ключи. Обновление ключей через разные промежутки времени в то время, когда доступ потенциальных взломщиков блокирован, должно очевидным образом затруднить работу взломщиков (Кирсал, 2007а). Это исследование основано на идее о том, что основная угроза исходит от внешних источников, а осуществлять управление внутренними источниками сравнительно легко, так как внутренние источники известны. Ключи обновляются через различные промежутки времени в то время, когда доступ к системе извне запрещен. Так как в этом исследовании механизм задержки дешифрования не используется, то был разработан другой протокол, включающий в себя комбинацию протокола аутентификации Керберос и протокол обмена зашифрованными ключами (Кирсал, 2006) с добавлением свойства "задержки дешифрования" протокола аутентификации Керберос (Кирсал, 2007б), (Кирсал, 2008).

Для того, чтобы моделировать протоколы, моделируются также участники, использующие протокол (Эне, 2006). Как показано в этой работе, для того, чтобы представить модель нарушителя в CSP, начальные шаги включают в себя определение объема информации, который может быть доступен нарушителю с указанными ранее возможностями (Эне и Гемиконакли, 2005).

В простом протоколе предполагается, что имеется два взаимодействующих принципала, A и B, и противник, являющийся нарушителем. Нарушитель моделируется таким образом, что он может перехватывать сообщения по всем направлениям, вбрасывать в сеть новые сообщения и передавать сообщения (Шнайдер, 1997).

В работе (Шнайдер, 1997) нарушитель в сети представляется следующим образом:

a. с неизвестным числом клиентов:

$NET = (|||_{j \in USER} USER_j) \mid [trans, rec] \mid ATTACKER$

b. только с двумя участниками (клиент/агент):

$NET = (USER_A \,|||\, USER_B) \mid [trans, rec] \mid ATTACKER$

Кроме того, в работе (Шнайдер, 1997) приводятся следующие действующие теоремы и описание нарушителя:

$ATTACKER \text{ sat } (INIT \cup (tr \Downarrow trans)) \vdash tr \Downarrow rec$

Эта теорема используется здесь для того, чтобы объяснить, что множества всех сообщений, проходящих через канал записи, являются функцией первоначального знания нарушителя и множеств сообщений на входе в канал передачи. Кроме того, в работе (Шнайдер, 1997) дается следующее описание нарушителя:

ATTACKER(S) = trans? i? j?m → ATTACKER (S U {m}) □ i, j ∈USER, S ├ m rec.i!j!m → ATTACKER (S)

Кроме этого, применение правила вывода к анализу типового протокола Керберос при наличии службы TGS свидетельствует о том, что этот протокол подлежит атаке с маскировкой TGS. Как отмечалось в исследовании Эне и Гемиконакли (2005), для аутентификации по протоколу Керберос требуется, чтобы клиент C отправил запрос на сервер аутентификации AS, запрашивая мандат для данного сервера приложений V. Сервер AS направляет в ответ запрошенный мандат, состоящий из билета и ключа сеанса, зашифрованных с помощью ключа клиента. Обмен по протоколу Керберос может также происходить при наличии службы TGS. Модель вывода процесса CSP имеет следующий вид:

1. $C \rightarrow AS : Options \| ID_c \| Realm \| ID_{tgs} \| Times \| Nonce_1$
2. $AS \rightarrow C : Realm \| ID_c \| Ticket_{tgs} \| E_{kc}[K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}]$
3. $C \rightarrow TGS : Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c^b$
4. $TGS \rightarrow C : Realm_c \| ID_c \| Ticket_v \| E_{kc,tgs}[K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v]$
5. $C \rightarrow V : Options \| Ticket_v \| Authenticator_c^c$
6. $V \rightarrow C : E_{kc,v}[TS_2 \| Subkey \| Seq\#]$

Тем не менее, в этом же исследовании показывается, что в распределенных системах, с которыми нарушитель может в разумных пределах входить во взаимодействие и в которых он имеет вычислительные возможности, принадлежащие к тому же административному домену, работа протокола Керберос может быть нарушена. Другими словами, вероятность того, что нарушитель сможет выдать себя за принципала, выше, если сервер AS и служба TGS находятся в одной и той же широковещательной сети.

Кроме того, в работе Шнайдера (1997) для определения свойств защиты для протоколов в качестве трассовых спецификаций используются правила трассовой семантики. Это осуществляется с помощью следующих определений:

$$P \textbf{ sat } S \Leftrightarrow \forall \, tr \in \text{traces}(P) \bullet S(tr),$$

где P – процесс, а *S* – предикат. P удовлетворяет S, если S(tr) выполняется для каждого следа *tr* от P.

С точки зрения возникновения событий в его следах, для некоторых множеств событий R и T используется следующее определение:

$$P \textbf{ sat } R \textbf{ precedes } T \Leftrightarrow \forall \, tr \in \text{traces}(P) \bullet (tr \uparrow R \neq \langle\rangle \Rightarrow tr \uparrow T \neq \langle\rangle),$$

где *P* удовлетворяет предикату R **предшествует** *T* в том случае, если любым возникновениям событий из T предшествует возникновение какого-либо события из R в любом следе *tr* от P.

Как отмечалось ранее, в этом же исследовании (Шнайдер, 1997) также вводится и определяется система правил для верификации спецификаций. В соответствии с этим исследованием множество правил определяются как **атом A,** в нем рассматриваются еще три множества, которые известны как множество участников в сети **U,** множество моментов, используемых этими участниками при работе протокола **N,** и множество ключей шифрования **K.** Вместе эти атомы определяются как **A = U ∪ N ∪ K.** Пространство сообщений **M** содержит все сообщения и сигналы, которые появляются во время работы протокола так, что $m \in A \Rightarrow m \in M$. Ранговая функция **ρ** определяется для того, чтобы отобразить события и сообщения на множество целых чисел **ρ: M→Z.** Это пространство делится на две части для характеризации тех сообщений, которые могут быть захвачены нарушителем (Шнайдер, 1997):

$M_P^- = \{m \in M \mid \rho \leq 0\}$ $\quad$ $M_P^+ = \{m \in M \mid \rho > 0\}$,

где M $_{P}^{-}$ определяется как неположительный ранг, для тех сообщений, которые враг никогда не захватит, где M $_{P}^{+}$ обозначает положительный ранг, без нарушения работы протокола.

Общая теорема о ранговых функциях приводится для того, чтобы обеспечить правильность верификации протокола в отношении его свойств защиты в том случае, если все шаги теоремы доказаны (Шнайдер, 1997).

1. For the sets *R* and *T,* there is a rank function **ρ: M→Z:** $\forall\, m \in$ **IK** $\bullet\ \rho\,(m) > 0$
2. $\forall$ **S** $\subseteq$ M, $m \in$ M $\bullet\ ((\forall m' \in$ **S** $\bullet\ \rho\,(m') > 0)$ ^ **S** $\vdash m) \Rightarrow \rho\,(m) > 0$
3. $\forall\, t \in$ **T** $\bullet\ \rho\,(t) \leq 0$
4. $\forall\, i \in$ **U** $\bullet$ *User*$_i$ ‖ *Stop* **maintains** ρ

R

then NET **sat** *R* **precedes T**

3. Незавершенные работы:

Несмотря на наличие большого числа подходов к аутентификации, повышающих уровень защиты сети, различные виды атак продолжают появляться.

Предлагаемая схема (Кирсал, 2005) была разработана для обеспечения аутентификации доверенной третьей стороной для беспроводных сетей, в которых требуется обеспечить высокий уровень защиты. Кроме того, сценарий предлагаемого протокола представляет собой комбинацию протокола Керберос и протокола обмена зашифрованными ключами (Кирсал, 2006). Так как предлагаемый протокол является протоколом защиты, основанным на временной модели, то в нем используются "штампы времени" для задержки дешифрования сообщений взломщиками. В предыдущем исследовании (Кирсал, 2007а) был предложен подход, предусматривающий закрытие внешнего доступа к сети на некоторый период времени (например, на 140 секунд) для того, чтобы можно было относительно безопасным способом распределить среди пользователей случайным образом сгенерированные ключи. Был разработан другой протокол, представляющий собой комбинацию протокола аутентификации Керберос и протокола обмена зашифрованными ключами (Кирсал, 2006) с добавлением свойства "задержки дешифрования" протокола аутентификации Керберос (Кирсал, 2007б). Показано, что, благодаря строгим правилам шифрования и спецификациям аутентификации никаких атак обнаружено не было, даже тогда, когда к разделу "Информация о нарушителе" ("#Intruder Information") были добавлены новые опции "Угадываемый" и "Вскрываемый" (Кирсал, 2008). Протокол, предлагаемый в настоящей работе, представляет собой одну из версий протокола, опубликованного в работе (Кирсал, 2008), в рамках схемы, разработанной в работе (Кирсал, 2007а). Предлагаемая система показана на Рис.1.

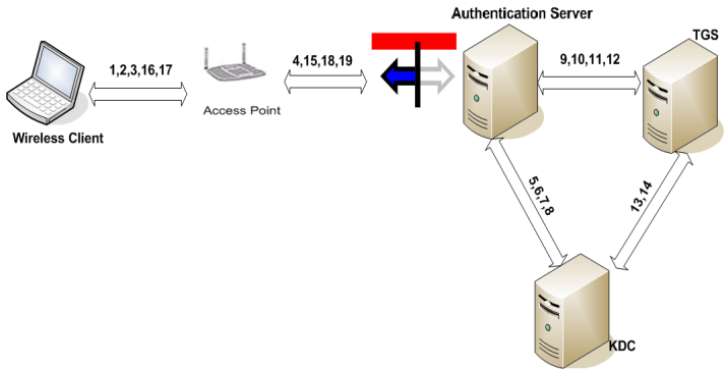


Рис.1. Предлагаемая схема

Приведенный ниже сценарий является частью сценария предлагаемого протокола:

#Processes

INITIATOR(A,S,na) knows SK(A), SKey(A), PK(A), passwd(A,B)

RESPONDER(B,S,nb) knows SK(B), SKey(B), passwd(A,B)

SERVER(S,kab) knows PK, SKey, passwd

```
#Protocol description
0. -> A : B
[A != B]
1. A -> S : {B}{SKey(A)}
2. S -> A : {S,A,ts,{kab}{PK(A)},PK(B)%pkb}{passwd(A,B)}
3. A -> B : {A, ts, na, {kab}{pkb % PK(B)}}{passwd(A,B)} % v
[A != B]
4. B -> S : {A}{SKey(B)}
5. S -> B : {S, B, PK(A) % pka}{passwd(A,B)}
[decryptable(v,pka) and nth(decrypt(v,pka),1)==A \
 and nth(decrypt(v,pka), 2) == now \
 and decryptable(nth(decrypt(v,pka), 3), passwd(A,B)) \
 and decryptable(nth(decrypt(v,pka), 4), SK(B))]
<na := nth (decrypt (nth(decrypt(v,pka), 3))) ; \
kab := nth (decrypt (nth(decrypt(v,pka), 4), SK(B)), 1)>
6. B -> A : {nb,na,tb}{kab}
7. A -> B : {nb,ta}{kab}
#Specification
TimedAgreement(A,B,2,[kab])
#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, Sam, Nm, PK, SPK, SK(Mallory), SKey(Mallory)}
Guessable = SessionKey
Crackable = SessionKey
Crackable = ServerKey
Crackable = Password
```

В разделе "Процессы" ("#Processes"), первый параметр каждого процесса (здесь A, B и S) должен представлять идентификацию личности агента, используемую в разделе "Описание протокола" ("#Protocol description"). Имена даются в соответствии с функциями, выполняемыми различными агентами. В данном протоколе были выбраны имена: ИНИЦИАТОР (INITIATOR), ОТВЕТЧИК (RESPONDER) и СЕРВЕР (SERVER) так, как они были использованы в протоколе в работе (Кирсал, 2007б, Кирсал, 2008).

В разделе "Описание протокола" сам протокол определяется перечислением шагов по порядку. Сообщение 0 используется для запуска протокола и сообщает A имя агента, с которым ему следует вести протокол. Так как указанный выше протокол основан на использовании времени, то в качестве переменных в сообщениях применяются штампы времени *ta*, *tb* и *ts*. Сообщения шифруются с помощью пароля, который создается A и B, а также распределяется сервером. Это увеличивает время, которое должно уйти у нарушителя для дешифрования данного сообщения. Кроме того, в разделе "Информация о нарушителе" ("#Intruder Information") первоначально указываются имя нарушителя и множество значений данных, которые ему известны (Кирсал, 2008), (Лоэв, 1998). В разделе "Знания нарушителя" ("Intruder knowledge") находятся идентификаторы и функции протокола, которые известны нарушителю, и он может придавать любые иные значения этим идентификаторам и функциям.

3.1 Модель CSP предлагаемого протокола:

В этом разделе моделируется представление предложенного выше протокола как сети с помощью алгебры CSP и определяется свойство аутентификации для этой сети как трассовая спецификация.

При моделировании различных процессов протокола возможность расширяемости системы CSP позволяет вводить в эти процессы дополнительные элементы.

Приведенные ниже сценарии являются представлениями трех участников предлагаемого протокола.

```
INITIATOR(A, S, na) =
 [] B : Agent @ A != B &env_I.A.(Env0, B,<>) ->
output.A.S.(Msg1, Encrypt.(SKey(A), <B>),<>) ->
[] kab : SessionKey @ [] ts : TS @ [] pkb : addGarbage_(PublicKey) @
    input.S.A.(Msg2, Encrypt.(passwd(A, B), <S, A, Timestamp.ts, Encrypt.(PK(A), <kab>), pkb>),<>) ->
   output.A.B.(Msg3, Encrypt.(passwd(A, B), <A, Timestamp.ts, na, Encrypt.(pkb, <kab>)>),<>) ->
   [] nb : Nonce @ [] tb : TS @
    input.B.A.(Msg6, Encrypt.(inverse(kab), <nb, na, Timestamp.tb>),<>) ->
   [] ta : TS @
    output.A.B.(Msg7, Encrypt.(kab, <nb, Timestamp.ta>),<nb>) ->
   close.A.INITIATOR_role -> STOP
 RESPONDER(B, S, nb) =
   [] A : Agent @
   [] v : addGarbage_({Encrypt.(passwd(A, B), <A, Timestamp.ts, na, Encrypt.(pkb,
<kab>)>) | A <- Agent, B <- Agent, kab <- SessionKey, na <- Nonce, ts <- TS, pkb <-
addGarbage_(PublicKey)}) @
    A != B & input.A.B.(Msg3, v,<>) ->
   output.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->
   [] pka : addGarbage_(PublicKey) @ [] now : TS @
    decryptable(v, pka) and nth(decrypt(v,pka), 1) == A and nth(decrypt(v,pka), 2) == now and
decryptable(nth(decrypt(v,pka), 3), passwd(A,B))  and decryptable(nth(decrypt(v,pka), 4), SK(B)) &
    input.S.B.(Msg5, Encrypt.(passwd(A, B), <S, B, pka>),<Timestamp.now>) ->
   RESPONDER'(B, S, nb, A, v, pka, nth(decrypt(nth(decrypt(v,pka),3))))
RESPONDER'(B, S, nb, A, v, pka, na) =
 RESPONDER''(B, S, nb, A, v, pka, na, nth(decrypt(nth(decrypt(v,pka),4),SK(B)),1))
RESPONDER''(B, S, nb, A, v, pka, na, kab) =
   [] tb : TS @
    output.B.A.(Msg6, Encrypt.(kab, <nb, na, Timestamp.tb>),<nb>) ->
   [] ta : TS @
    input.A.B.(Msg7, Encrypt.(inverse(kab), <nb, Timestamp.ta>),<nb>) ->
   close.B.RESPONDER_role -> STOP
SERVER(S, kab) =
   [] A : Agent @ [] B : Agent @
    input.A.S.(Msg1, Encrypt.(SKey(A),<B>),<>) ->
   [] ts : TS @
    output.S.A.(Msg2, Encrypt.(passwd(A, B), <S, A, Timestamp.ts, Encrypt.(PK(A), <kab>), PK(B)>),<>) ->
   input.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->
   output.S.B.(Msg5, Encrypt.(passwd(A, B), <S, B, PK(A)>),<>) ->
   close.S.SERVER_role -> STOP
```

В приведенной выше модели ключевые слова *"Ввод" (input)* и *"Вывод" (output)* используются для определения приложения получения и отправления, соответственно, при этом ключевые слова *trans* и *rec* являются общими определениями для этой цели, используемыми в определениях системы CSP в работах Шнайдера. Кроме того, вместо ключевых слов $USER_A$ (ПОЛЬЗОВАТЕЛЬ), $USER_B$, используются слова INITIATOR и RESPONDER.

Представление каждого процесса с помощью CSP (считающихся агентами) показывает, что объекты сообщений зашифрованы своими собственными публичными ключами.

ИНИЦИАТОР A создает и отправляет сообщение Msg3, а получатель B хранит это сообщение в переменной *v*, не пытаясь интерпретировать его. Иными словами, ОТВЕТЧИК B дешифрует это сообщение и выполняет соответствующие проверки только после получения сообщения на будущих шагах, которое определяется как Msg5. Сообщение 3 было зашифровано с помощью обратного ключа, полученного в сообщении 5. Так как полученный обратный пароль является самим паролем, то B ожидает обычного пароля. Это осуществляется в следующей части:

A != B & input.A.B.(Msg3, v,<>) ->

output.B.S.(Msg4, Encrypt.(SKey(B), <A>),<>) ->

[] pka : addGarbage_(PublicKey) @ [] now : TS

При проверке сообщения 5 функции "decryptable", "decrypt" и "nth(_, n)" используются для целей задержки дешифрования.

Благодаря использованию задержки дешифрования, B не может автоматически извлечь любые поля из сообщения 3, так что в модели задержки дешифрования требуется ввести дополнительные назначения. Эти дополнительные назначения определяются следующим образом:

RESPONDER'(B, S, nb, A, v, pka, nth(decrypt(nth(decrypt(v,pka),3))))

RESPONDER'(B, S, nb, A, v, pka, na) =

RESPONDER''(B, S, nb, A, v, pka, na, nth(decrypt(nth(decrypt(v,pka),4),SK(B)),1))

В первом назначении RESPONDER', назначает вектор инициализации (nonce) *na* в качестве третьего поля сообщения 3, а само сообщение, шифруется с помощью пароля A – B, приходится расшифровывать с помощью обратного ключа, который сам по себе является паролем.

Во втором назначении RESPONDER'(B, S, nb, A, v, pka, na) = RESPONDER''(B,.) назначает ключ сеанса *kab* в качестве четвертого компонента сообщения 3, в первое поле этого сообщения шифруется с помощью публичного ключа B, и дешифрование приходится осуществлять с помощью обращения этого ключа, что представляет собой секретный ключ B.

Так как предлагаемый протокол является чувствительным к времени, то введение любой задержки должно препятствовать любой попытке нарушителя запустить атаку. В связи с этим, используемый здесь метод задержки дешифрования предназначен для задержки действий нарушителя.

В разделе "Спецификация" ("#Specification") предлагаемого протокола ОТВЕТЧИК B закончил работу протокола при взаимодействии с A. Это проверяется с помощью приведенного ниже процесса CSP, который предполагает, что A работает с B по протоколу в течение последних 2 временных единиц и что между ними имеется взаимная договоренность. Эта взаимная договоренность зависит от значения выбранного ключа сеанса:

AuthenticateINITIATORToRESPONDERTimedAgreenent_

kab(A) = signal.Running1.INITIATOR_role.A?B?nb ->

signal.Commit1.RESPONDER_role.B.A.nb -> STOP

AlphaAuthenticateINITIATORToRESPONDERTimedAgreement_kab(A) =

{|signal.Running1.INITIATOR_role.A.B,

signal.Commit1.RESPONDER_role.B.A |

B <- inter(Agent, HONEST)|}

Нарушитель может попытаться предпринять первую попытку атаковать на шаге 3, когда A отправляет вектор инициализации (nonce) *na* в адрес B. Благодаря спецификации временного соглашения по протоколу, шансы агента попытаться осуществить соединение будут отменены сервером по времени в связи с безуспешными попытками соединения, предотвращая, таким образом, атаку.

В дополнение в штампам времени, для аутентификации между агентами A и B используются также векторы инициализации (nonces).

Кроме того, в разделе "Информация о нарушителе" первоначально указывается имя нарушителя и множество значений данных, которые ему известны. В разделе "Знания нарушителя" находятся идентификаторы и функции протокола, которые известны нарушителю, и он может придавать любые иные значения этим идентификаторам и функциям.

Приведенное ниже определение CSP представляет первоначальные значения нарушителя с определениями:

```
IK0_init = union({Alice, Bob, Mallory, Sam, Nm, SK(Mallory), SKey(Mallory),
passwd(Mallory, Alice), passwd(Mallory, Bob),          passwd(Alice, Mallory),
passwd(Bob, Mallory),
passwd(Mallory, Mallory), Garbage}, TimeStamp)
INTRUDER_1 =
   (chase(INTRUDER_0)
   [[ hear.m_ <- send.A_.B_.(l_,m_,se_) |
         (l_,m_,se_,re_) <- DIRECT_MSG,
 A_ <- diff(SenderType(l_),{Mallory}), B_ <- ReceiverType(l_) ]]
    [|{| hear |}|] STOP)
 [[ say.m_ <- receive.A_.B_.(l_,m_,re_) |
    (l_,m_,se_,re_) <- DIRECT_MSG,
 A_ <- SenderType(l_), B_<- ReceiverType(l_)]]
```

Работа нарушителя определена в приведенном выше коде вместе с ее связью с первоначальными знаниями.

Известные первоначально факты, которые добавляются в рамках приведенного ниже сеанса, – такие ключевые слова, как *leak, hear, say* – используются для сигнализации о том, что, возможно, секрет был раскрыт, для того, чтобы можно было слышать и произносить сообщение во время аутентификации и передавать сообщение по сети.

```
SAY_KNOWN_0 =
   (inter(IK1, ALL_SECRETS_DI) != {} & dummy_leak -> SAY_KNOWN_0)
   [] dummy_send -> SAY_KNOWN_0
   [] dummy_receive -> SAY_KNOWN_0
 SAY_KNOWN =
   SAY_KNOWN_0
    [[ dummy_leak <- leak.f_ | f_ <- inter(IK1, ALL_SECRETS_DI) ]]
    [[ dummy_send <- send.A_.B_.(l_,m_,se_) |
         (l_,m_,se_,re_) <- DIRECT_MSG, components_(m_) <= IK1,
```

```
        A_ <- diff(SenderType(l_),{Mallory}), B_ <- ReceiverType(l_) ]]
    [[ dummy_receive <- receive.A_.B_.(l_,m_,re_) |
        (l_,m_,se_,re_) <- DIRECT_MSG, components_(m_) <= IK1,
        A_ <- SenderType(l_), B_ <- ReceiverType(l_) ]]
STOP_SET = {| send.Mallory |}
 INTRUDER =
(INTRUDER_1 [| STOP_SET |] STOP) ||| SAY_KNOWN
IntruderInterface = Union({{| send, receive |}, {|crack|}})
AlphaSystem = {|env, send, receive, close, tock|}
SystemManagerInterface = inter(AlphaSystem,CRACKING_M::AlphaManager)
SYSTEM = (SYSTEM_M::TSYSTEM_1 [|SystemManagerInterface|] CRACKING_M::Manager)
        [|IntruderInterface|] INTRUDER_M::INTRUDER
```

Доказано, что, с точки зрения предотвращения атак, построенный протокол работает успешно, несмотря на детально определенные попытки осуществления связи нарушителем.

4. Обсуждение:

В настоящей работе предлагается подход к улучшению защитных свойств протокола аутентификации Керберос, а с также представление предлагаемого подхода с помощью процесса CSP.

Предлагаемый протокол, который содержит усовершенствования по сравнению с аутентификацией по протоколу Керберос, предназначен для повышения уровня защиты и минимизации угрозы возможных атак (Кирсал, 2007а,б и 2008).

Как указывалось в предыдущем разделе, в более раннем исследовании (Кирсал, 2007б) предусматривалось закрытие внешнего доступа к сети на некоторый период времени для того, чтобы можно было сравнительно безопасным способом распределить среди пользователей сгенерированные случайным образом ключи. Благодаря свойству задержки дешифрования протокола Керберос и в связи с тем, что этот протокол основан на аутентификации с использованием времени, доказано, что, с точки зрения предотвращения атак, этот протокол функционирует успешно, несмотря на серьезные попытки соединения со стороны нарушителей. Этот процесс исследуется с помощью подхода, который разработан Шнайдером для идентификации недостатков в структуре протокола.

В ходе реализации процесса удалось определить и исследовать атаки, которые рассматривались ранее.

5. Выводы:

В настоящей работе приводятся коды процесса CSP для нового протокола, предлагаемого для повышения уровня защиты протокола аутентификации Керберос. На основании разработанного и проверенного протокола (Кирсал, 2007а, 2007б) строится новый протокол с целью увеличения времени, которое потребуется нарушителю для взлома шифра, и, следовательно, повышения уровня безопасности.

Для обнаружения любых недостатков в конструкции протокола применяются процессы CSP, предложенные Шнайдером, что в результате позволяет идентифицировать атаки. Этот протокол основан на увеличении времени, которое потребуется нарушителю для взлома шифра, и, следовательно, он обеспечивает повышение уровня безопасности.

В дополнение к задержке дешифрования в настоящей работе предлагается повышение уровня защиты сети путем временного ограничения внешнего доступа к системе.

В дальнейшем будут выполнены работы по анализу производительности предлагаемого подхода для того, чтобы выбрать параметры для обеспечения приемлемого уровня безопасности и производительности.

6. Ссылки:

1. M. Abadi and R. Needham, "Prudent Engineering for Cryptographic Protocols." *IEEE Transactions on Software Engineering*, vol. 22(1): pp. 6-15, 1996.

2. S.M. Bellovin, and M. Merritt, "Limitations of the Kerberos Authentication System". *USENIX winter 1991,* pp.253-268. 1991.

3. A.H. Eneh., O. Gemikonakli and R. Comley, "Security of Electronic Commerce Authentication Protocols in Economically Deprived Communities", The Fifth Security Conference 2006, Las Vegas, Nevada, April 2006, ISBN: 0-9772107-2-3.

4. A.Harbitter and D. A. Menascé, "A Methodology for Analyzing the Performance of Authentication Protocols". *ACM Transactions on Information and System Security,* vol. 5(4): pp. 458-491, 2002.

5. C.A. Hoare, "Communication Sequence Process". *Prentice- Hall*, International Englewood Cliffs. New Jersey. 1985.

6. Y. Kirsal, A. Eneh and O. Gemikonakli, "A Solution to the Problem of Trusted Third Party for IEEE 802.11b Networks", *PGNET2005*, Liverpool UK, pp.333-339, 2005.

7. Y. Kirsal and O. Gemikonakli, "An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols", *CISSE 2006,* 2006.

8. Y. Kirsal and O. Gemikonakli, "Frequent Key Renewal under Pseudo-Secure Conditions for Increased Security in Kerberos Authentication and Its Impact On System Performability", *3rd International Conference on Global E-Security,* University of East London (UeL), Docklands, UK, 2007a.

9. Y.Kirsal and O.Gemikonakli, "Further Improvements to the Kerberos Timed Autentication Protocol", *CISSE 2007*, 2007b.

10. Y.Kirsal and O. Gemikonakli, "Improving Kerberos Security through the Combined Use of the Timed Authentication Protocol and Frequent Key Renewal", 6th IEEE International Conference on Cybernetic Systems 2008, Middlesex University, London, UK

11. G. Lowe, "An Attack on the Needham-Schroeder Public-key Authentication Protocol." *Information Processing Letters*. vol: 56(3), pp. 131-133, 1995.

12. G. Lowe, "Some New Attacks upon Security Protocols", *Proceedings of 9th IEEE Computer Security Workshops*, pp. 162 – 170, 1996.

13. G. Lowe, "CASPER: A Compiler for the Analysis of Security Protocols". *Proceedings of the 10th Computer Security Foundation Workshop.* pp.18-30., 1998

A. Mishra and W. A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", *White paper*, UMIACS-TR-2002-10, February 2002.

14. M. R. Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers." *Communication ACM* (21) pp.993–999, 1978.

A. W. Roscoe "CSP and Determinism in Security Modelling". *IEEE Symposium on Security and Privacy.* pp. 115-127, 1995.

15. S. Schneider. "Verifying authentication protocols with CSP" *10th Computer Security Foundations Workshop,* IEEE. pp. 741-758, 1997.

16. "Security White Paper Evolution, Requirements, and Options"

Доступен на сайте: http://wifiplanet.com/tutorials/articles.php/965471

[Составлено: 27 апреля 2005г.]

[Последняя ревизия: 13 сентября 2007г.]

Обмен электронными документами с ЭЦП по телекоммуникационным каналам связи в унифицированной системе приема, хранения и первичной обработки налоговых деклараций и бухгалтерской отчетности

Шалимов М.А.

Самарский государственный аэрокосмический университет им. академика С.П. Королева
г. Самара, Россия
mishmeister@yandex.ru

Exchange of electronic documents with the electronno-digital signature on telecommunication channels in a unified system for receiving, storing and processing tax declarations and accounting reports

Shalimov M.A.

The Samara state space university of academician S.P. Koroleva
Samara, Russia
mishmeister@yandex.ru

Цель работы

Цель данной работы заключается в автоматизации обмена электронными документами с электронно цифровой подписью по телекоммуникационным каналам связи между налогоплательщиками и налоговыми инспекциями.

Термины, используемые в работе

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Квитанция о приемке налоговой декларации (формы бухгалтерской отчетности) - электронный документ, формируемый налоговым органом и содержащий налоговую декларацию (форму бухгалтерской отчетности) в электронном виде, подписанную ЭЦП налогоплательщика и заверенную ЭЦП налогового органа;

Ключевой носитель – отчуждаемый носитель (дискета, eToken, и т.п.), содержащий один или несколько ключей ЭЦП.

Конфиденциальная информация - требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации.

Подтверждение отправки – содержащий ЭЦП электронный документ от налогового органа, в котором зафиксирована дата и время отправки налогоплательщиком налоговой декларации (бухгалтерской отчетности) в электронном виде по телекоммуникационным каналам связи.

Пользователь – налоговый орган или налогоплательщик (хозяйствующий субъект, в т.ч. кредитная организация), осуществляющий информационный обмен в рамках Системы.

Протокол входного контроля налоговой декларации (формы бухгалтерской отчетности) - электронный документ, формируемый налоговым органом и подписанный ЭЦП налогового органа, содержащий результаты проверки налоговой декларации (формы бухгалтерской отчетности) на соответствие требованиям утвержденного формата представления налоговой и бухгалтерской отчетности в электронном виде и правилам ее заполнения;

Система информационного обмена электронными документами с ЭЦП по телекоммуникационным каналам связи (далее – Система) - совокупность программных и аппаратных средств, обеспечивающих представление налоговой и бухгалтерской отчетности и информационных услуг в электронном виде по телекоммуникационным каналам связи, принадлежащая Участникам Системы, а также совокупность нормативных и организационно-методических документов, регламентирующих взаимоотношения Участников Системы;

Средства криптографической защиты информации (СКЗИ) – сертифицированные в порядке, установленном законодательством Российской Федерации аппаратные и (или) программные средства, обеспечивающие шифрование, контроль целостности и применение ЭЦП при обмене электронными документами в Системе и совместимые с СКЗИ, используемыми в системе ФНС России.

Электронный документ (ЭД) с ЭЦП – документ, в котором информация представлена в электронно-цифровой форме и содержащий ЭЦП.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

ЭЦП налогоплательщика – ЭЦП, владельцем сертификата ключа которой является должностное лицо налогоплательщика (хозяйствующего субъекта), использующее средства ЭЦП в рамках Системы.

ЭЦП налогового органа – ЭЦП, владельцем сертификата ключа которой является должностное лицо налогового органа, использующее средства ЭЦП в рамках Системы.

Общие положения

Пользователи должны применять для защиты информации средства ЭЦП и СКЗИ, сертифицированные в порядке, установленном законодательством Российской Федерации.

На основании федерального закона об электронно цифровой подписи используемые во взаимоотношениях между Пользователями электронные документы, заверенные ЭЦП, являются оригиналами, имеют юридическую силу, в соответствии с требованиями законодательства Российской Федерации подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

Пользователи признают, что применение в Системе сертифицированных средств ЭЦП и СКЗИ, которые реализуют ЭЦП и шифрование, достаточно для обеспечения конфиденциальности информационного взаимодействия, а также подтверждения того, что электронный документ:

исходит от Пользователя (подтверждение авторства документа);

не претерпел изменений при информационном взаимодействии Пользователей в рамках Системы (подтверждение целостности и подлинности документа).

Система строится по общим принципам, единым для всех Пользователей на территории Российской Федерации.

В рамках Системы Пользователи применяют разработанное или сертифицированное федеральным государственным унитарным предприятием "Главный научно-исследовательский вычислительный центр Федеральной Налоговой Службы".

Все электронные документы, квитанции и протоколы, передаваемые в рамках Системы, должны быть заверены ЭЦП отправителя и переданы по телекоммуникационным каналам связи только в зашифрованном виде.

Налогоплательщик подготавливает налоговые декларации (бухгалтерскую отчетность) в соответствии с утвержденными форматами в электронном виде с ЭЦП (набором ЭЦП) и представляет их по телекоммуникационным каналам связи в налоговый орган. При этом в соответствии с настоящим Регламентом, информационный обмен между налогоплательщиком и налоговым органом реализуется следующими электронными документами:

- подтверждение отправки, содержащее дату отправки налогоплательщиком налоговой декларации (бухгалтерской отчетности), формируемое в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности);
- протокол входного контроля налоговой декларации (бухгалтерской отчетности), формируемый в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности);
- квитанция о приемке налоговой декларации (бухгалтерской отчетности) в электронном виде, формируемая в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности).

Налогоплательщик, получивший подтверждение отправки, содержащее дату отправки налоговой декларации (бухгалтерской отчетности) в налоговый орган, проверяет подлинность ЭЦП в подтверждении отправки, заверяет подтверждение отправки ЭЦП налогоплательщика и в течение суток (без учета выходных и праздничных дней) высылает в адрес отправителя подтверждения. Налоговая декларация (бухгалтерская отчетность) считается представленной налогоплательщиком в налоговый орган. Подтверждение отправки, содержащее ЭЦП обеих сторон (отправителя и получателя), сохраняется как отправителем, так и получателем в соответствующих хранилищах электронных документов.

Налогоплательщик, получивший протокол входного контроля представленной налоговой декларации (бухгалтерской отчетности), проверяет подлинность содержащейся в протоколе ЭЦП налогового органа, заверяет протокол ЭЦП налогоплательщика и в течение суток (без учета выходных и праздничных дней) высылает в адрес налогового органа. Содержащий ЭЦП налогового органа и налогоплательщика протокол сохраняется в соответствующих хранилищах электронных документов.

Налогоплательщик, получивший квитанцию о приемке - представленную налогоплательщиком налоговую декларацию (бухгалтерскую отчетность) заверенную ЭЦП налогового органа, проверяет подлинность содержащейся в квитанции ЭЦП налогового органа и сохраняет квитанцию в хранилище электронных документов. Если в протоколе входного контроля содержится информация, что представленная налоговая декларация (бухгалтерская отчетность) содержит ошибки, налогоплательщик в течение пяти суток (без учета выходных и праздничных дней) устраняет указанные налоговым органом ошибки, заново подготавливает налоговую декларацию (бухгалтерскую отчетность) в электронном виде с ЭЦП и отправляет ее в адрес налогового органа, повторяя процедуру представления налоговой декларации (бухгалтерской отчетности).Если в течение шести часов с момента отправки налоговой декларации (бухгалтерской отчетности) налогоплательщик не получил из налогового органа протокол входного контроля и/или квитанцию о приемке представленной налоговой декларации (бухгалтерской отчетности), он заявляет в налоговый орган (или специализированному оператору связи, в случае представления налоговых деклараций (бухгалтерской отчетности) через специализированных операторов) о данном факте и, при необходимости, повторяет процедуру представления налоговой декларации (бухгалтерской отчетности).

Налоговая декларация (бухгалтерская отчетность) считается принятой налоговым органом по установленной форме в электронном виде в соответствии с законодательством Российской Федерации в случае, если налогоплательщик получил следующие электронные документы:

- формируемое налоговым органом подтверждение отправки, содержащее дату отправки налоговой декларации (бухгалтерской отчетности);
- формируемый налоговым органом протокол входного контроля, содержащий результаты проверки налоговой декларации (формы бухгалтерской отчетности) на соответствие требованиям утвержденного формата электронного представления;
- формируемую налоговым органом квитанцию о приемке - представленную налогоплательщиком налоговую декларацию (бухгалтерскую отчетность), заверенную ЭЦП налогового органа.

Описание работы системы

Для описания обмена электронными документами рассмотрим работу системы «ГНИВЦ ПРИЕМ регион» разработанную Федеральным государственным унитарным предприятием "Главный научно-исследовательский вычислительный центр Федеральной Налоговой Службы".

Система соответствует следующим приказам Федеральной налоговой службы РФ:

- Временному регламенту обмена электронными документами с ЭЦП по телекоммуникационным каналам связи в унифицированной системе приема, хранения и
- Первичной обработки налоговых деклараций и бухгалтерской отчетности, утвержденному приказом ФНС РФ от 12.12.2006 г. № САЭ-3-13/848@.
- Приказу № САЭ-3-27/346@ от 13.06.06г. «Об организации сети доверенных удостоверяющих центров»
- Приказу № ММ-3-13/469@ от 08.08.2007г. «Об утверждении унифицированного формата транспортного сообщения..».

Таким образом данная система обладает рядом преимуществ перед другими системами:

- Без спец операторная система сдачи, напрямую на сервер ГНИВЦ ФНС оперативность сдачи отчётов: своевременно приходящие подтверждения о доставке и протоколы проверки налоговых деклараций
- Сохранение конфиденциальности переданной информации: использование электронной цифровой подписи и средств шифрования данных
- Полное соответствие системы федеральным законам и нормативно правовым актам РФ,а так же приказам Федеральной налоговой службы РФ.

Пользователю выдается ключевой носитель – отчуждаемый носитель (дискета, eToken, и т.п.), содержащий один или несколько ключей ЭЦП, для дальнейшей подписи и шифрования документов. На Вычислительный прибор пользователя устанавливаются программные продукты необходимые для работы с ключевым носителем, например при работе с ключевым носителем типа eToken устанавливаются следующие программные продукты: «Aladin PKI client» и «КриптоПро CSP». Средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивает реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей. «Aladin PKI client» обеспечивает совместную работу программного продукта «КриптоПро CSP» с отчуждаемым ключевым носителем типа eToken.

Необходимо создать почтовую программу, способную загружать и обрабатывать налоговую и бухгалтерскую отчетность. Принцип работы программы заключается в следующем:

- Перед началом работы, программа должна проверить необходимые обновления на веб-сервере разработчика, и при необходимости предложить пользователю установить обновления.
- Необходимо реализовать механизм загрузки файлов отчетности в формате txt или xml, при этом должна присутствовать возможность проверить файл на соответствии принятым нормам выгружаемых деклараций.
- В соответствии с временным регламентом САЭ-3-13-848 от 12 декабря 2006г. Все электронные документы, квитанции и протоколы, передаваемые в рамках системы, должны быть заверены ЭЦП отправителя и переданы по телекоммуникационным каналам связи только в зашифрованном виде. Для этого необходима возможность совместного использования данной почтовой программы с программным продуктом «КриптоПро CSP». Почтовая программа должна подписывать и шифровать документы электронно цифровой подписью клиента.
- Необходимо реализовать возможность обмена электронными документами с сервером налоговой службы, при этом программа должна авторизоваться на почтовом сервере налоговой инспекции, проверять наличие входящих писем, проверять наличие готовых к отправке документов, и при наличии отправлять.

Заключение

Благодаря применению данной системы юридические лица и частные предприниматели могут сдавать отчетность через Интернет. Данная система удобна как пользователям, так и работникам налоговой службы. Благодаря системе уменьшается бумажный документооборот, упрощается процесс сдачи отчетности, налогоплательщикам не надо сдавать декларации на бумажных носителях, а следовательно экономиться время как налогоплательщиков так и работников налоговой службы.

Список используемой литературы

- Временный регламент САЭ -3-13-848 от 12 декабря 2006г.
- Постановление Правительства РФ №691 от 23 сентября 2002 г.
- Приказ ФСБ РФ № 66 от 9 февраля 2005 г.
- Федеральный закон об электронной подписи №1 от 26 декабря 2001 г.
- Приказ ФАПСИ от 13 июня 2001 г. N 152.
- Регламент удостоверяющего центра ООО «Гарант Телеком».

5 Секция

Образовательные проекты (программы и методики обучения) в области компьютерной безопасности

Educational projects (training programs and methods) in computer security

Учебный курс «Компьютерные угрозы: методы обнаружения и анализа»

Адамов А.С.
Соавторы: Кудина М.В., Чувило О.А., Сапрыкин А.С.

Харьковский Национальный Университет Радиоэлектроники
г. Харьков, Украина
alexander.adamov@dnt-lab.com

Training course "Computer threats: detection and analysis methods"

Adamov A.S.
co-authors: Kudina M.V., Chuvilo O.A., Saprykin A.S.

Kharkov National University of Radio electronics
Kharkov, Ukraine
alexander.adamov@dnt-lab.com

Курс «Компьютерные угрозы: методы обнаружения и анализа» содержит лекционные и лабораторные занятия на двух языках: русском и английском. Основной задачей курса является повышения уровня знаний студентов в области компьютерной безопасности. Рассмотрены основные типы компьютерных угроз, даны понятия и классификация вредоносных программ, современные виды сетевых атак, а также методы и средства защиты компьютерных систем и сетей. Кроме того, на лабораторных работах студенты получают базовые навыки обнаружения и анализа потенциально вредоносных программ: динамический и статический анализ.

Особое внимание уделено системам антивирусной защиты от Лаборатории Касперского для серверов и рабочих станций. В рамках курса студенты учатся работать с последними версиями продуктов,

такими как: KAV и KIS 2009. Для описания типов вредоносных программ в курсе используется классификация, разработанная Лабораторией Касперского.

На первых лекциях происходит знакомство с предметной областью вопроса. История создания вредоносных программ. Антивирусные системы и современные тенденции их развития. Сравнительный анализ антивирусов. Пути заражения компьютеров. Классификация вредоносных программ. Антивирусные технологии будущего поколения.

Отдельным пунктом в курсе идет актуальная на данный момент проблема мошенничества в Интернет, включающая лекции на следующие тематики: фишинг, банкинг, мошенничество в онлайн-играх. Также освещены вопросы безопасности и конфиденциальности в IP коммуникациях и в социальных сетях, атаки на которые сегодня пугают своей регулярностью.

В рамках курса «Компьютерные угрозы: методы обнаружения и анализа» мы постарались собрать максимально полезную, интересную и актуальную информацию о технологиях, которые используются вредоносным ПО:

- новое направление в скрытии информации - основы стеганографии;
- методы обфускации вредоносных программ;
- техники реверс-инжиниринга для вредоносных программ;
- технологии скрытия вредоносной активности в системе, руткит технологии;
- принципы использования эксплойтов;
- ботсети.

На лабораторных работах студенты учатся защищать ПК с помощью антивирусных продуктов и без них. Приобретают навыки работы с дизассемблером, а также опыт распаковки и расшифровки исполняемых файлов.

В лабораторной работе № 1 «Инсталляция и настройка Антивирус Касперского» учащиеся устанавливают продукт Kaspersky Internet Security 2009; знакомятся с назначением и функциями данного приложения; с его интерфейсом, с основными принципами работы.

Лабораторная работа № 2 «Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений» посвящена приобретению навыков обнаружения на компьютере вредоносных программ, изучению основных методов по устранению последствий вирусных инцидентов без использования антивирусного программного обеспечения. Также студенты знакомятся с определением вируса и вредоносных программ, с типами вредоносных программ и их описанием, с жизненными циклами различных типов вредоносных программ, с действиями червей при заражении компьютера, с возможностями лечения компьютеров без использования антивирусного программного обеспечения.

Лабораторная работа № 3 «Исследование уязвимостей Интернет браузеров в контексте новых веб технологий». Данная работа актуальна в свете встраивания вредоносных скриптов в популярные сайты. Предназначена для ознакомления студентов с содержанием современных угроз безопасности в Интернет; с сущностью понятия программной уязвимости; с принципами встраивания вредоносного кода в скрипты; с механизмом активации вредоносного кода.

В лабораторной работе № 4 «Основы работы с дизассемблером» изложены основы статического анализа программ с помощью дизассемблеров с целью обнаружения присутствия вредоносной составляющей. Студенты изучают основные приемы дизассемблирования приложений. Знакомятся с методами и средствами анализа программ; с интерфейсом и возможностями интерактивного дизассемблера IDA Pro; с базовыми приемами анализа Win32-программ.

В лабораторной работе № 5 «Технологии распаковки исполняемого кода» учащиеся получают навыки определения наличия упаковщика исполняемых файлов и его идентификации. Изучают особенности некоторых упаковщиков исполняемых файлов и методы распаковки\упаковки; методику восстановления распакованных файлов.

Основной особенностью курса является его актуальность. Материалы курса постоянно обновляются в соответствии с последними угрозами, появляющимися на просторах Интернет. Так, в свете последней эпидемии сетевого червя Kido (Conficker/Downadup), заразившего порядка 10 миллионов

компьютеров, в курс были включены материалы, посвященные описанию функциональности одной из версий червя.

На сегодняшний день курс включен в учебную программу Харьковского национального университета радиоэлектроники и читается иностранным магистрам и студентам 4 курса на русском и английском языке. Также проводятся факультативные занятия на базе клубной программы «Elite Teaching Club».

Хочется верить, что знания, полученные студентами, в рамках данного курса окажутся полезными и помогут защитить персональную информацию и предотвратить заражение компьютерных систем и сетей в каждом отдельном случае. Не стоит забывать, что установленный в системе антивирус не является гарантией ее безопасности. Важно знать, как можно сделать защиту компьютерной системы максимально эффективной, а также с какими типами современных угроз можно столкнуться сегодня в сети Интернет.

Учебная программная система для изучения методов криптографической защиты информации

Азизян Н.А., Косолапова Е.Н.

Государственный Инженерный Университет Армении (Политехник)
г. Ереван, Армения
ninaazizyan@rambler.ru

Educational software system for research into methods of the cryptographic protection of information

Azizyan N.A., Kosolapova Y.N.

State Engineering University of Armenia (Polytechnic)
Erevan, Armenia
ninaazizyan@rambler.ru

This program appears to be an effective arrangement for laboratory works in universities. It contains a great number of classical and modern cryptographic algorithms and their detailed descriptions, hesh functions, digital signatures and etc., and what is important, it is easy in use.

As of today, cryptography is one of the most widespread and effective means of protection of digital information. Wide development of the Internet has made it the most convenient and accessible means, of not only communication, but also of running the business. The demand is growing, for the products for protection of information, especially in Internet-applications. At that, considering the fact that the Internet is inherently available to all, there is a natural necessity of use of the means for protection of information, not only for provision of confidentiality, but also for authentication of users. It is a weighty argument for the benefit of urgency of cryptography studying, not only by the experts in the field of information technologies, but also by broad audience of users of computers and the Internet network. Therefore the fact is rather natural, that the interest towards cryptography and applied solutions on its basis, all over the world, has changed essentially. The sphere of application of cryptographic methods for protection of intellectual property has extended sharply. Researches in cryptography widen in private companies, which have not been earlier associated directly with information safety. The cryptography combines the methods of protection of information interactions of the various natures, based on data transformation using confidential algorithms, including algorithms that use confidential parameters. The term "information interaction" or "process of information interaction" designates here such a process of interaction between two and more subjects, the basic content of which consists in transfer and/or processing of information. There are not many basic methods of transformation of information which the modern cryptography has, but all of them are "bricks" for the creation of applied systems.

Considering all the above, it is possible to draw conclusions, that in our age of information technologies, when the information represents one of the most valuable phenomena on Earth, how important it is for any state to train highly skilled experts in the field of information protection.

Certainly, big role in preparation of the respective personnel is given to higher educational institutions; however, this problem is not as simple as it seems at first glance, because the cryptography contains rather complex mathematics in its modern form. Beginning of training of those students having no idea about cryptography and cryptanalysis, with modern algorithms which are complex enough in both their logic, and in mathematics contained in them, would not be expedient. It would be rather correctly to start training according to historical development of cryptography (starting from classical algorithms and finishing with modern ones), which makes a successful practise at our university.

In this connection, there was necessary to create software for laboratory studying and research of cryptographic methods, which software could provide flexible change-over of the complexes of laboratory works according to particular curriculum of the discipline. As a result, an educational research cryptographic system has been created, which includes the most widespread and known cryptographic algorithms (both modern and classical), enables to carry out simple cryptanalysis operations; it has friendly interface, i.e. it is convenient and clear to work with. The interface of the system has been realized in Armenian, according to the language of training at our university, however, since the code of the system is open (open source), in case where desirable, it would be possible to translate it for working in other languages, and also, supplement with new cryptographic algorithms.

Generalizing all listed above, one can come to conclusion that the given programme presents efficient means for carrying out laboratory works with those students studying cryptography, and also for those persons interested in cryptography, since it contains large enough number of classical algorithms, as well as those urgent as of today, along with their descriptions, digital signatures, hashing functions, contains stage-by-stage educational demonstration of the most complex and interesting algorithms, and which is important, the programme is rather simple in use.

На сегодняшний день криптография является одним из наиболее распространенных и эффективных средств защиты цифровой информации. Широкое развитие Интернета сделало его наиболее удобным и доступным средством не только общения, но и ведения бизнеса. Растет спрос на продукты для защиты информации, особенно в Internet-приложениях. При этом с учетом того, что Интернет по своей сути является общедоступным, возникает естественная необходимость использования средств защиты информации, не только для обеспечения конфиденциальности, но и для аутентификации пользователей. Это является веским доводом в пользу актуальности изучения криптографии не только специалистами в области информационных технологий, но и широким кругом пользователей компьютеров и сети Интернет. Поэтому довольно естественным является тот факт, что во всем мире существенно изменился интерес к криптографии и прикладным решениям на ее основе. Резко расширилась сфера применения криптографических методов для защиты интеллектуальной собственности. Расширяются исследования по криптографии в частных компаниях, ранее не связанных напрямую с информационной безопасностью. Криптография объединяет методы защиты информационных взаимодействий различного характера, опирающиеся на преобразование данных по секретным алгоритмам, включая алгоритмы, использующие секретные параметры. Термин «информационное взаимодействие» или «процесс информационного взаимодействия» здесь обозначает такой процесс взаимодействия двух и более субъектов, основным содержанием которого является передача и/или обработка информации. Базовых методов преобразования информации, которыми располагает современная криптография немного, но все они являются «кирпичами» для создания прикладных систем.

Учитывая все вышеперечисленное, можно сделать выводы, что в наш век информационных технологий, когда информация представляет собой одно из ценнейших явлений на земле, насколько важно для любого государства готовить высококвалифицированных специалистов в области защиты информации.

Конечно же, большую роль в подготовке соответствующих кадров играют высшие учебные заведения, однако задача эта не так проста, как кажется на первый взгляд, потому что криптография в современном ее виде содержит довольно сложную математику. Начинать обучение студентов, не имеющих никакого представления о криптографии и криптоанализе с современных алгоритмов, которые достаточно сложны как по своей логике, так и по содержащейся в них математике, не является целесообразным. Правильнее всего начинать обучение согласно историческому развитию криптографии (начиная с классических алгоритмов и кончая современными), что успешно практикуется в нашем университете.

В связи с этим стало необходимым создание программного средства для лабораторного изучения и исследования криптографических методов, которое может обеспечить гибкую перенастройку комплексов лабораторных работ в соответствии с конкретным учебным планом дисциплины. В результате создана учебная исследовательская криптографическая система, которая включает самые распространенные и известные криптографические алгоритмы (как современные, так и классические), дает возможность проводить несложные криптоаналитические действия, имеет дружественный интерфейс, т. е. удобна и понятна для работы. Интерфейс системы реализован на армянском языке, в соответствии с языком обучения в нашем университете, однако поскольку код системы является открытым (opensource), то при желании его можно перевести для работы на других языках, а так же, дополнить новыми криптографическими алгоритмами.

Обобщая вышеперечисленное, можно сделать заключение о том, что данная программа является эффективным средством для проведения лабораторных работ со студентами, изучающими криптографию, а так же для лиц интересующихся криптографией, так как она содержит довольно большое количество классических, а также актуальных на сегодняшний день алгоритмов и их описаний, цифровые подписи, хеш функции, содержит поэтапные учебные показы наиболее сложных и интересных алгоритмов, и что немаловажно, программа довольно проста в использовании.

Формирование устойчивости к негативному влиянию интерне

Зорина И.В.

НИИРПО Департамента образования города Москвы
г. Москва

lisa14@inbox.ru

Developing resistance to the negative effects of the Internet

Zorina I.V.

Scientific Research Institute for the Development of Education
Moscow, Russia

lisa14@inbox.ru

To improve the quality of vocational education it is necessary to use Internet.

In project:

- It is determined Internet's resource for improving quality of vocational education.
- It is determined risks of negative influence of Internet.
- It is defined psychological and pedagogical abilities to resist against harmful influence of Internet.
- It is created recommendation for organization vocational education with effecter use of Internet.

В проекте:

- выявлены информационные ресурсы Интернет для повышения качества профессионального образования;
- выявлены основные факторы риска негативного влияния Сети;
- определены психолого - педагогические условия формирования устойчивости к вредному воздействию Интернет;
- разработана модель формирования устойчивости к негативному влиянию Интернет с использованием стрессора, в мотивационных целях.
- подготовлены рекомендации педагогам для организации профессионального образования с эффективным использованием учебной среды Интернет.

Обучение основам компьютерной безопасности младших школьников

Олевская Л.Н.

Ноябрьский Колледж профессиональных и информационных технологий
Ноябрьск, Россия
olevslud@yandex.ru;

Teaching primary school children the basics of computer security

Olevskaya L.N.

Noyabrsk Professional and Informational Technologies College
Noyabrsk, Russia
olevslud@yandex.ru

This work represents the program of extra curricular activity course“Computer security basis” for primary school children and the educational tasks set. Studying this program the pupils receive storage and finding information skills, introduce with the rules and methods of computer data protection. The program allows to form negative attitude to the legal offence in computer security field, to develop logical and critical pupil’s thinking, the ability to take a decision.

The barest necessity of modern education is the development of such methods in teaching and educational work, where the modern information technologies studying are harmoniously combined with the information culture formation in computer security field. Specified problems must be solved in the context of the subject “Information and Computer Technologues” at secondary school.

Teaching “Information” in the primary school in our days is the usual phenomenon, but the content of this course doesn’t reflect the computer security questions, as to our point of view is very important.

Computer security studying process will be maximum effective at primary school age. The childhood – is the age at person’s life when he learn and master the majority of information first of all that, which helps him to live in society.

The aim of this research work is to develop the program of computer security studying, adopted for primary school children.

The problems are the following:

- to prove the advisability and efficiency of studying computer security at primary school age;
- to develop the extra curricular activity course program “Computer security basis”;
- to work out the program methodical leading in the form of tasks set.

The extra curricular activity course program“Computer security basis” is developed as the result of this research work, which helps from the primary school age to inculcate the main storage and usage information skills, introduce with the rules and methods of computer data protection.

The main items of the program:

- information and its forms;
- information bearer;
- means and methods of information security;
- viruses and antiviral programs;

- Internet and its security;
- legal offence in computer security field.

В представленной работе разработана программа кружка «Основы компьютерной безопасности» для младшего школьного возраста, комплект учебных заданий. Обучаясь по программе, учащиеся получают навыки хранения и поиска информации, знакомятся с правилами и методами защиты компьютерных данных. Программа позволит сформировать негативное отношение к правовым нарушениям в области компьютерной безопасности, развивать логическое и критическое мышление школьников, умение принимать решения.

Насущной задачей современного образования становится разработка таких методов учебно-воспитательной работы, где бы гармонично сочеталось обучение современным информационным технологиям с формированием информационной культуры в области компьютерной безопасности. Обозначенные задачи должны решаться в рамках предмета «Информатика и ИКТ» средней школы.

Преподавание информатики в начальной школе в наши дни стало обычным явлением, однако содержание этого курса не отражает вопросы компьютерной безопасности, что на наш взгляд необходимо.

В младшем школьном возрасте процесс обучения компьютерной безопасности будет максимально эффективным. Детство – это та пора в жизни человека, когда он узнает и усваивает большое количество информации, прежде всего той, которая помогает ему жить в социуме.

Цель работы: разработать программу обучения компьютерной безопасности, адаптированную для младшего школьного возраста.

Задачи:

- обосновать целесообразность и эффективность обучения компьютерной безопасности в младшем школьном возрасте;
- провести отбор ученого материала в области компьютерной безопасности учитывая возраст учащихся;
- составить программу кружка «Основы компьютерной безопасности»;
- разработать методическое сопровождение программы в виде комплекта учебных заданий.

В результате проведенной работы разработана программа кружка «Основы компьютерной безопасности», которая позволит уже с младшего школьного возраста привить учащимся навыки хранения и использования информации, познакомить с правилами и методами защиты компьютерных данных, сформировать негативное отношение к правовым нарушениям в области компьютерной безопасности.

Основные направления программы:

- Информация и её виды;
- Носители информации;
- Средства и методы защиты информации;
- Вирусы и антивирусные программы;
- Интернет и безопасность;
- Правовые нарушения в области компьютерной безопасности.

Программа содержит:

- Планируемые результаты обучения;
- Примерный перечень формируемых компетенций, получаемых знаний, осваиваемых умений и приобретаемых навыков;
- Формы и методы организации учебной деятельности учащихся в процессе обучения;

- Примерное тематическое планирование занятий.

Сформированный комплект заданий позволит закрепить изученный учебный материал, направлен на развитие критического мышления, умения логически мыслить принимать решения.

Практическая значимость работы заключается в возможности применения разработанной программы и комплекта заданий в образовательной деятельности в области информационных технологий.

6 Секция

Спам. Методы обнаружения спама с анализом содержимого и без него. Фишинг

Spam: detecting spam with and without content analysis. Phishing

Автоматизированный контент-анализ спам-сообщений на различных языках. Концептуальный анализ

Ермакова Л.М.

Пермский государственный университет
г. Пермь, Россия
liana87@mail.ru

The automated content-analysis of spams messages in various languages. A conceptual analysis

Ermakova L.M.

Perm state university
Perm, Russia
liana87@mail.ru

The main objective of this research is to develop and to investigate methods of spam detection based on content analysis and linguistic corpora. Neural network and algorithm of BPE were implemented. This technique can be used for both languages: English and French.

Every positive phenomenon has underside, and, for example, rapid growth of the popularity of e-mail is accompanied by increase of the flow of unauthorised mass distributions, frequently using the means of social engineering.

Spam – *is anonymous non-requested mass dispatching of e-mail messages.*

According to Kaspersky's Laboratory, today from 80 to 97% of all electronic messages in the Internet is a spam. There are various methods of fighting spam (maintaining blacklists, search of spammer's tricks, Bayesian lexical filtration, detection of mass dispatches of the same kind, etc.), but none of them gives a hundred-percent guarantee of protection against undesirable dispatches. Combined application of semantic methods with other methods of filtration of the correspondence essentially increases their efficiency; however, semantic analysis has not yet appeared beyond the thresholds of research laboratories. In addition, the spam is multilingual, and it is important to correctly sort it, not having lost really necessary messages,

which is especially important for the business-users conducting extensive correspondence with foreign contractors.

On the basis of comparative and descriptive analyses we have carried out classification of spam, analysed grammatical, lexical and syntactical features, and determined their frequency of occurrence, having revealed, in particular, a significant role of emotive vocabulary. As a result, we have constructed mathematical model of spam-message which in large enough percentage of cases gives exact result during automatic screening of spam of messages. The basis of this model is formed by neural network with application of algorithm of reverse distribution of mistake, and the task of identification of spam was reduced to the following stages:

1. definition of specific grammatical means used by spammers;
2. definition of emotive means;
3. classification of spam;
4. review of the methods of social engineering;
5. construction of recognition algorithm on the basis of artificial neural networks;
6. training of neural network;
7. carrying out research using methods of case linguistics;
8. conceptual analysis;
9. reveal similarities and distinctions between messages in French and English languages.

As a result of research, a programme was realised, capable to determine, whether the message is spam, based on the entered text.

The programme operates for 2 languages: English and French.

The realised neural network uses 8 basic attributes:

1. percentage of pronouns and possessive determinatives
2. presence of appeal
3. presence of link
4. presence of lists
5. presence of the symbol @
6. proposal not to receive such letters any more
7. the letter begins with interrogative or exclamatory sentence
8. graphical highlighting of individual words

In case of English language, filtration based on presence of "formulas of politeness" is also used. It has been revealed, that the first attribute is extremely important for French language, but in English its role is a bit smaller.

The constructed model of content filtration allows to determine with high accuracy, whether the message is a spam. In the control sample, the result appeared to be authentic in 95% of cases. At that, 1% of spam-messages is passed. The number of false operations makes 4%. All false operations relate to generated letters (automatic notices, advertising dispatches, and so forth). It is concerned with their linguistic features. In addition, users frequently relate such letters to spam. This is a so-called intermediate zone – "semi-spam". With a high degree of confidence one can say, that attribution of such a message to the category of doubtful letters is not critical for user.

Conceptual analysis enables to reveal semantic dominant of a message. During the research, key concepts of spam-messages were revealed. Having revealed the concept which is the main for the received message, it would be possible to attribute this message, with some degree of confidence, to spam or non-spam. For realisation of this method, neural networks would be the most suitable, since they are not determined and capable of training. Revealing of dominating concepts in legal correspondence is possible. On the basis of the main concepts of spam and dominating concepts of e-mail, it would be possible to construct a vector of incoming attributes. In combination with already found attributes, it would be possible to obtain an effective method of spam filtration.

Advantages of this technology consist in the following:

1. Opportunity of combined application along with available technologies (the majority of existing spam-filters work with lexical aspect of language, whereas the grammar also plays an important role in classification of correspondence; combined application of analyses of various language levels is capable of increasing the efficiency of filtration)
2. Universality (suitable for different types of spam).
3. Scalability.
4. Ease of updating (possibility of updating of weight factors only, rather than the whole bases).
5. Possibility to make computations in parallel (for example, paralleling of computations in the neural network, or search of attributes).

Thus, the obtained results allow to say that there are prerequisites for creation of spam-filter of a new generation, based on linguistic features of undesirable dispatch, much more efficiently, than those methods widely used today, based on the analysis of words contained in the text.

In future, it is planned to:

- Reveal new attributes and update those results already available.
- Realise the algorithm of automatic determination of the quantity of neurons of the intermediate layer.
- Further train the neural network.
- Further investigate similarities and distinctions between messages in various languages.
- Acquire new statistical data.
- Create a parser for French and Russian language, for the purpose of revelation of new attributes and realisation of automatic search of attributes, which was suspended because of the absence of grammatical parser.
- Expand the area of application of the realised neural network to include Russian language.

Create a new spam-filter, which could be used in combination with the available technologies.

У любого положительного явления есть обратная сторона и, например, быстрый рост популярности электронной почты сопровождается увеличением потока несанкционированных массовых рассылок, зачастую использующих средства социальной инженерии.

Спам - *это анонимные незапрошенные массовые рассылки электронной почты.*

По данным Лаборатории Касперского сегодня от 80 до 97% всех электронных сообщений в Internet – спам. Существуют различные методы борьбы со спамом (ведение черных списков, поиск спамерских трюков, байесовской лексической фильтрации, обнаружение массовых однотипных рассылок и др.), но ни один из них не дает стопроцентной гарантии защиты от нежелательных рассылок. Совместное использование семантических методов с другими способами фильтрации корреспонденции существенно увеличивает их эффективность, однако семантический анализ пока не вышел за пороги исследовательских лабораторий. Кроме того, спам многоязычен и важно корректно его отсортировать, не потеряв действительно нужные послания, что особенно важно для бизнес-пользователей, ведущих обширную переписку с зарубежными контрагентами.

На основе сравнительного и описательного анализов мы провели классификацию спама, проанализировали грамматические, лексические и синтаксические особенности, определили их частотность, выявив, в частности, значительную роль эмотивной лексики. В результате мы построили математическую модель спам-сообщения, которая в достаточно большом проценте случаев дает точный результат при автоматическом отсеивании спам -сообщений. В основе этой модели лежит нейронная сеть с применением алгоритма обратного распространения ошибки и задача распознавания спама свелась к следующим этапам:

1. определение специфических грамматических средств, используемых спамерами;
2. определение эмотивных средств;
3. классификация спама;

4. обзор методов социальной инженерии
5. построение алгоритма распознавания на основе искусственных нейронных сетей;
6. обучение нейронной сети
7. проведение исследования методами корпусной лингвистики
8. концептуальный анализ
9. выявить сходства и различия между сообщениями на французском и английском языках

В результате исследований была реализована программа, способная по введенному тексту определить, является ли сообщение спамом.

Программа работает для 2 языков: английского и французского.

Реализованная нейронная сеть использует 8 основных признаков:

1. процентное содержание местоимений и притяжательных детерминативов
2. наличие обращения
3. наличие ссылки
4. наличие списков
5. наличие символа @
6. предложение больше не получать такие письма
7. письмо начинается с вопросительного или восклицательного предложения
8. графическое выделение отдельных слов

В случае английского языка также используется фильтрация по наличию «формул вежливости». Было выявлено, что первый признак является чрезвычайно важным для французского языка, но в английском его роль несколько меньше.

Построенная модель контентной фильтрации позволяет с большой точностью определить, является ли сообщение спамом. На контрольной выборке результат оказался достоверным в 95% случаев. При этом пропускается 1% спам-сообщений. Число ложных срабатываний составляет 4%. Все ложные срабатывания относятся к сгенерированным письмам (автоматическим уведомлениям, рекламным рассылкам и пр.). Это связано с их лингвистическими особенностями. Кроме того, зачастую сами пользователи относят подобные письма к спаму. Это так называемая промежуточная зона – «полуспам». С большой долей уверенности можно сказать, что отнесение такого сообщения к разряду сомнительных писем не является критичной для пользователя.

Концептуальный анализ дает возможность выявить семантическую доминанту сообщения. В процессе исследования были выявлены ключевые концепты спам-сообщений. Выявив концепт, который является главным для полученного сообщения, можно с некоторой долей уверенности отнести это сообщение к спаму или неспаму. Для реализации этого метода лучше всего подходят нейронные сети, т.к. они не детерминированы и способны к обучению. Возможно выявление доминирующих концептов в легальной корреспонденции. На основе главных концептов спама и доминирующих концептов электронной почты можно построить вектор входных признаков. В сочетании с уже найденными признаками можно получить эффективный метод фильтрации спама.

Преимущества данной технологии заключаются в следующем:

6. Возможность совместного использования с имеющимися технологиями (большинство существующих спам-фильтров работают с лексическим аспектом языка, в то время как грамматика также играет немаловажную роль в классификации корреспонденции; совместное применение анализов различных языковых уровней способно увеличить эффективность фильтрации)
7. Универсальность (подходит к разным типам спама)
8. Расширяемость
9. Легкость обновления (возможность обновлять не целые базы, а только весовые коэффициенты)

10. Возможность сделать вычисления параллельными (например, распараллелить вычисления нейронной сети или поиск признаков)

Таким образом, полученные результаты позволяют говорить о том, что существуют предпосылки для создания спам-фильтра нового поколения, основанного на языковых особенностях нежелательной рассылки, гораздо более эффективного, чем широко используемые в наши дни, основанные на анализе содержащихся в тексте слов, методы.

В дальнейшем планируется:

- Выявление новых признаков и корректировка уже имеющихся результатов.
- Реализация алгоритма автоматического определения количества нейронов промежуточного слоя
- Дальнейшее обучение нейронной сети
- Дальнейшее исследование сходств и различий между сообщениями на различных языках
- Получение новых статистических данных
- Создание парсера для французского и русского языков с целью выявления новых признаков и реализации автоматического поиска признаков, который был приостановлен из-за отсутствия грамматического парсера
- Расширить область применения реализованной нейронной сети на русский язык

Создание нового спам-фильтра, который можно будет использовать совместно с имеющимися технологиями

Методы обнаружения спама без анализа содержимого текста сообщения

Кириченко С.

Самарский государственный аэрокосмический университет им. академика С.П. Королева

г. Самара, Россия

ank@ssau.ru

Methods of detecting spam without analysis of the message text

Kirichenko S.

The Samara state space university of academician S.P. Koroleva

Samara, Russia

ank@ssau.ru

При рассмотрении и изучении какого-либо явления, необходимо его четко определить. При рассмотрении проблем, связанных со "спамом" это особенно важно, так как имеется большое количество различных определений, многие из которых слишком расплывчаты для практического использования. В тексте этой статьи использованы такие определения:

- **Спам** - *анонимная незапрошенная массовая рассылка электронной почты.* Все эпитеты в определении являются важными, другие виды массовых рассылок почты в данном тексте спамом не считаются. Большинство спам рассылок носят рекламный или другой коммерческий характер, это важно при рассмотрении экономики спама, но не так важно с технической точки зрения. ICQ, SMS и другие подобные рассылки в статье не рассматриваются.
- **Легальная рассылка** - *массовая рассылка электронной почты, запрошенная пользователем.* Предполагается, что пользователь легальной рассылки изъявил желание ее получать. Как правило, легальные рассылки не анонимны.
- **Обычная или легальная электронная почта** - *электронная почта между пользователями, либо между автоматическими системами и пользователями.* Обычная почта в первую очередь не является массовой, получателей отдельного сообщения обычно единицы.

В рамках отдельной почтовой системы видна только часть общей картины - спам приходит со сравнительно небольшого количества IP-адресов, имеет относительно небольшое число модификаций, единичная рассылка продолжается небольшое время. Более полную картину происходящего имеют крупные почтовые системы и провайдеры с миллионами пользователей, однако полной картиной не обладают и они.

В то же время, единичная рассылка на миллионы адресов занимает существенное время - от нескольких часов до нескольких суток. Если обнаружить ее "на старте" и каким-либо образом блокировать, то ущерб от спама понесут только те пользователи, чьи адреса были использованы в начале рассылки. Другими словами, необходимо собирать данные о спам-почте из максимально-возможного количества точек сети, обрабатывать их максимально быстро и делать доступными данные о происходящей в настоящее время рассылке для всех участников системы.

В настоящее время реализованы такие методы быстрого сбора данных о рассылках (перечислены в порядке убывания распространенности в мире):

- прием спама в специальные "ловушки" (honeypot) - E-mail адреса, предназначенные только для приема спама;
- голосование пользователей - пользователь, получивший спам, нотифицирует об этом систему сбора данных, предоставляя образец спама;
- анализ всей проходящей через почтовую систему почты с сообщением контрольных сумм отдельных сообщений на центральный сервер.

На основании собранных данных, которые выглядят как "такое-то письмо принято в мире столько-то раз", либо "на такое-то письмо пожаловались столько-то раз", строятся списки массовых на данный момент времени рассылок, которые становятся доступными участникам системы в реальном времени. Почтовые системы, приняв письмо, могут узнать его статус и либо отвергнуть (уничтожить, перенаправить в архив или карантин) как спам, либо передать получателю.

Сбор спама с помощью адресов -"ловушек"

Наиболее крупная сеть адресов-ловушек для анализа спама в реальном времени организована и поддерживается компанией Brightmail (www.brightmail.com). Детали реализации известны только из публикуемых этой компанией документов, согласно им сеть сбора спама состоит более чем из миллиона почтовых адресов-ловушек; данные по спаму пополняются и пользователями самой системы. На основании полученных спам-сообщений составляются списки сигнатур сообщений и списки правил анализа заголовков, которые доставляются подписчикам системы практически в реальном времени. Согласно публикациям компании Brightmail, ею используются как четкие сигнатуры (hashes), идентифицирующие в точности данное сообщение, так и нечеткие, которые приспосабливаются к меняющимся спамерским письмам.

Решение Brightmail Anti-Spam доступно только на коммерческой основе в виде plug-in к системам Sendmail и MS Exchange, online-сервиса и в составе некоторых сетевых устройств (Network Appliances).

Вследствие коммерческого характера системы получить данные об ее пригодности для фильтрации российского спама затруднительно. Доступны лишь данные тестов PC Magazine, согласно которым уровень обнаружения спама составил 77.79%, а уровень ложных срабатываний системы - 0.05% всех сообщений.

Аналогичная схема сбора образцов спама реализована в системе SkyScan AS компании MessageLabs. На основе маркетинговых документов компании, можно предположить, что используемые методы очень похожи на систему Brightmail; как и в случае Brightmail существенная информация о системе практически нигде не опубликована.

В тестах PC Magazine сервис SkyScan показал уровень обнаружения спама в 96% при доле ложных срабатываний 0.48%

Поддержание большого числа адресов-ловушек требует больших человеческих и административных ресурсов - это не должны быть "пустые" адреса, они должны активно функционировать - публиковаться на WWW-сайтах, форумах и конференциях, регистрироваться в онлайн-сервисах и прочим образом имитировать поведение обычного пользователя с точки зрения спамера. По всей видимости, данная технология применима только в условиях компании-разработчика антиспамерского ПО, либо в условиях крупного почтового сервиса. Создание подобной системы на базе только усилий волонтеров представляется маловероятным.

Голосование пользователей

Метод распределенного обнаружения спама методом голосования пользователей заключается в следующем:

1. Почтовая система, принявшая письмо, рассчитывает его сигнатуру, передает ее на сервер системы обнаружения и получает ответ - спам это или нет.

2. Если пользователь получил письмо, которое он считает спамом, то он может проголосовать "против него" - переправив в систему сбора данных сообщение о том, что данное письмо является спамом,

3. Если одно письмо (одна сигнатура) имеет достаточно много голосов "против", то система сбора данных считает данное письмо спамом.

Вышеописанная схема реализована в системе Vipul's Razor/Cloudmark SpamNet. Эта система включает в себя:

- сеть серверов под управлением компании Cloudmark;
- бесплатное клиентское ПО для Unix (как для почтовых серверов, так и для почтовых клиентов) и бесплатное право использования серверов системы;
- платная подписка на сервис для клиентов Windows

- платное серверное ПО для Windows-серверов и подписка на сервис для корпоративных пользователей.

Исходно система Vipul's Razor была целиком бесплатной, однако после выхода Razor Version 2 (Razor v2, июнь 2002 года) установилась описанная выше схема -бесплатные версии для Unix-систем и платные для Windows.

В Razor v2 используются как четкие контрольные суммы текста письма (SHA1) , так и два варианта нечетких:

- Nilsimsa (lexx.shinn.net/cmeclax/nilsimsa.html)- метод расчета нечетких сигнатур, которые слабо меняются при небольшом изменении исходных данных (в настоящее время этот способ не используется т.к. метод Nilsimsa давал заметное число ложных срабатываний)
- Ephemeral Signatures - короткоживущие сигнатуры, основанные на случайном выборе кусочков текста для их построения (сервер сообщает клиенту необходимые данные для выбора, клиент осуществляет выбор и расчет сигнатуры). Считается, что такие сигнатуры спамерам сложно подделать, так как заранее неизвестно, какие участки текста сообщения будут использованы для анализа письма.

Клиентское ПО Razor/SpamNet поддерживает механизмы голосования "против" текста сообщения (т.е. за признание его спамом) и голосование "за" (т.е. реакция на ложные срабатывания системы). Для поддержки Ephemeral Signatures письмо при голосовании передается на сервер целиком.

Клиенты регистрируются на сервере, получая уникальный идентификатор, используемый в дальнейшем при голосованиях. Поддерживается "Truth Evaluation System" - система расчета уровня доверия к отдельным голосующим пользователям, основанная, по всей видимости, на сравнении похожести распределения голосований данного пользователя со средним по системе в целом.

Правила системы запрещают автоматическое голосование "против", за исключением использования адресов-ловушек.

Статистика и качество работы системы Razor/ SpamNet:

В настоящее время система обрабатывает более 100 млн. сообщений в сутки.

Согласно документам Cloudmark, уровень обнаружения спама данной системой достигает 95%. С другой стороны, статистика, публикуемая на сайте Cloudmark.com, показывает, что доля обнаруженного спама во всем потоке почты составляет около 25%. Так как общая доля спама в почте в настоящее время составляет около половины (по данным Brightmail, MessageLabs и самой Cloudmark), то получается, что на самом деле система Razor/SpamNet обнаруживает порядка 50% спама.

Согласно тестам PC Magazine, уровень обнаружения спама этой системой составляет 83%, уровень ложных срабатываний - 6.7%

Для спама, получаемого в России, качество работы Razor существенно хуже - по тестам автора на выборке из 11600 спам-сообщений, уровень обнаружения спама равен 10%, хотя уровень ложных срабатываний крайне низок (одно сообщение на 5000). По всей видимости, распространенность Razor в России невелика, соответственно и сигнатур русскоязычных писем в базе практически не имеется.

Проект Pyzor (pyzor.sourceforge.net) был начат, как клиент к Razor, написанный на языке Python. Однако автора (Frank Tobin) беспокоил тот факт, что серверная часть системы Razor не является открытой (недоступна как в виде исходных текстов, так и в виде исполняемых модулей), в результате Pyzor в настоящее время реализует свой алгоритм подсчета контрольных сумм (дайджест SHA по тексту письма, очищенному от html-тегов) и имеет отдельный сервер контрольных сумм. Объединение Pyzor-серверов в общую сеть и обмен данных между серверами не предусмотрены.

Судя по всему, проект заброшен автором и никем более не развивается. В данном обзоре Pyzor упомянут для полноты картины.

Анализ всей поступающей почты

Анализ всей проходящей через почтовую систему почты подразумевает, что для каждого почтового сообщения генерируются контрольные суммы, которые передаются на сервер сбора статистики. В ответ сервер сообщает количество зарегистрированных повторов данного письма. Начиная с некоторого количества повторов можно считать данное письмо спамом. Очевидно, что подобная

технология не будет отличать легальные массовые рассылки от спама, следовательно, требуются "белые списки" в которые такие рассылки будут внесены.

Данная технология реализована в проекте DCC - Distributed Checksum Clearinghouse (www.rhyolite.com/anti-spam/dcc/). Программное обеспечение DCC распространяется в исходных кодах по очень либеральной лицензии. Пользователям доступен как клиент, который может быть использован с имеющейся сетью DCC-серверов, так и свой сервер, который можно установить либо независимо, либо включить в общую DCC-сеть. Включенные в DCC-сеть сервера обмениваются данными о частотных контрольных суммах практически в реальном времени.

Система DCC поддерживает как анонимных, так и авторизованных клиентов. DCC-сервер можно сконфигурировать так, чтобы сообщения о спаме он принимал только от авторизованных пользователей. В системе реализован и аналог механизма голосования - отдельное сообщение (его контрольная сумма) может быть явно помечено как "спам" или "не спам".

В системе используется сразу несколько типов контрольных сумм - четкая сумма MD5 по всему тексту сообщения, отдельные контрольные суммы по адресам отправителя, получателей и части заголовков письма и два типа нечетких сумм, рассчитанных на работу с меняющимся текстом письма.

В настоящее время публичная сеть DCC обрабатывает около 40 млн. "уникальных сообщений" в сутки (публикуемая статистика не учитывает число отдельных получателей каждого письма), но не имея доступа к детальной информации у нас нет возможности перевести это число в привычные единицы. Точно так же, публикуемая статистика по обнаруженному спаму - около 30% в среднем - приводится в уникальных сообщениях, перевести это в "обычные проценты" без дополнительных данных нельзя, так как. Непонятно, как выяснить долю повторяющихся писем.

Тесты автора данной статьи, проведенные по подборке получаемого в России спама, показывают уровень обнаружения спама в 25% (в обычных терминах) при нуле ложных срабатываний (без учета получаемых легитимных рассылок с большим числом подписчиков).

Сравнительный анализ методов

Три рассмотренных метода кардинально отличаются по способу сбора спама, остальные характеристики у них близки - по полученным образцам спама генерируются сигнатуры, почтовая система может сравнить сигнатуру полученного письма с известными системе, а в случае совпадения - решить, является ли полученное письмо нежелательным.

Однако различия в способах сбора приводят к существенному отличию в поведении распределенных систем в целом.

Качество работы:

Качество работы (процент определяемого спама) распределенных систем зависит от ряда свойств системы:

- От представительности выборки - количества разнообразного собираемого спама.
- От соответствия выборки, имеющейся в системе, потоку спама конкретного пользователя.
- От методов построения контрольных сумм - насколько качественно они работают с персонализированным (со случайными последовательностями) спамом.

Судя по публикуемым данным, наиболее представительной выборкой в настоящее время обладают системы с ловушками почты, в первую очередь Brightmail, обрабатывающая около 2 млрд. сообщений в сутки. У основанных на других принципах сбора спама систем DCC и Razor потоки сообщений имеют примерно один порядок - около 100 млн. сообщений в сутки (с учетом разницы методов подсчета), однако в случае DCC в систему попадает информация обо всем потоке почты, а в случае Razor - только по выбору пользователя, соответственно представительность DCC несколько выше. Принципы построения нечетких контрольных сумм в DCC и Razor похожи, качество их должно быть близким. Соответственно, качество работы у DCC должно быть выше за счет большей представительности - что и наблюдается в тестах.

Ложные срабатывания:

Ложные срабатывания - это ошибочное принятие за спам-сообщения того, что спамом не является. Не имея детальных данных по системам с ловушками спам-почты, рассматривать этот аспект их

работы невозможно. Рассмотрим проблему ложных срабатываний для двух оставшихся классов систем:

1. Системы с голосованием пользователей зависят в определении спама от выбора пользователей. По опыту автора, пользователи часто считают спамом вполне "легальные" сообщения - рассылки, на которые они подписались и не знают, как отписаться, сообщения от автоматических почтовых "роботов" и так далее. Уровень "шума" на потоке жалоб обычно составляет не более нескольких процентов. С другой стороны, обычно число жалоб на легальные сообщения меньше жалоб на массовый спам. С учетом вышесказанного, системы с голосованием должны либо повышать "порог срабатывания" (число жалоб, при котором письмо считается спамом), либо мириться с ложными срабатываниями, когда за спам принимаются легитимные рассылки. Судя по появлению механизма "голосования за" в Razor v2, данное свойство является определенной проблемой - полностью от ложных срабатываний избавиться не удается.

2. Системы с анализом всей почты принципиально подразумевают возможность ложного срабатывания - для этих систем легальные рассылки и спам выглядят одинаково. Другими словами, почтовые системы, использующие DCC или аналоги должны поддерживать белые списки для всех легальных рассылок, которые хочется получать. В существенной степени, проблема ложных срабатываний переложена на конечного пользователя.

Возможность компрометации распределенных систем

В последнее время происходят массовые DoS-атаки на системы RBL, что говорит о накоплении спамерами достаточных ресурсов для попыток устранения не нравящихся им антиспамерских систем. С учетом этого факта, необходимо рассмотреть возможность компрометации распределенных систем сбора статистики.

Компрометация подобных систем возможна в двух вариантах: либо система резко снижает качество работы (долю распознаваемого спама), либо же резко увеличивается число ложных срабатываний. В дальнейшем будем рассматривать возможность компрометации только с использованием заложенных в сами системы механизмов работы.

- Системы с ловушками для почты - качество их работы зависит от почты, поступающей в ловушки. Снизить качество работы можно в ситуации, когда спам в эти ловушки перестал приходить. С учетом количества ловушек в коммерческих системах это маловероятно. Количество ложных срабатываний можно увеличить, "завалив" ловушки легитимной почтой. В обоих случаях, для компрометации системы необходимо, чтобы в руки спамеров попала существенная часть списка ловушек, компрометация без этого списка малореальна.

- Системы с голосованием пользователей. Качество работы таких систем зависит от активности пользователей - число жалоб на письмо пропорционально массовости его рассылки и количеству пользователей системы. Таким образом, снизить качество распознавания можно путем уменьшения количества спама приходящего голосующим участникам, но именно этого они и так добиваются. Другими словами, ухудшение качества распознавания за счет внешнего воздействия представляется нереальным. Компрометация системы путем увеличения числа ложных срабатываний представляется возможной - для этого спамерам нужно стать голосующим участником и голосовать "против" легитимных рассылок. Потенциально это возможно, данную проблему система Razor/SpamNet нейтрализует путем присваивания рейтинга голосующим участникам - для компрометации системы необходимо большое количество голосующих участников с хорошим рейтингом. Это опять возможно, но требует уже больших организационных ресурсов. В то же время, проблема ненамеренной компрометации базы данных Razor легальными рассылками есть и на сегодняшний день.

- Системы анализа всей проходящей почты. Данные системы строят объективную статистику проходящей почты, классифицируя ее по частоте, а не по содержанию. Занизить частотность какой-либо рассылки без нарушения целостности системы представляется невозможным. Компрометация системы за счет ложных срабатываний теоретически возможна т.к. нет способа проверить реальное число получателей сообщения, о котором рапортует почтовый сервер.

В системе DCC заложена потенциальная возможность принимать отчеты только от авторизованных клиентов, однако в настоящее время эта возможность на публичной сети DCC-серверов не используется.

Необходимо отметить, что компрометация путем увеличения числа ложных срабатываний существенна только для легальных массовых рассылок, компрометировать единичные сообщения затруднительно, ибо для компрометации необходимо получить образец компрометируемого письма до того, как оно получено большинством получателей. Для обычных писем это малореально.

В то же время, для легко компрометируемой на сегодня системы DCC проблема пропуска массовых легальных рассылок имеется и без компрометации, их в любом случае нужно вносить в белый список.

Проблемы распределенных методов

Наиболее существенной проблемой для вышеописанных методов детектирования массовых рассылок является "персонализация" спама - каждое современное спамерское письмо существует в огромном количестве вариантов с незначительными отличиями в тексте. Насколько известно автору, на сегодняшний день ни одна из распределенных систем полностью данную проблему не решила.

В то же время, пути решения достаточно понятны - существует богатый разработанный математический аппарат, предназначенный для поиска похожих текстов и фрагментов текстов (сигнатуры Рабина и т.п.), который постепенно начинает использоваться в распределенных системах обнаружения спама.

Вторая существующая проблема связана с ложными определениями легальных рассылок как спама. Эта проблема характерна как для методов, анализирующих всю почту, так и, в меньшей степени, для систем с голосованием пользователей. Решение этой проблемы на локальном уровне возможно путем создания белых списков, включающих все принимаемые данной почтовой системой рассылки. На глобальном уровне можно создавать как всеобщие белые списки (с какой-то политикой), либо вводить методы, позволяющие уверенно и надежно идентифицировать источник рассылки.

Таким методом может быть, например, необязательная электронная подпись содержания легальных рассылок, позволяющая уверенно идентифицировать отправителя. Подписанные сообщения могли бы с гарантией проходить через почтовые фильтры.

Перспективы и пути развития распределенных систем анализа электронной почты

Дальнейшее усовершенствование распределенных систем анализа электронной почты можно разделить на два основных направления: улучшение уже построенных механизмов и создание принципиально новых методов анализа.

А. Усовершенствование имеющихся механизмов распределенных систем, очевидно, будет включать борьбу с описанными выше проблемами. Будет увеличиваться защищенность систем от компрометации, качество обработки писем с добавками случайного текста, снижаться уровень ложных срабатываний. Очевидно, что будет увеличиваться и охват распределенных систем - их эффективность в борьбе со спамом автоматически будет приводить к появлению новых клиентов.

Б. Новые возможности распределенных систем анализа. Обладание большим массивом получаемых в реальном времени данных о распространении отдельного сообщения открывает совершенно новые возможности для надежного обнаружения спама. По всей видимости, большой эффект должно дать объединение имеющихся способов фильтрации спама (RBL, детерминированный контентный анализ, статистический анализ) с данными, поставляемыми распределенными системами.

Можно привести такие потенциальные примеры:

- Автоматическое построение короткоживущих черных списков IP-адресов в реальном времени. Если какое-либо сообщение, расклассифицированное как спам, рассылается в настоящее время с некоего списка IP-адресов, то весь этот список может быть временно помечен как "черный" и какой-либо прием почты с этих машин - запрещен. Такое блокирование может осуществляться быстро, его можно делать только на время рассылки.

- Ретроспективный анализ источников спама и построение черных списков на его основе. Способ предполагает анализ источников спама, рассылающих сообщения, которые не были классифицированы как спам сразу (например, по причине наличия в них больших

объемов случайного текста). Если данные рассылают только спам, то они могут быть помещены в сравнительно долгоживущие черные списки.

- Анализ активности отдельных машин при рассылке почты, выявление "схем поведения" пользовательской машины, рассылающей спам. По всей видимости, такая машина должна отличаться по поведению, как от обычного почтового сервиса, так и от пользовательского компьютера.

- Накопление и анализ изменений текста внутри одной массовой рассылки (один основной текст с переменными добавками). Можно как выделять общие части таких сообщений статистическими методами, так и исследовать алгоритм случайных изменений с целью предсказания дальнейших вариаций.

Богатые потенциальные возможности распределенных систем анализа почты имеют в себе и скрытые опасности - контроль над такой системой дает множество потенциальных возможностей контроля почты, не связанных с фильтрацией спама. Для предотвращения слишком большого интереса к подобным системам, они должны накапливать сведения только о массовых рассылках, а не по электронной почте в целом. Технологии распространения спама растут пропорционально новым методам борьбы со спамом. К сожалению, такова жизнь, но это неплохо, значит прогресс на месте не стоит.

Спам и методы его обнаружения. Фишинг

Сергеева А.М., Файзуллин Р.В.

Башкирский Государственный Аграрный Университет
г. Уфа, Россия
Predator07@mail.ru

Spam: detecting spam with and without content analysis. Phishing

Sergeeva A.M., Fayzullin R.V.

Bashkir State Agrarian University
Ufa, Russia
Predator07@mail.ru

В последнее время стали учащаться случаи жалоб пользователей Сети Интернет на то, что в их адрес приходит все больше и больше непрошеной корреспонденции рекламного характера. Такие письма называются в Сети спамом.

Актуальностью данной темы является усовершенствование методов обнаружения спама с целью улучшения работы пользователей с электронной почтой и методов борьбы с фишингом.

Целью и главной задачей работы является изучение спама и методов его обнаружения, а также одного из способов мошенничества при помощи спама – фишинга и методов борьбы с ним.

Спам – анонимная не запрошенная массовая рассылка электронной почты. Это определение довольно хорошо соотносится с мировой практикой и определениями спама, положенными в основу американского и европейского законодательства о спаме. Кроме того, это определение можно эффективно использовать на практике. Большинство спам- рассылок носят рекламный или другой коммерческий характер, это важно при рассмотрении экономики спама.

У спамера есть очень много методов узнать Ваш адрес электронной почты, чтобы потом производить по нему рассылки. Есть масса программ, которые собирают адреса людей, пишущих письма в телеконференции и группы новостей. Такая программа способна собрать за час тысячи адресов и создать из них базу данных для дальнейшей рассылки по таким адресам спама. Некоторые из спамеров в своих рассылках предлагают приобрести за несколько долларов компакт диск с такой информацией. Еще один метод состоит в том, что спамеры просматривают различные периодические издания, откуда извлекают адреса электронной почты фирм, подавших объявление.

Спамерские рассылки можно избежать следующим образом:

1) Постарайтесь не оставлять своего адреса электронной почты на различного рода серверах сомнительного содержания.

2) Никогда не отвечайте на письма спамеров - тем самым вы даете им знать, что Ваш адрес реально существует и поступающая туда почта читается владельцем. Если в их письме сказано, что Вы можете исключить себя из листа, послав по определенному адресу команду "remove" - в большинстве случаев это ложь. Последовав такому совету, Вы только подтвердите возможность использования Вашего адреса для дальнейших рассылок.

3) Не стоит посылать в адрес спамера кучи мусора. Возможно, Вы неверно определили, откуда в действительности пришел спам, и пострадают люди, не имеющие к спамеру никакого отношения.

Особенности современных массовых рассылок приводят к тому, что в рамках отдельной почтовой системы видна только часть общей картины – спам приходит со сравнительно небольшого количества IP-адресов, имеет относительно небольшое число модификаций, единичная рассылка продолжается небольшое время. Более полную картину происходящего имеют крупные почтовые системы и ISP с миллионами пользователей, однако полной картиной не обладают и они.

В то же время, единичная рассылка на миллионы адресов занимает существенное время – от нескольких часов до нескольких суток. Если обнаружить ее «на старте» и каким-либо образом блокировать, то ущерб от спама понесут только те пользователи, чьи адреса были использованы в начале рассылки. Другими словами, необходимо собирать данные о спам-почте из максимально-возможного количества точек сети, обрабатывать их максимально быстро и делать доступными данные о происходящей в настоящее время рассылке для всех участников системы.

В настоящее время реализованы такие *методы быстрого сбора данных о рассылках:*

- прием спама в специальные «ловушки» (honeypot) - E-mail адреса, предназначенные только для приема спама;
- голосование пользователей – пользователь, получивший спам, нотифицирует об этом систему сбора данных, предоставляя образец спама;
- анализ всей проходящей через почтовую систему почты с сообщением контрольных сумм отдельных сообщений на центральный сервер.

Три рассмотренных метода кардинально отличаются по способу сбора спама, остальные характеристики у них близки – по полученным образцам спама генерируются сигнатуры, почтовая система может сравнить сигнатуру полученного письма с известными системе, а в случае совпадения – решить, является ли полученное письмо нежелательным. Однако различия в способах сбора приводят к существенному отличию в поведении распределенных систем в целом.

Из выше рассмотренных методов можно выделить две основные проблемы: 1. Наиболее существенной проблемой для данных методов детектирования массовых рассылок является «персонализация» спама – каждое письмо существует в огромном количестве вариантов с незначительными отличиями в тексте. 2. Определение легальных рассылок как спама. Эта проблема характерна как для методов, анализирующих всю почту, так и, в меньшей степени, для систем с голосованием пользователей.

Для усовершенствования распределенных систем анализа электронной почты можно выделить два основных направления: улучшение уже построенных механизмов и создание принципиально новых методов анализа.

Первым является, усовершенствование имеющихся механизмов распределенных систем. Будет увеличиваться защищенность систем от компрометации, качество обработки писем с добавками случайного текста, снижаться уровень ложных срабатываний. Очевидно, что будет увеличиваться и охват распределенных систем – их эффективность в борьбе со спамом автоматически будет приводить к появлению новых клиентов.

Вторым является, новые возможности распределенных систем анализа. Обладание большим массивом получаемых в реальном времени данных о распространении отдельного сообщения открывает совершенно новые возможности для надежного обнаружения спама. По всей видимости, большой эффект должно дать объединение имеющихся способов фильтрации спама (RBL, детерминированный контентный анализ, статистический анализ) с данными, поставляемыми распределенными системами.

Один из способов мошенничества с помощью спама — «Фишинг» (англ. *phishing* от *fishing* — рыбалка). Он представляет собой попытку спамеров выманить у получателя письма номера его кредитных карточек или пароли доступа к системам онлайновские платежей. Такое письмо обычно маскируется под официальное сообщение от администрации банка. В нём говорится, что получатель должен подтвердить сведения о себе, иначе его счёт будет заблокирован, и приводится адрес сайта (принадлежащего спамерам) с формой, которую надо заполнить. Среди данных, которые требуется сообщить, присутствуют и те, которые нужны мошенникам. Для того, чтобы жертва не догадалась об обмане, оформление этого сайта также имитирует оформление официального сайта банка.

Существуют различные методы для борьбы с фишингом, включая законодательные меры и специальные технологии, созданные для защиты от фишинга.

Также в данной работе были рассмотрен спам и методы борьбы с ним, а также основные проблемы предложенных методов; описан фишинг и методы борьбы с ним.

Распознавание фишинговых веб-страниц без использования "черных" списков

Чувило Олег Александрович

Харьковский национальный университет радиоэлектроники
г. Харьков, Украина
oleg.chuvilo@dnt-lab.com

Detection of phishing web pages without using blacklist's

Chuvilo O.A.

Kharkov National University of Radio electronics
Kharkov, Ukraine
oleg.chuvilo@dnt-lab.com

The method developed in this paper will allow to detect phishing web pages without using of "black" lists

Every year, the popularity of services like Internet banking, as well as storing the information at remote servers (Google Docs, etc.), grows. It results in growth of fishing sites and webs-pages targeted at theft of information required for access to bank accounts, e-mail and other confidential information.

At present, for protection against fishing, the method of "black" lists is basically used. At that, the user is unprotected until the moment of entering of the fishing sites into the lists.

The purpose of this work consists in development of a method allowing distinguishing of fishing web-pages without the use of "black" lists.

For the purpose of timely detection of fishing web-pages it is proposed to use comparison of contents of web-pages. Usually user continuously works with rather small amount of Internet resources, to which the confidential information is transmitted. It allows to adjust the URL list and the contents corresponding to them. Further, by comparing the content of pages with which the user works, and the content of pages in the base, similar ones can be determined. Having compared their URL, it would be possible to draw a conclusion as regards attributing the resource to legal ones, or on the contrary.

Advantage of the method consists in possibility to determine fishing pages prior to their inclusion into the lists of fishing sites.

However, the necessity of active participation of the user in setting-up the system has been an essential drawback.

Use of the given method in anti-fishing system would allow to determine timely the threats, and warn the user of the risk.

С каждым годом растет популярность таких сервисов как интернет банкинг, а также хранение информации на удаленных серверах (Google Docs и т.д.). Это приводит к росту фишинговых сайтов и веб-страниц направленных на похищение информации необходимой для доступа к банковским счетам, электронной почте и другой конфиденциальной информации.

В данный момент для защиты от фишинга в основном используется метод «черных» списков. При этом пользователь является незащищенным до момента внесения фишинговых сайтов в списки.

Цель данной работы заключается в разработке метода позволяющего распознавать фишинговые веб-страницы без использования «черных» списков.

Для своевременного определения фишинговых веб-страниц предлагается использовать сравнение содержимого веб-страниц. Обычно пользователь постоянно работает с относительно небольшим количеством интернет ресурсов на которые передается конфиденциальная информация. Это позволяет настроить список URL и соответствующее им содержимое. Далее сравнивая содержимое страниц с которыми работает пользователь и содержимое страниц в базе можно определить похожие. Сравнив их URL можно сделать вывод о принадлежности ресурса к легальным или наоборот.

Преимуществом метода является возможность определить фишинговые страницы до внесения их в списки фишинговых сайтов.

При этом необходимость активного участия пользователя при настройке системы является существенным недостатком.

Использовании данного метода в антифишинговой системе позволит своевременно определять угрозы и предупреждать пользователя об опасности.

7 Секция

Средства анализа и тестирования

Analyzing and testing modern means of protection

Система автоматического обнаружения ошибок в коде параллельных программ на языке Си++, использующих OpenMP (VivaMP)

Колосов А.П., Рыжков Е.А.

Тульский государственный университет
г. Тула, Россия

zeratul@home.tula.net

System for the autodetection of errors in code of parallel programs in the C++ language using OpenMP (VivaMP)

Kolosov A.P., Ryzhkov E.A.

Tula state university
Tula, Russia

zeratul@home.tula.net

По оценкам компании Evans Data, проводящей опросы среди разработчиков ПО, общее количество программистов в мире к 2009 году составит 17 миллионов человек, причем 630.000 из них считают, что главной проблемой в разработке параллельных приложений является нехватка программных средств для их создания, тестирования и отладки.

Программный продукт VivaMP, разработанный на основе созданного ранее статического анализатора Viva64, предназначен для автоматического обнаружения ошибок в коде программ, написанных на языке Си++, использующих для распараллеливания расширение языка OpenMP. Это расширение было выбрано из-за того, что оно, по оценкам некоторых экспертов, может стать одним из наиболее популярных.

Особенности VivaMP:

1. VivaMP ориентируется исключительно на поиск ошибок, возникающих при распараллеливании кода.

2. Как и Viva64, VivaMP обеспечивает полноценную интеграцию со средой разработки Microsoft Visual Studio, позволяя осуществлять навигацию по файлам, проектам и решениям, выполнять переход к месту с ошибками, использовать интегрированную справочную систему[3].

3. Ориентация VivaMP на один класс ошибок позволяет сделать настройку VivaMP максимально простой. Практически, программа готова к работе сразу же после установки, что выгодно отличает ее от программ-конкурентов.

Литература

1. Timothy Prickett Morgan Evans Data Cases Programming Language Popularity: [http://www.itjungle.com/tug/tug121406-story03.html], 14.12.2006.
2. Michael Suess Why OpenMP is the way to go for parallel programming: [http://www.thinkingparallel.com/2006/08/12/why-openmp-is-the-way-to-go-for-parallel-programming/], 12.08.2006.

Сайт проектов VivaMP и Viva64. http://www.Viva64.com

Компьютерный вирус как инструмент анализа и модернизации современных средств защиты

Приходько М.А.

Институт Государственного Управления, Права и Инновационных Технологий
г. Москва, Россия

spex19@mail.ru

The computer virus as an instrument for analysing and modifying modern security systems

Prihodko M.A.

Institute of Public Administration, Law and Innovation Technologies
Moscow, Russia

spex19@mail.ru

Annotation: This work describes how to use “safe viruses” to analyze modern security systems and to build the next generation of security systems similar to human’s immune system. Key properties of such “safe viruses” are formulated, and main problems of their usage are discussed.

In medicine, where non-infliction of harm is one of the main principles, yet for a long time, dangerous, and sometimes, simply fatal viruses are used for the good of a human being. For example, while producing "alive vaccines", which inherently represent **alive virus,** weakened in a special way, in order that being introduced into an organism of a human being, it could make for developing antibodies. In a similar manner, computer viruses can not only be used for **deliberate** analysis of the means of protection, but could also become **prototype** of the means of protection of new generation.

The global information system (totality of all hardware and software tools) can be considered as *information organism*. From this point of view it would be reasonable not to protect each individual *information cell* (indivisible hardware-software complex – a computer), but the entire organism as a whole. For that purpose, it would be necessary to develop a global *information immune system,* which basic component would be formed by *computer antibodies* – virus-like programmes directed towards destruction of threats of a particular nature.

By analogy with the organism of a person (and the immune system), the number of computer antibodies should be **monitored.** Computer antibodies should not be distributed (propagate) uncontrollably, and it would be necessary to support a particular population, which size could be increased in case of detection of the centre of infection with a computer virus.

In case of detection of the centre of infection, computer antibodies should have an opportunity, to inform of that, the other computer antibodies possessed of the necessary properties for destruction of the revealed virus. And the latter should have an opportunity of a fast reproduction and moving to the centre of infection.

Let's formulate minimal requirements towards computer antibodies:

- possibility to communicate with each other;
- possibility to propagate;
- possibility of not only chaotic, but also purposeful moving;
- possibility of self-destruction;
- possibility to maintain the size of population.

It is obvious, that wide use of computer antibodies would only be possible after solution of a whole range of tasks:

- realization of the mechanism of identification of computer antibody (including by anti-virus programmes), protected against possibility of use of this mechanism by harmful viruses;
- realization of the mechanism of communications between antibodies;

- realization of the mechanism of self-regulation of the number of population of computer antibodies of a particular kind;
- realization of the mechanism of purposeful reproduction and self-destruction;
- realization of the mechanism of purposeful motion of computer antibody to the centre of infection;
- solution of legal problems.

The second variant of use of "good viruses" is a purposeful check-up of the quality of the means of protection, or analysis of the ways of distribution of computer viruses.

In the first case, computer virus plays a role of "the scanner of vulnerabilities". And its tasks include communication of the information about the found vulnerability to the checking structure.

In the second case, a safe virus is distributed by all possible ways, for analysis of the ways of motion of computer threats, and mapping the routes of their fastest distribution.

Each copy of "good virus" should be provided with individual **unique** identifier which will be transferred from a parent generating new copy of virus, to a "child" (in addition to its own identifier). This would not simply allow to find out "where" the viruses are distributed, but also "how", including – to reveal the centres generating the largest waves of infection, since the presence of hierarchical relations between copies of the virus would allow to count up the number of generated copies of virus, and also construct the routes of distribution, from the very first, to the last copy.

The second necessary property – possibility to accumulate information about the "parent" that generated the given copy of virus, and also all its parents, till the first opportunity is found, to transfer this information by means of electronic communication into the analytical centre.

The most serious problem of the use of "litmus viruses" includes legal aspects of such an activity. Not only the very possibility to use a non-malignant virus, which is distributed "secretly" among the users, but also the volume and nature of the information which is allowed to be collected by such virus. Whether a legal base for the use of similar mechanisms would be created – the future of modern protection means depends on that.

Nevertheless, an example of modern medicine instils hopes that in this or that form the experience, which has been accumulated by computer trespassers, eventually, will be used not only for causing harm, but also for protection against such actions. And one day, personal computer would not only be protected by personal antivirus, but also the entire information immune system.

В медицине, где ненанесение вреда – один из основных принципов, уже давно используются опасные, а иногда и просто смертельные вирусы во благо человека. Например, при изготовлении «живых вакцин», которые по своей сути представляют **живой вирус**, ослабленный специальным образом, чтобы, будучи введенным в организм человека, дать последнему возможность выработать антитела. Так и компьютерные вирусы могут использоваться не только для **сознательного** анализа средств защиты, но и стать **прототипом** средств защиты нового поколения.

Глобальную информационную систему (совокупность всех аппаратных и программных средств) можно рассматривать как *информационный организм*. С этой точки зрения разумно защищать не каждую отдельную *информационную клетку* (неделимый программно-аппаратный комплекс – компьютер), а весь организм в целом. Для этого необходимо разработать глобальную *информационную иммунную систему*, основной составляющей которой станут *компьютерные антитела* – вирусоподобные программы, направленные на уничтожение угроз определенного характера.

По аналогии с организмом человека (и его иммунной системой) **ч**исло компьютерных антител должно **контролироваться.** Компьютерные антитела не должны распространяться (размножаться) бесконтрольно, а необходимо поддерживать определенную популяцию, размер которой может быть увеличен при обнаружении очага заражения компьютерным вирусом.

При обнаружении очага заражения компьютерные антитела должны иметь возможность сообщить о нем другим компьютерным антителам, обладающим необходимыми свойствами для уничтожения найденного вируса. А последние должны иметь возможность быстрой репродукции и перемещения к очагу заражения.

Сформулируем минимальные требования к компьютерным антителам:

- возможность обмениваться сообщениями друг с другом;
- возможность размножаться;
- возможность не только хаотичного, но и целенаправленного перемещения;
- возможность самоуничтожения;
- возможность поддержания размера популяции.

Очевидно, что широкое использование компьютерных антител возможно только после решения целого ряда задач:

- реализация механизма идентификации компьютерного антитела (в том числе антивирусными программами), защищенного от возможности использования этого механизма вредоносными вирусами;
- реализация механизма коммуникации между антителами;
- реализация механизма саморегуляции численности популяции компьютерных антител определенного вида;
- реализация механизма целенаправленной репродукции и самоуничтожения;
- реализация механизма целенаправленного перемещения компьютерного антитела к очагу заражения;
- решение правовых проблем.

Второй вариант использования «хороших вирусов» – целенаправленная проверка качества средств защиты или анализ путей распространения компьютерных вирусов.

В первом случае компьютерный вирус исполняет роль «сканера на уязвимости». А в его задачи входит передача информации о найденной уязвимости проверяющей структуре.

Во втором случае безопасный вирус распространяется всеми возможными способами для анализа путей перемещения компьютерных угроз и построения карты маршрутов их наиболее быстрого распространения.

Каждый экземпляр «хорошего вируса» должен снабжаться индивидуальным **уникальным** идентификатором, который от родителя, порождающего новую копию вируса, будет передаваться «ребенку» (помимо его собственного идентификатора). Это позволит не просто узнать «куда» распространяются вирусы, но и «как», в том числе – выявить очаги, порождающие самые крупные волны заражения, т.к. наличие иерархической связи между экземплярами вируса позволит подсчитать число порожденных копий вируса, а также построить маршруты распространения от самой первой до самой последней копии.

Второе необходимое свойство – возможность накапливать информацию о «родителе», породившем данный экземпляр вируса, а также всех его родителях, пока не будет найдена первая возможность передать эту информацию средствами электронной связи в аналитический центр.

Самая серьезная проблема использования «лакмусовых вирусов» – правовые аспекты такой деятельности. Не только сама возможность использования доброкачественного вируса, который распространяется «скрытно» от пользователей, но и объем и характер информации, который разрешен для сбора таким вирусом. Будет ли создана юридическая база для использования подобных механизмов – от этого зависит будущее современных средств защиты.

Тем не менее, пример современной медицины вселяет надежду на то, что в той или иной форме опыт, накопленный компьютерными злоумышленниками, в конце концов, будет использован не только для нанесения вреда, но и для защиты от подобных действий. И однажды защищать персональный компьютер будет не только личный антивирус, но и целая информационная иммунная система.

8 Секция

Экономические модели и аналитические аспекты информационной безопасности

Economic models and analytical aspects of IT security

Расчет финансовых потерь предприятий от деятельности вредоносных программ

Бочарникова М.В.
Соавторы: Сапрыкин А.С., Киктенко В.А., Адамов А.С.

Национальный Технический Университет "Харьковский Политехнический Институт"
г. Харьков, Украина
bocharnikova-m@mail.ru

Calculation of an enterprise's financial losses caused by malware activities

Bocharnikova M.V.
co-authors: Saprykin A.S., Kiktenko V.A., Adamov A.S.

National Technical University "Kharkov Polytechnical Institute"
Kharkov, Ukraine
bocharnikova-m@mail.ru

В современном мире стремительное развитие информационных технологий приводит к более эффективной работе всех структур и подразделений предприятий, но в тоже время с каждым днем увеличивается вероятность проникновения вредоносных программ в компьютерную систему, что может повлечь за собой не только кратковременные сбои в сети, но и полную остановку деятельности предприятия. Убытки, наносимые вредоносными программами по всему миру, исчисляются миллиардами долларов и продолжают ежегодно расти. Деструктивное действие вирусных технологий ощущают как крупные компании, так и компании, среднего бизнеса, где информационной безопасности уделяется достаточно мало внимания, а число компьютеров постоянно увеличивается.

С экономической точки зрения деятельность любого предприятия можно представить в виде набора показателей, профессионально оценивая которые можно с определенной долей вероятности судить о настоящем положении дел на этом предприятии и делать необходимые прогнозы на будущее. Набор этих показателей (показатели ликвидности, рентабельности, устойчивости, показатели

производительности труда, роста объема производства, количества затрат и др.) в совокупности дает возможность сделать очень качественную комплексную оценку и характеристику финансового состояния. Объединяя эти показатели в одну многофакторную модель (с помощью статистических данных за как можно больший промежуток времени) можно выявить закономерности и зависимости, анализируя которые в будущем можно судить об изменениях в работе предприятия. Эти изменения могут происходить как в сторону улучшения конечного финансового результата, так и соответственно его ухудшения и являться следствием воздействия различных внутренних и внешних факторов, наша задача состоит в том, чтобы определить воздействие именно вредоносного программ и оценить ущерб от их деструктивной активности. Эти изменения носят разносторонний характер, что связано со спецификой отраслей экономики, с текущими особенностями действующих предприятий, с состоянием экономической среды, в которой они работают.

Главным фактором, который непосредственно оказывает прямое влияние на размер ущерба от вредоносных программ, является простой компьютерной сети. За период времени, в течение которого предприятие не имеет возможности осуществлять свою деятельность в полном объеме, оно терпит убытки, что в последствии выражается в ухудшении всех финансово-экономических показателей ее деятельности. Немаловажными факторами являются также потеря ценной информации и ухудшение имиджа фирмы, что выражается в невозможности противостоять вирусным атакам.

Выделим следующие составляющие показателей деятельности и элементы возникающих затрат, которые напрямую позволяют оценить величину ущерба от простоя, а именно: затраты времени специалистов на устранение вредоносной программы; стоимость утраченных данных; расходы на аппаратно-технические средства и программное обеспечение; простой системы; потери рабочего времени сотрудников из-за простоя системы; снижение производительности труда; ущерб, нанесенный деловой репутации пострадавшей фирмы.

Также нетрудно посчитать изменения производительности труда (количество произведенной продукции по отношению к средней численности сотрудников), связанные с недозагрузкой рабочего персонала.

На рисунке 1 представлены показатели, которые были использованы при разработке системы подсчета экономического ущерба предприятия от действия вредоносных программ.

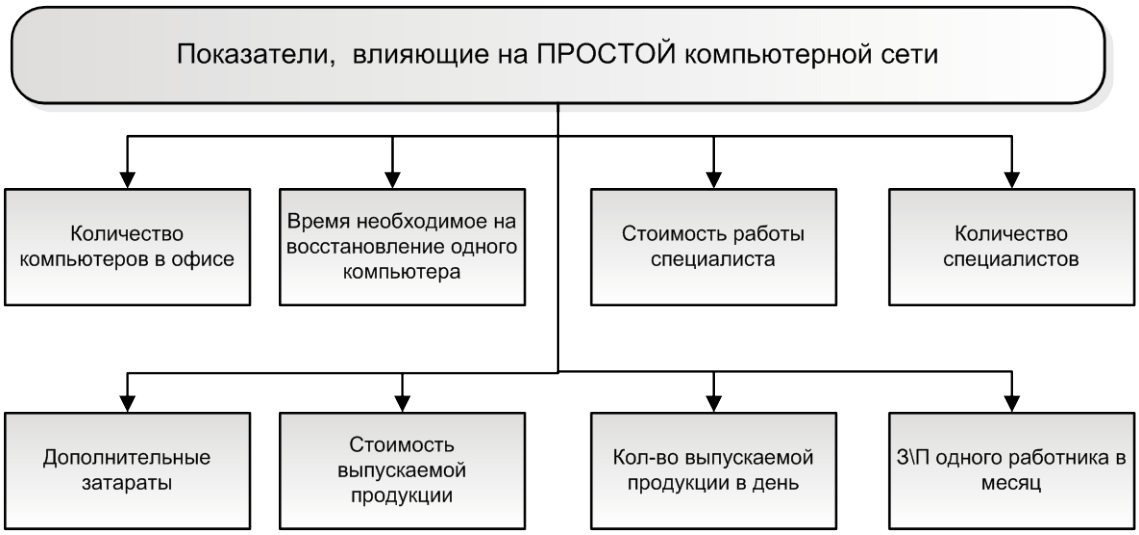


Рисунок 1 – Показатели, влияющие на простой компьютерной сети

Работа программы представлена на рисунке 2 и рисунке 3.

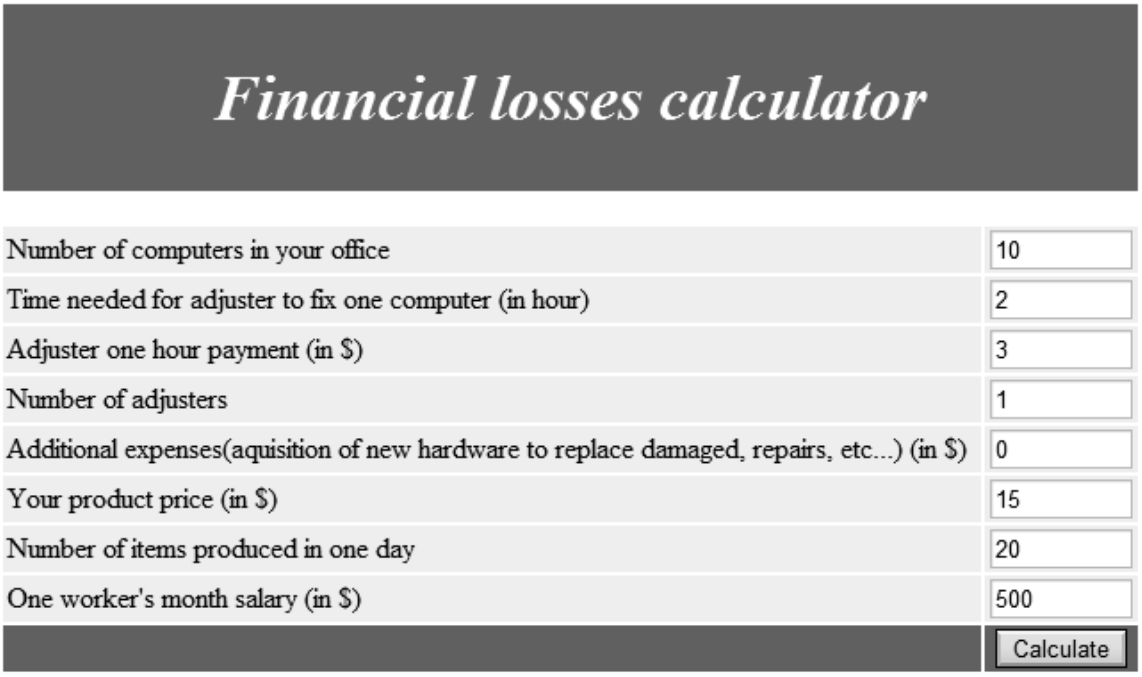


Рисунок 2 – Главное окно программы

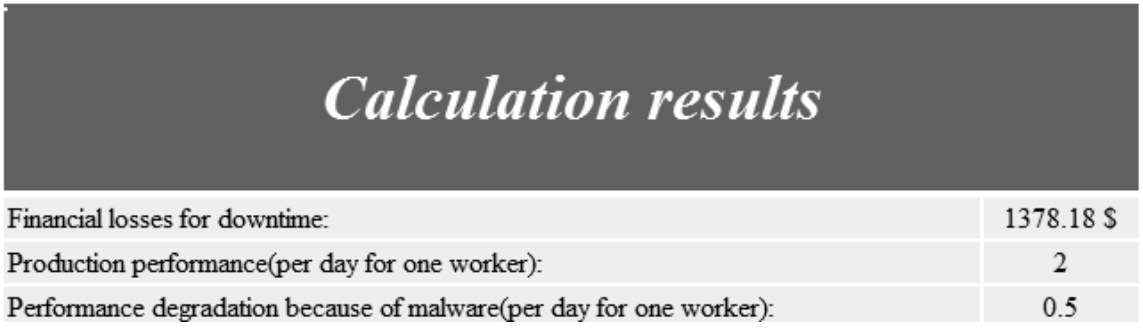


Рисунок 3 – Результат работы программы

В программе также предусмотрено сохранение результатов расчетов в базу данных для дальнейшего анализа.

Исходный код программы представлен в приложении 1.

С помощью разработанной системы можно подсчитать финансовый ущерб предприятия от простоя компьютерной сети и дать качественную оценку производительности труда.

Некоторые подходы к обоснованию затрат на обеспечение системы информационной безопасности хозяйствующего субъекта

Курнавина Т.С.

Московский энергетический институт (Технический университет)
Москва, Россия

Some approaches to a substantiation of expenses for system of information safety

Kurnavina T.S.

Moscow Power Engineering Institute (Technical University)
Moscow, Russia

Introduction

The system of information safety today becomes an indispensable condition of successful operation in any area of activity of a managing subject. At that, if the question of expediency of creation of the information safety system (ISS) for a managing subject (MS) is not disputable, then the question of reasonable volumes of financing of the expenses on protection of information is still open for the decision-making persons (DMPs). One cannot say that there is no attention towards this problem. In specialised editions, publications on the subject appear periodically, but today, there are no scientifically sound and verified mechanisms for substantiation of expenses on the creation of ISS, taking into consideration the factors significant for DMPs. On the other hand, the normative documents used today by the experts in protection of information, on the management of information risks, organisation of the systems of information safety, and other documents [1-4], consider this problem predominantly from the point of view of a specialist in organisation of ISS and management of information risks, which is far from being always convincing to the DMPs, making decisions as regards financing of ISS.

This work considers several new approaches to substantiation of expenses on organisation of ISS MS with the account of the various factors, values of risks and limitations allowing in full measure to realise the principle of "reasonable adequacy" while organisation of ISS MS.

Two opinions regarding the problem

Generally speaking, the number of opinions and views as regards the structure and organization of ISS MS is much more than two. In addition to that of the DMPs, there are opinions, as regards its rational organization, of bookkeepers, economists, lawyers, managers and other employees participating in the processes of reception, processing, storage and communication of information, organizing office work, or serving computer facilities, means of communications and liaison. We shall consider opinions and positions of only two basic participants in the process of substantiation of expenses: DMP on definition of the budget on the system on ISS and Expert in information safety. The analysis has shown that they have absolutely different opinions as regards this process (table 1).

Table No. 1

Opinions of different experts as regards the mechanisms of substantiation of expenses on information safety system of the organization

№ №	DMP	Expert in protection of information
	Mechanism of substantiation of the expenses	
1	Protection of information – is the necessary function of conducting modern business, therefore, for decision-making regarding protection of information, DMP not only needs knowledge of probability of risk and possibility of damage, but also other information usually used for performance evaluation of business: • expenses on realization of protective measures for each risk (Zi). It is desirable that these expenses be distributed in time within the planned period; • liquidity ratios of actives (Ki), related to the sphere of provision of information safety for each risk; • description of characteristics of occurrence of risk (a single event, realisation of threat in full, or series of incidents in which the threat is realised gradually, etc.); • dynamics of obsolescence of the actives related to risk for formation of the system of their depreciation charges; • combinations of these parameters, for example, the ratio of expenses for decrease of risk and probable damage at its realization, etc.	Protection of information is the function of Service of information safety in provision of business. Financing of expenses on information safety is made on the basis of results of evaluation and analysis of risks by existing risk management mechanisms [2]. Economic methods of evaluation of the efficiency are thus not used. In the basis of evaluation of risk, there is multiplicative criterion, which is set by qualitative or quantitative evaluation of probability and damage in the form of multiplicative criterion: R= U*P, (1) where U – value of damage; P – probability of occurrence of risk.
2	**Ideal model of expenses on ISS**	
	$Z = \sum_i z_i \rightarrow \min$, (2) with $u_i >> z_i$, $p_i > p_0$, $Z < Z_0$ where , *I* – area of accepted, reduced or transmitted risks; u_i – damage through i-risk; p_i – probability of i-risk; p_o – probability, with which risks are accepted. It is determined most often from the point of view of the Expert in protection of information. Z_0 – maximum allowable expenses from the point of view of DMP. Other approach is also possible. For example, with the set level of budget Z_0 , to construct an ISS, with which, maximum reduction in damage from realisation of risks is possible: $U = \sum_i u_i \rightarrow \max$ (4)	$Z = \sum_i z_i$ (3) with $r_i \geq r_0$, $r_i = u_i p_i$ where, r_0 – boundary of risks determined most often from the point of view of the Expert in protection of information. r_i – current risk.

As one can see from the table, the points of view regarding organization of ISS MS differ to a considerable degree. At that, whereas the actions of the Expert in protection of information are regulated by domestic and foreign standards, there are no convincing mechanisms for DMP today for decision-making as regards financing of ISS. In addition, the approach to evaluation of the value of risk based on one parameter (1) can only be acceptable, when the damage is incurred constantly during the considered period of time Δt, and the distribution density function P(t) has the form of uniform law of distribution. While processing information

risks, all the expenses associated with reduction, transfer or elimination of risk are not taken into account. This does not allow to evaluate to the full, the efficiency of solutions of the information protection system of the managing subject. Thus, the existing approaches to evaluation and processing of risks are not convincing for DMP, and other mechanisms are required to perform evaluation of the offered solutions in the sphere of protection of information.

Analysis of existing approaches towards substantiation of expenses on the information safety system

The first attempts of creation of the mechanisms for performance evaluation of the solutions for protection of information, quite naturally, were based on application of financial-analytical and investment tools by analogy with performance evaluation of IT. However, whereas for IT such approach can be proved in many cases, since it gives analysts a possibility to estimate or measure economic effects from introduction of IT, in case of ISS it sets a complicated problem. The essence of it consists in that there is a substitution of concepts while evaluating economic effects. For investment projects as the basic parameter of economic efficiency, variation of profits of the MS is considered, before and after implementation of the project, and in case of performance evaluation of investments into ISS, the evaluation of prevented damage is considered, which has a probabilistic nature, and cannot be measured objectively and shown in the balance sheets of an enterprise. The effects gained from the protection are "dissolved" among other arrangements of organizational and technical nature; therefore, it is not always obviously possible to particularly evaluate them. Moreover, the actives associated with protection of information influence the product cost and reduce profit. These circumstances have resulted in that there was a necessity of creation of new approaches to substantiation of expenses, which would be clear to DMP, and would take into account probabilistic nature of information risks.

Technique of substantiation of expenses on the basis of two-factorial model of information risks

The simplest is the method of evaluation of risks on the basis of two-factorial model

$R=<P,U>$, with $Z \leq Z_0$ (5)

The essence of the mechanism of substantiation of expenses is presented in Fig. 1. All information risks are displayed in the system of coordinates (Probability, Damage). At that, some areas are allocated for the analysis:

The first area (the right top corner) represents risks, probability of which is high, and damage in case of their realisation is essential. This is the area of accepted risks, so the MS will bear certain expenses on their prevention, transfer or reduction. When processing each risk, the condition (5) is checked. In the event it is met, the risk would be accepted.

The second area is of non-accepted risks, which have small probability of occurrence, and minor loss in case of their realisation. These risks, quite naturally, are not considered during the course of analysis, or processed last, with weak restrictions on financing of ISS.

Finally, the third area represents those risks which are only included subject to available resource for financing of the protection of information.

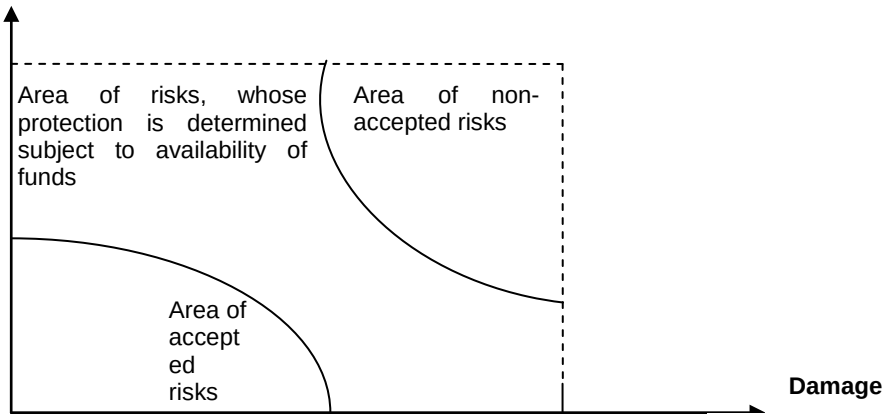


Fig. 1. Distribution of risks in two-factorial model for substantiation of expenses on information safety

This approach can be acceptable in those cases where DMP sees an approximate level of expenses on the protection of information. And this is associated, in the first place, with financial capabilities of the MS.

The methodology of substantiation of expenses on the basis of three-factorial model of information risks

More interesting is the approach to substantiation of expenses on the basis of three-factorial model of information risks, presented in FIg. 3.

The system of preferences in three-factorial model for selection of information risks from the position of DMP, could be formulated in the following form:

(6)

on the stipulation that $Z_{i-1} + Z_X < Z_0$

where x and y – comparable risks;

p_X, p_y – probabilities of risks;

u_X, u_y – value of damage for two comparable risks;

z_X, z_y – value of expenses, either associated with reduction of the damage down to acceptable level, or with its elimination for risks x and y;

z_{i-1} – total expenses at the previous (i-1) stage of comparison of information risks;

– generality quantifier;

– designation of non-rigorous dominancy of variable x over variable y.

P

Probability of risk

Area, whose protection is determined subject to availability of funds

Area, mandatory for protection

Pmin

Area, not mandatory for protection

Variants of hang-the-expense policy **(Z)**

Umin

Damage

U

Z

expenses

Fig. 2. Distribution of risks in three-factorial model for substantiation of expenses on information safety

The expression 6 has the following meaning: with paired comparison of two risks (x, y), one of which (x) has the values of probability and damage exceeding or equal to the respective values of the 2-nd risk (y), whereas expenses on reduction or elimination of risk are smaller of equal to 2-nd, the preference is given to the first (x) risk, under the stipulation that total expenses on the information safety system do not exceed the given (z_0).

The expression 2.2 does not describe all possible cases of probability ratios of risks, damage and possible expenses, for example, when $(p_x < p_y) \wedge (u_y > u_y)$, etc. In that case, it would be necessary to introduce additional parameters for the purpose of decision making about inclusion or exclusion of the respective risk. The following ratio can serve as such parameter

(2.3)

The meaning of that parameter consists in that out of two risks, the one is selected, for which the ratio between damage and expenses is higher. However, other strategies of selection of risks are possible, subject to condition of existence of limitations on the amount of expenses on the system of information safety. The three-factorial model for substantiation of expenses allows to elaborate a formalized procedure for substantiation of decision-making for DMP in the sphere of protection of information.

Conclusions

The existing regulations and risks controlling mechanisms are not convincing for DMP while creating an information safety system, by virtue of their weak association with the goals of business, economic and financial activity of any organisation.

The used financial instruments for evaluation of economic efficiency of financial investments are also practically cannot be used for evaluation of the necessary level of expenses on ISS MS. The main reason of this fact consists in that in all tools of performance evaluation, return of financial investments is supposed, whereas in the analysis of efficiency of ISS, this parameter is shown in the form of prevented damage, which, in addition, has a probabilistic nature. For DMP, additional factors should be taken into account, allowing to evaluate the level of rationality of expenses on ISS.

Three-factorial models in many cases allow to construct ISS MS on the basis of revealing of the system of preferences of DMP, and in some cases, allow to find conditionally-optimum solutions for protection of information.

Literature

Standard, GOST R ISO/IEC 17799-2005. "Information technology. Practical rules of management of information safety";

Standard, GOST R ISO/IEC 27001-2006 "Information technology. Safety methods and means. Systems of management of information safety. Requirements";

Standard, GOST R ISO/IEC 13335-1-2006 "Information technology. Safety methods and means. Part 1. The concept and models of management of the safety of information and telecommunication technologies";

Standard, GOST R ISO/IEC 13335-3-2006 "Information technology. Safety methods and means. Part 3. Methods of management of the safety of information technologies".

Введение

Система информационной безопасности сегодня становится необходимым условием успешного ведения любого вида деятельности хозяйствующего субъекта. При этом, если вопрос о целесообразности создания системы информационной безопасности (СИБ) для хозяйствующего субъекта (ХС) не подвергается обсуждению, то вопрос о рациональных объемах финансирования затрат на защиту информации все еще остается открытым для лиц, принимающих решение (ЛПР). Нельзя сказать, что нет внимания к этой проблеме. В специализированных изданиях периодически появляются публикации на эту тему, но научно-обоснованных и верифицированных механизмов обоснования затрат на создание СИБ, учитывающих, значимые для ЛПР факторы, сегодня не существует. С другой стороны, используемые сегодня специалистами по защите информации нормативные документы по управлению информационными рисками, организации систем информационной безопасности и другие документы [1-4], рассматривают эту проблему преимущественно только со стороны специалиста по организации СИБ и управлению информационными рисками, что далеко не всегда является убедительным для ЛПР, принимающих решения на финансирование СИБ.

В этой работе рассматриваются некоторые новые подходы к обоснованию затрат на организацию СИБ ХС с учетом различных факторов, значений рисков и ограничений, позволяющих в полной мере реализовать принцип «рациональной достаточности» при организации СИБ ХС.

Два взгляда на проблему

Вообще говоря, количество мнений и взглядов на структуру и организацию СИБ ХС значительно больше двух. Свой взгляд на ее рациональную организацию имеют, кроме ЛПР, бухгалтеры, экономисты, юристы, менеджеры и другие сотрудники, участвующие в процессах приема, обработки, хранения и передачи информации, организующее делопроизводство, либо обслуживающие вычислительную технику, средства коммуникаций и связи. Мы рассмотрим мнения и позиции только двух основных участников процесса обоснования затрат: ЛПР по определению бюджета на систему на СИБ и Специалиста по информационной безопасности. Анализ показал, что они совершенно по разному относятся к этому процессу (табл.1).

Таблица №1

Взгляды различных специалистов на механизмы обоснования затрат на систему информационной безопасности организации

№ №	ЛПР	Специалист по защите информации
	Механизм обоснования затрат	
1	Защита информации – это необходимая функция ведения современного бизнеса, поэтому для принятия решения по защите информации ЛПР требуется не	Защита информации – это функция Службы информационной безопасности по обеспечению бизнеса.

	только знания вероятности риска и возможности ущерба, но и другая информация, обычно используемая для оценки эффективности бизнеса: • затраты на реализацию защитных мер по каждому риску (Z_i) Желательно, чтобы эти затраты были распределены по времени в планируемом периоде; • коэффициенты ликвидности активов (K_i), относящихся к сфере обеспечения информационной безопасности по каждому риску; • описание характеристик возникновения риска (одномоментное событие, реализация угрозы в полном объеме или серии инцидентов, в которых угроза реализуется постепенно и т.д.); • динамика морального износа активов, относящихся к риску для формирования системы их амортизационных отчислений; • комбинации этих показателей, например, отношение затрат на снижение риска и возможного ущерба при его реализации и др.	Финансирование затрат на информационную безопасность производится на основании результатов оценки и анализа рисков существующими механизмами управления рисками [2]. Экономические методы оценки эффективности при этом не используются. В основе оценки риска лежит мультипликативный критерий, который задается качественной или количественной оценкой вероятности и ущерба в форме мультипликативного критерия : R= U*P, (1) где U – значение ущерба; P – вероятность возникновения риска.
2	**Идеальная модель затрат на СИБ**	
	$Z = \sum_i z_i \to \min$, (2) при $u_i >> z_i$, $p_i \geq p_0$, $Z \leq Z_0$ где $i \in I$, *I* – область принимаемых, снижаемых или передаваемых рисков; u_i – ущерб по i-му риску; p_i – вероятность i-го риска; p_o – вероятность, при которой принимаются риски. Определяется чаще всего с точки Специалиста по защите информации. Z_0 – предельно допустимые затраты с точки зрения ЛПР. Возможен и другой подход. Например, при заданном уровне бюджета Z_0 построить СИБ, при которой возможно максимальное снижение ущерба от реализации рисков: $U = \sum_i u_i \to \max$ (4)	$Z = \sum_i z_i$ (3) при $r_i \geq r_0$, $r_i = u_i p_i$ где $i \in I$, r_o – граница рисков, определяемая чаще всего с точки Специалиста по защите информации. r_i – текущий риск.

Как видно из таблицы точки зрения на организацию СИБ ХС в значительной степени отличаются. При этом, если действия Специалиста по защите информации регламентированы отечественными и зарубежными стандартами, то для ЛПР сегодня не существует убедительных механизмов принятия решений на финансирование СИБ. Кроме того, подход к оценке величины риска по одному показателю (1) может быть приемлемым только в тех случаях, когда ущерб наносится постоянно в течение рассматриваемого периода Δt, а функция плотности распределения P(t) имеет вид равномерного закона распределения. При обработке информационных рисков совершенно не учитываются затраты, связанные с уменьшением, передачей или устранением риска. Это не позволяет оценить в полной мере эффективность решений по защите информационной системы хозяйствующего субъекта. Таким образом, существующие подходы к оценке и обработке рисков не

являются убедительными для ЛПР и требуются другие механизмы оценки эффективности предлагаемых решений в сфере защиты информации.

Анализ существующих подходов к обоснованию затрат на систему информационной безопасности

Первые попытки создания механизмов оценки эффективности решений по защите информации, вполне естественно, были основаны на применении финансово-аналитических и инвестиционных инструментов по аналогии с оценкой эффективности IT. Но если для IT такой подход может быть во многих случаях обоснован, так как предоставляет аналитикам возможность оценить или измерить экономические эффекты от внедрения IT, то для СИБ это большая проблема. Сущность ее заключается в том, что происходит подмена понятий при оценке экономических эффектов. Для инвестиционных проектов в качестве основного показателя экономической эффективности рассматривается изменение прибыли ХС до и после внедрения проекта, а при оценке эффективности вложений в СИБ рассматривается оценка предотвращенного ущерба, которая носит вероятностный характер и не может быть измерена объективно и показана в бухгалтерском балансе предприятия. Полученные эффекты от защиты «растворяются» среди других мероприятий организационного и технического характера, поэтому оценить их конкретно не всегда представляется возможным. Более того, активы, связанные с защитой информации оказывают влияние на себестоимость продукции и уменьшают прибыль. Эти обстоятельства привели к тому, что возникла необходимость создания новых подходов к обоснованию затрат, которые были бы понятны ЛПР и учитывали бы вероятностный характер информационных рисков.

Методика обоснования затрат на основе двухфакторной модели информационных рисков

Наиболее простым является метод оценки рисков на основе двухфакторной модели

$$R =< P, U >, \text{ при } Z \le Z_0 \qquad (5)$$

Сущность механизма обоснования затрат представлена на рис.1. Все информационные риски отображаются в системе координат (Вероятность, Ущерб). При этом выделяют несколько областей для анализа:

Первая область (правый верхний угол) представляет собой риски, вероятность которых высока, а ущерб при их реализации существенный. Эта область принимаемых рисков, а значит ХС будет нести определенные затраты на их предотвращение, передачу или снижение. При обработке каждого риска проверяется условие (5). В том случае, если оно выполняется, риск принимается.

Вторая область – непринимаемых рисков, которые имеют малую вероятность возникновения и незначительный ущерб при их реализации. Эти риски, вполне естественно не рассматриваются в ходе анализа , либо обрабатываются в последнюю очередь при слабых ограничениях на финансирование СИБ.

Наконец, третья область представляет собой те риски, которые включаются только при имеющимся ресурсе на финансирование защиты информации.

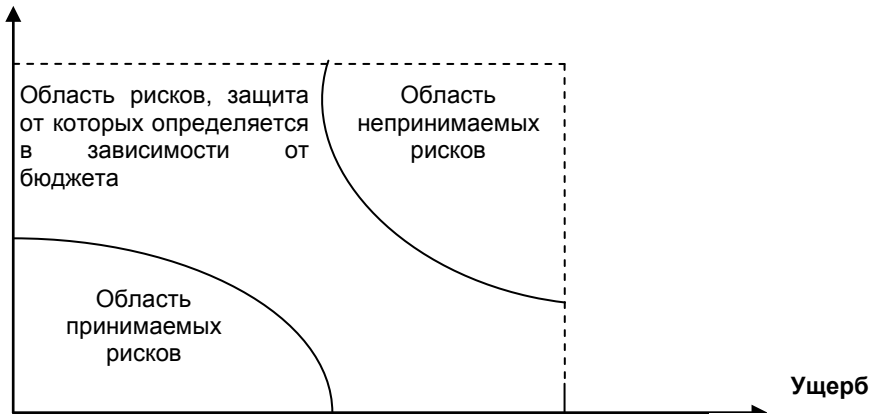


Рис.1. Распределение рисков в двухфакторной модели обоснования затрат на информационную безопасность

Такой подход может быть приемлем в тех случаях, если ЛПР представляет себе примерный уровень затрат на защиту информации. А это связано, прежде всего, с финансовыми возможностями ХС.

Методика обоснования затрат на основе трехфакторной модели информационных рисков

Более интересным, является подход к обоснованию затрат на основе трехфакторной модели информационных рисков, представленной на рис.3.

Систему предпочтений в трехфакторной модели выбора информационных рисков с позиций ЛПР можно сформулировать в следующем виде:

$$\forall(x,y)((p_x \geq p_y) \wedge (u_x \geq u_y) \wedge (z_x \leq z_y)) \rightarrow x \succ\approx y \quad (6)$$

при условии, что $z_{i-1} + z_x \leq z_0$

где x и y – сравниваемые риски;

p_x, p_y - вероятности рисков;

u_x, u_y - значения ущерба для двух сравниваемых рисков;

z_x, z_y - значение затрат, связанных либо со снижением ущерба до допустимого уровня, либо с его исключением для рисков x и y;

z_{i-1} - суммарные затраты на предыдущем (i-1) этапе сравнения информационных рисков;

$\forall$ - квантор общности;

$x \succ\approx y$ - обозначение нестрогого превосходства переменной x над y.

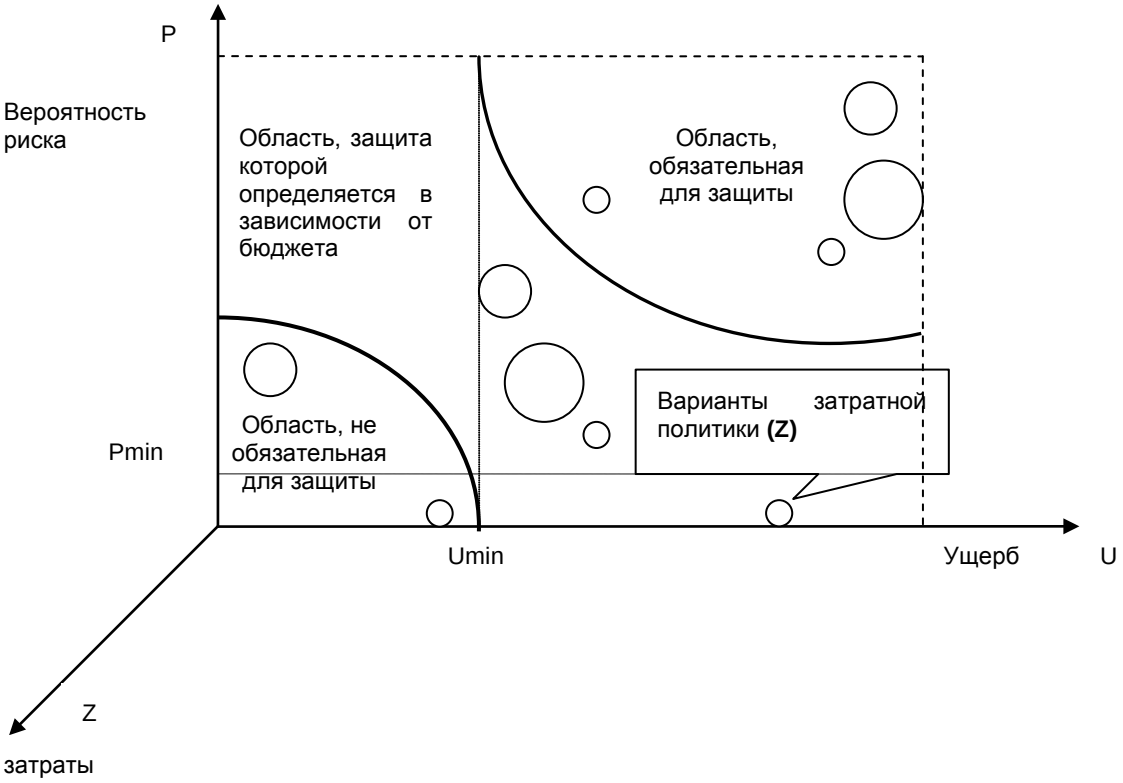


Рис.2. Распределение рисков в трехфакторной модели обоснования затрат на информационную безопасность

Выражение 6 имеет следующий смысл: при парном сравнении двух рисков (x,y), у одного из которых (x) значения вероятности и ущерба больше или равно соответствующим значениям 2-го риска (y), а затраты на снижение или устранение риска меньше или равны 2-му, предпочтение отдается первому (x) риску, при условии, что суммарные затраты на систему информационной безопасности не превышают заданных (z_0).

Выражение 2.2 не описывает все возможные случаи отношений вероятностей рисков, ущерба и возможных затрат, например, когда $(p_x < p_y) \wedge (u_x > u_y)$ и т.д. В этом случае необходимо вводить дополнительные показатели для принятия решения о включении и исключении соответствующего риска. Таким показателем может быть отношение

$$\left(\frac{u_x}{z_x} > \frac{u_y}{z_y} \right) \qquad (2.3)$$

Смысл этого отношения заключается в том, что из двух рисков выбирается тот, для которого отношения ущерба к затратам больше. Но возможны также и другие стратегии выбора рисков при условии существования ограничений по величине затрат на систему информационной безопасности. Трехфакторная модель обоснования затрат позволяет разработать формализованную процедуру обоснования решений в сфере защиты информаций для ЛПР.

Выводы

Существующие регламенты и механизмы управления рисками при создании системы информационной безопасности не являются убедительными для ЛПР в силу их малой связи с целями хозяйственной, экономической и финансовой деятельности любой организации.

Используемые финансовые инструменты для оценки экономической эффективности финансовых вложений также практически не могут быть использованы при оценке необходимого уровня затрат на СИБ ХС. Основная причина этого факта заключается в том, что во всех инструментах оценки эффективности предполагается возврат финансовых вложений, в то же время при анализе эффективности СИБ этот показатель проявляется в форме предотвращенного ущерба, который, к тому же, носит вероятностный характер. Для ЛПР должны быть учтены дополнительные факторы, позволяющие оценить уровень рациональности затрат на СИБ.

Трехфакторные модели во многих случаях позволяют построить СИБ ХС на основе выявления системы предпочтений ЛПР, а в некоторых случаях позволяют находить условно-оптимальные решения по защите информации.

Литература

Стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;

Стандарт ГОСТ Р ИСО/МЭК 27001-2006 ««Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

Стандарт ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»;

Стандарт ГОСТ Р ИСО/МЭК 13335-3-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».

Состояние рынка мобильных антивирусов: теоретические перспективы и практические методы. Особенности рынка платного мобильного контента и способы продвижения

Новоселов Н.А.

Южный Федеральный Университет
г. Ростов-на-Дону, Россия
Nik_novoselov@mail.ru

The state of the transportable antiviruses market: theoretical perspectives and practical methods. Features of the paid mobile content market and methods of advancement

Novoselov N.A.

Southern Federal University
Rostov-na-Donu, Russia
Nik_novoselov@mail.ru

The mobile antiviruses which have widely appeared in 2004-2005, till now, contrary to a prediction of analysts have not taken a worthy place in the market of a mobile content. We will consider a complex way of

development of the given segment of the market, consisting in notification of consumers, positioning «Kasperskij=mobile antivirus= comfort » with usage of modern communications and resources PR.

Мобильные антивирусы, широко появившиеся в 2004-2005 году, до сих пор, вопреки предсказанию аналитиков не заняли достойного места на рынке мобильного контента.

Широкое распространение мобильных устройств, каналов связи, усложнение платформы и используемых приложений не способствовали росту продаж средств защиты. Рассмотрим комплексный способ развития данного сегмента рынка, заключающейся в осведомлении потребителей, позионировании «Касперский=мобильный антивирус=комфорт» с использованием современных коммуникаций и средств PR.

Исследование сегмента.

Вводная часть

Причина малого распространения мобильных антивирусов отсутствие понимания пользователей о надобности защиты.

Товары, не относящиеся к товарам первой необходимости, покупаются по двум причинам: реальная или виртуальная надобность. Ко второй группе относится широкий выбор виртуальных атрибутов, необходимых для индивидуума, например: похудание (хлебцы, биодобавки), социальный статус (украшения), эмоциональный статус (импульсивные покупки) и другие. Один и тот же товар может иметь социальную и эмоциональную ценность. Атрибуты в сочетании с потребностями формируют полезность товара, субъективно воспринимаемую индивидуумом.

ПОЛЕЗНОСТЬ - удовольствие, удовлетворение потребностей, исполнение запросов, которое получают люди от потребления товаров и пользования услугами.

Виртуальные атрибуты антивируса

Антивирус в целом значит для пользователя: безопасность, надежность защиты, комфорт, стабильность. При этом первые два фактора не важны для многих пользователей: компьютеры не содержат конфиденциальной или коммерческой информации. Мотивация типичных пользователей основывается на эмоциональном уровне: страх материальных потерь, обмана, нарушения функционирования компьютера. Следовательно, антивирус – это товар, обладающий виртуальными эмоциональными атрибутами. Клиент, приобретая антивирус, получает уверенность в эмоциональной безопасности и комфорте при работе на компьютере.

Вышесказанное относится также и к мобильным устройствам. Пользователи все чаще становятся зависимыми от качества их работы: контакты в единственном экземпляре, органайзер, доступ в Интернет, личная информация в памяти.

Логично, что многие пользователи мобильных устройств при наличии или ощущении угрозы будут стремиться обезопасить свой привычный образ жизни, состояние и информацию. Вторая часть определения полезности состоит из осознания потребителя надобности продукта, того, что он получит при его использовании. Понимание может сформироваться и как следствие проблемы, и как получение ощущения потребности извне. То есть, для примера, может быть реальный вирус или средствами PR и рекламы создать ощущение необходимости, обязательности наличия программного обеспечения на компьютере. Но и случай явной проблемы требует наличия информации о возможностях решения, доступного, понятного и оперативного.

В итоге, для того, чтобы пользователь принял решение о полезности и приобрел программное обеспечение, у него должна быть сформирована потребность и известен способ ее удовлетворения. Только после этого, исходя из ожиданий, он прибегает к тому или иному решению. То есть покупает, тот или иной антивирус, исходя из доступной или известной ему информации.

Создание потребности

Для создания категории необходимо создать атрибут в сознании потребителей. Чем значимей и важнее он будет для пользователей как необходимость, тем чаще будут приниматься решении о покупке. При этом, товар или услуга на основе которого создается категория, чаще всего остаются лидером рынка. Важно учесть, что новинка должна быть в сознании потребителя, а не в рейтингах специализированных изданий.

Анализ рынка

Анализ предложения рынка

Введем в поисковом запросе «антивирус для мобильного» и проанализируем ТОП 10 – это то, что обычно видит потенциальный потребитель.

Первые две результата поиска – являются ссылками на ресурс закачки программного обеспечения, причем без удовлетворительного уровня информации о продукте. Остальные ссылки – 4 более годовалой давности, две ссылки имеют более пятилетнюю историю: 2003 и 2004 год. Другой запрос «вирусы на мобильном» дает первой ссылку на Касперский.ру на новость о Cabir-е от 2004 года, «антивирус телефон» - самый большой по количеству запросов поиск – 8 тыс. за последний месяц . Первый результат – ветка форума от 2005 года.

В итоге, пользователь не получает информацию об актуальности и важности темы и может посчитать это видом Интернет аферы.

Анализ возможностей спроса рынка

1. **Количество устройств.** Одним из главных факторов-показателей емкости рынка программного обеспечения является количество устройств, способных его использовать. Рассмотрим сектора:

    1. Средства связи: мобильные телефоны, смартфоны, коммуникаторы. Как сообщает Ассоциация GSM, общее число мобильных подключений в мире добралось до 4-х миллиардов 2009. По прогнозам Ассоциации, уже в 2013 году их количество может составить около 6 миллиардов, что эквивалентно почти всему сегодняшнему населению планеты

    Интересно отметить, что мировой финансовый кризис по прогнозам аналитиков не даст прекратиться росту продаж умных телефонов, и процент прироста рынка будет равен 5-7% [4].

    2. GPS (системы глобального позиционирования). Согласно новому отчету Berg Insight, объёмы продаж PND в Европе и Северной Америке будут продолжать расти следующие 10 лет. Максимума они достигнут в 2012 году с объёмом в 56 млн. штук.

    3. КПК (карманные персональные компьютеры). Вымирают как сегмент рынок в пользу коммуникаторов.

    4. Нетбуки (малые ноутбуки). Продажи нетбуков в 2009 году превысят 35 миллионов штук.

    5. Модули компьютерных систем (принтеров, мышей, приводов).

    6. Бытовая техника, умные дома.

    7. Видео - и игровые приставки.

Видно, что явно прослеживается рост рынка мобильных устройств. При этом большинство пользователей не отличает тип мобильного устройства, его характерные особенности и платформу. Как будет дальше указано, уровень знания определяется возрастом и в целом прогрессирует со временем, особенно в России. На отечественном рынке уровень продвинутого пользователя – редкость, когда, например, в Германии 20% населения имеет данные навыки

2. **Емкость рынка.** Количество средств, затрачиваемое на мобильный контент растет. Общее количество мобильных платежей к 2013 году составит $860 млрд., выручка - $10 млрд.

3. **Мобильный трафик.** Исследование Cisco показало: за пять лет объем мобильного трафика должен вырасти в 66 раз (Рис. 1).



Рис.1. Рост трафика в мире.

Рынок демонстрирует хорошую динамику, как со стороны пользователей, так и со стороны операторов услуг и ритейлеров. Последние стимулируют опять интерес клиентов. При этом Российский рынок далек от насыщения, в сравнении с общемировым уровнем. Так же он изолирован от мировых компаний за счет недоработок правовой базы, непонятной позиции правительства, непрозрачности рынка и прочих факторов.

Анализ пользователей и восприятия сегмента.

1. **Стратификация в виртуальном пространстве.** Человек, пользующийся современными технологиями и Интернетом, имеет определенный уровень «компьютерной грамотности» и определенным образом ведет себя в сети – создает и поддерживает образ или образы. Исходя из этого, пользователи делятся на классы и целевые аудитории по другим принципам. Стратификация ведется по уровню знания компьютера, программного обеспечения и поведению с коммуникативными особенностями в сети Интернет. Действительно, принадлежность к определенным группам в сети по большей части определяется не социальным или должностным статусом человека, а набором личных компетенций/навыков.

2. **Особенности сегмента мобильного ПО.**

Рынок мобильных интеллектуальных машин образован сегментацией первоначального рынка стационарных систем. Мобильный контент образован похожим способом. Но, в отличие от первого, второй рынок обладает существенными особенностями. Как следствие, на данном этапе развития, рынок мобильных программных решений позволяет глобальный брендовый подход.

3. **Мировые тенденции маркетинга**.

Общемировые тенденции рынка программного обеспечения – директ маркетинг. Данный подход означает не только создание ПО специально для определенных платформ, но и способы продвижения, рассчитанные на очень узкую целевую аудиторию или вообще конкретного человека.

4. **Система Media relations.**

Витруально-интерактивный способ продвижения для контента является почти единственным: он на порядке дешевле, изначально учитывает фокусировки и позволяет использовать определенные бонусы, которые будут рассмотрены именно в блоке формирования медиа плана далее.

Медиаплан

На основе данных можно поострить медиаплан продвижения мобильного антивируса.

1. **Подготовка**.

Очень важно иметь хорошую аналитическую базу: на ее основе вероятно предугадать варианты развития рынка. Также, важно понять ведущие ассоциативные ряды в сознании потребителей, динамику их развития. Важна подготовка, вплоть до действий менеджеров и готовых публикаций, так как сфера информационных технологий гораздо мобильней и динамичней существующих методов. Сравнимо с эффективностью и доверием к «сарафанному радио» и скоростью

репортажа в реальном времени с доступом в 24 часа. Также, в отличии от существующих СМИ, любой пользователь может достаточно точно транслировать и пересылать готовые тексты. Любая ошибка войдет в века.

2. **Этап начальной реализации**.

Данный этап необходимо сопровождать исследованиями и количествами запросов и поиска по информационным ресурсам.

Методы воздействия вводятся последовательно и в последствии не отбрасываются, а модернизируются и контролируются. Важно соблюдать лидерство по всем параметрам: обсуждаемость, ТОП10 и прочее. Новости и информации должны быть близки к ЦА и находится в ее системе ценностей, при фокусировании на существенно разных ЦА, необходимо контролировать отсутствие конфликтных пересечений и то, что атрибут не должен противоречить ценностям групп. Итогом должен стать того, что проинформировано все общество и определенные группы становятся двигателями продвижения, генераторам информации. Надо учесть факт перетрансляции информации и то, что данная информация будет понятна и лояльно для всего общества.

3. **Полная реализация, наращивание темпов.**

Этап реализации предполагает доходность существующего рынка или приближение к прибылям. Мониторинг аудиторий носит выборочный характер, и в случае удачного развития событий предполагает рассмотрение нишевых категорий и последовательный их захват. Результат: создание у пользователя постоянной необходимости в актуальной защите мобильным антивирусом, который отождествляется с созданным брэндом.

4. **Поддержание существования сегмента.**

Реализация этого плана не требует чрезмерного финансирования: существующие средства Интернет коммуникаций слабо заполнены рекламой, очень подвижны и перспективны. Требуется большое количество и высокий уровень креатива, обеспеченного качественной коммуникационной поддержкой. Как указывалось ранее, рынок чувствителен к скорости ответа. Для этого, подразделение по работе в этом направлении должно иметь четкую систему, прозрачность, высокий корпоративный дух. Необходима четко простроенная горизонтально простроенная система, автоматизированная и кризисоустойчивая.

Если вернуться к прогнозам развития мобильного рынка, становится ясно, что данный сегмент рынка является емким и прибыльным в дальнейшем.

Экономические модели и аналитические аспекты информационной безопасности

Семенихина В.С.

Пермский государственный университет
г. Пермь, Россия
svarya@mail.ru

Economic models and analytical aspects of information safety

Semenihina V.S.

Perm state university
Perm, Russia
svarya@mail.ru

At the time of well-being, growth of quotations, rates and parameters of profitableness, the issues of optimisation, achievement of maximum efficiency, were considered, most likely, in a formal manner. Whereas in the developed situation, where most part of companies assume reduction of budgets on maintaining the facilities of information technology (IT) by one-fifth (and maybe more), this problem becomes vital. More and more risks-managers address such parameters like TCO, TEI, and others, in their search of the ways of maximally reliable counting up of all losses borne by the organisations.

Crisis is the time of changes, and the most suitable time to look more intently, at where, and on what, the cash flows are directed. Now, when addressing the items of expenses, including on IT, it would be necessary to understand, what you would get in return for these expenditures. Correlation between risks and the system of safety that exist, is a practical first stage on the way of improvement of expenditures on information safety. What shall be right at the beginning? The basis for consideration of safety of an AS shall be formed by the analysis of threats and risks.

In the work I have considered threats and risks of companies, depending on the readiness of their system of information safety (IS). Having looked at statistics of Garther Group about the percentage ratio of the companies of various levels, a joyful conclusion was made, that the companies, during the days of rapid growth, similarly actively developed their IT-systems. And at the times of severe economy on the expenses which are not being basic at creation of the goods or services, many will only be satisfied with maintaining their existing system. Sometimes it will be enough to ensure safety of information system of the enterprise. And it is first of all associated with the fact, that a large number of companies (55%) are on the 2 and the third level in terms of the degree of readiness of there IS systems. Thus, these companies can provide former reliability of the system even with such essential reductions of financing. But achieving of any level of safety of an enterprise is not guaranteed by the protections themselves. Here, determining would be conformity of measures with available threats. If during the analysis it has been revealed, that measures and expenses differ, it would be necessary to begin to think about re-structuring of the system of IS. What is it fraught with? First of all, it would be necessary to understand, which volume of money resources and for which needs would be required. For that purpose, a number of basic methodologies exist, for calculation of the various parameters, from applied information economy assisting in analysis of risks, to aggregate cost of ownership, which allows to estimate direct and indirect expenses borne by an enterprise in connection with the maintenance of IT-system.

For convenience of consideration, these methodologies are grouped by the purposes of destination. Probabilistic techniques are helpful in the analysis of risks, qualitative – in case where rating is required, of the effect from expenses of money resources on realization of protection against this or another threat, and financial – for direct calculations of monetary resources. It would be desirable to note, that qualitative ones are very obvious for demonstration by what methods and means the threats are neutralized, and how these methods and means are optimal.

Notwithstanding the fact, that calculations form rather simple task, in case of information safety this is not the case. Except for direct costs, such as expenses on acquisition of technical and software means, there are still such expenses, like idle time and user expenses. I hope, that in my work it is maximally easily stated, what are these expenses, and why they are required to be taken into account. In addition, the question of calculation of expenses appeared to be not such one-sided and simple, namely because of that, existing models of TCO both have the right exist and are actively used. During studying of the existing models and approaches of the Garther Group and Microsoft companies, I understood that they do not meet all requirements, and do not reflect all points of view as regards safety issues. Three variants of the angle of consideration of this question, proposed by me, should pass practical tests, in order that it would be possible to draw a conclusion on how convenient they are in use, and meet the existing needs of new approaches.

The material examined and considered by me is capable of helping at the final stage of work in the analysis of the system of information safety, and the models considered by me and the methods of approach to this question are capable of helping in simplifying the stage of financial calculations. Having understood it, the companies can be sure, that expenses on IT will not do harm to their enterprises, and can only be of use during hard times of financial instability.

Во времена благополучия, роста котировок, курсов и показателей доходности, вопросами оптимизации, достижения максимальной эффективности занимались скорее формально. В сложившейся же ситуации, когда большая часть компаний предполагает сокращение бюджетов на поддержание ИТ-средств на одну пятую (а то и больше), этот вопрос стоит максимально остро. Все больше риск-менеджеров обращается к таким показателям как TCO, TEI, и другие, в поисках способов максимально достоверно подсчитать все убытки, которые несут организации.

Кризис – время перемен, и самое подходящее время пристальнее взглянуть на то, куда и на что направляются денежные потоки. Сейчас, обращаясь к статьям расходов на ИТ в том числе, нужно понимать, что получишь в замен на эти расходы. Соотнесение рисков и той системы безопасности что существует – практический первый этап на пути оздоровления расходов на информационную безопасность. Что же в самом начале? Основой рассмотрения безопасности АС является анализ угроз и рисков.

В своей работе я рассмотрела, каковы угрозы и риски компаний в зависимости от зрелости их системы ИБ. Посмотрев на статистику Garther Group о процентном соотношении компаний различных уровней, радостным заключением стало то, что компании во времена бурного роста столь же активно развивали и свои ИТ-системы. И во времена суровой экономии на затратах, не являющихся основными при создании товара или услуги, многие будут довольствоваться лишь поддержанием существующей системы. Иногда этого будет достаточно, чтобы обеспечить безопасность информационной системы предприятия. И это прежде всего связанно с тем, что большее количество компаний (55%), имеют находятся на 2 и третьем уровне по уровню зрелости своих систем ИБ. Таким образом, эти компании смогут обеспечить прежнюю надежность системы даже при столь существенных сокращениях финансирования. Но достижения какого-либо уровня безопасности предприятия не гарантируют сами по себе защищенности. Определяющим здесь является – соответствие мер с имеющимися угрозами. Если в ходе анализа было выявлено, что меры и затраты различаются, стоит задуматься о реструктуризации системы ИБ. Чем это чревато? В первую очередь, необходимо понять, какой объем денежных средств и на какие нужды необходим. Для этого существует несколько основных методологий подсчета различных показателей, от прикладной информационной экономики, помогающей при анализе рисков, до совокупной стоимости владения, которая позволяет оценить прямые и косвенные затраты, которые несет предприятие в связи с содержанием ИТ-системы.

Для удобства рассмотрения, эти методологии сгруппированы по целям назначения. Вероятностные методики приходят на помощь при анализе рисков, качественные – в случае необходимости оценки эффекта от затрат денежных средств на реализацию защиты от той или иной угрозы, и финансовые – при непосредственных денежных подсчетах. Хочется отметить, что качественные, позволяют являются очень наглядными для демонстрации какими методами и средствами нейтрализуются угрозы, и на сколько эти методы и средства являются оптимальными.

Не смотря на то, что подсчеты - весьма простая задача, но в случае информационной безопасности – это не так. Кроме прямых затрат, таких как расходы на приобретение технических и программных средств, имеются ещё такие расходы как простой и пользовательские затраты. Надеюсь, что в моей работе максимально доступно изложено что это за затраты и почему их необходимо учитывать. Кроме этого, вопрос подсчета затрат оказался не таким однобоким и простым, именно по этому существующие модели TCO обе имею право на жизнь и активно используются. В ходе изучения существующих моделей и подходов компаний Garther Group и Microsoft, поняла, что они не отвечают

всем потребностям и не отражают всех взглядов на вопросы безопасности. Предложенные мной три варианта угла рассмотрения этого вопроса должны пройти практические испытания, чтобы можно было сделать вывод о том, насколько они удобны в использовании и отвечают существующим потребностям в новых подходах.

Изученной и рассмотренный мной материал способен помочь на конечном этапе работы по анализу системы информационной безопасности, и рассмотренные мною модели и методы подхода к этому вопросы способны помочь упростить этап финансовых подсчетов. Разобравшись с ним, компании могут быть уверены, что расходы на ИТ не повредят их предприятиям, и смогут приносит только пользу в тяжелые времена финансовой нестабильности

Метод оценки экономической эффективности внедрения криптографических систем

Смирнов М.О.

Нижегородский государственный университет им Н.И. Лобачевского
г. Нижний Новгород, Россия
mishasmirnov@yandex.ru

Method for estimating the economic efficiency of introducing cryptographic systems

Smirnov M.O.

Nizhniy Novgorod state university it N.I. Lobachevsky
Nizhniy Novgorod, Russia
mishasmirnov@yandex.ru

In the present work provides a method for calculating the economic efficiency of the implementation of cryptographic protection to changing the parameters of safety. Economic efficiency is measured in monetary terms, which allow you to choose the best system for the business in terms of economic processes.

Performance evaluation in case of introduction of cryptographic protection systems (CPS) becomes more and more topical in connection with rapid development of the technologies of protection and cracking of such systems. In many cryptographic algorithms existing today, it is possible to flexibly enough choose the length of the key. On the one hand, there are recommended lengths, which would be securely safe, and on the other hand, the market is growing, of low-power devices, for which cryptography is necessary, too. For such devices, there is frequently a problem of saving the resources, owing to which problem, the application of complicated algorithms is unacceptable, since it results in essential rise in price of the devices. Such evaluation is especially topical now, since overpayment for an excessive level of protection is inexpedient, though on the other hand there is a risk of application of an unreliable system.

The task of this article has been the development of a technique for evaluation of economic efficiency of introduction of a CPS, expressed as money equivalent. For such evaluation, the concept of risk is used, as the average value of the size of deficient profit, as against the desirable profit [1]. We shall consider the main varied parameter to be the length of key, upon which the crypt-stability is dependent.

This particular definition of risk was chosen because of the results of calculations that would be most understandable for businessmen. If explain the efficiency of cryptographic system in mathematical terms, to a person without mathematical education, it would be difficult for him to choose an optimal alternative. If we give a financial substantiation based on particular material benefit of this system for a businessman, he could select the variant that is most suitable to him. Those systems for which economic efficiency has been calculated, gain a considerable preference in the market.

There are several methods of evaluation of damage resulted from cracking. All of them use three basic characteristics of crypt-stability of the system [2]:

$C_{кр}$ – mathematical expectation of the number of operations required to crack the system;

$DC_{кр}$ – dispersion of mathematical expectation of the number of operations for cracking;

$P(L, C)$ – probability of cracking of algorithm with the length of a key L by C operations.

Knowing these characteristics, it is possible to count the losses at cracking, and time of cracking. However, the existing methods do not give an answer to the question: what material losses will be in case of cracking, since cracking of CPS has probabilistic nature, which is not taken into account in any way in these methods. It is possible, that even a single cracking would be enough for the system not to pay back, as the profit received from it, is a probabilistic value, too, and it is necessary to take that into account in calculations, alongside with the losses from cracking.

We shall construct algorithm for calculation of risk. If there is certain information system, which even in an indirect manner promotes earning of profit of the company, then it would be the necessary condition for origination of CPS.

The profit Π is formed by the proceeds, received with the help of information system and expenses on its use $З$. These expenses are summed from obligatory expenses $З_0$ (which would definitely be spent, hence, their dispersion equals to zero), and the expenses suffered as a result of cracking of the system $З_{ВЗ}$, that would be received by the attacker, who successfully cracked the information system. We shall designate as $В$, the average value of proceeds with dispersion DB. The values $В$ Π, $З$ are necessarily calculated at financial planning, so the company would have to know, how many it plans to spend and receive.

Let us consider that system will be cracked with probability $P_{ВЗ}$. We shall present formulas for computation of profit and risk.

1) We shall calculate the average and dispersion of expenses:

Expenses	$З_0$	$З_0 + З_{ВЗ}$
Probability	$1-P_{ВЗ}$	$P_{ВЗ}$

$$З = З_0(1-P_{ВЗ})+ P_{ВЗ}(З_0+ З_{ВЗ}),$$

$$DЗ = EЗ^2 - З^2,$$

where, $EЗ^2 = З_0^2(1-P_{ВЗ})+ P_{ВЗ}(З_0+ З_{ВЗ})^2$.

2) Let us obtain financial result:

$$Q=B-З,$$

$$DQ=DB + DЗ + 2\rho\, DB \cdot DЗ,$$

where, ρ – correlation factor.

3) Considering that Π is function of Q, it would not be difficult to obtain an expression for average value and dispersion of profit [3]:

where $\gamma(t) = 0.5 + \Phi(t)$; – Laplace function; – Gauss function.

4) Suppose, it is necessary to get the profit in amount of Π_0. Then the deficient profit:

$\Delta\Pi$	0	Π_0-Π
if	$\Pi >= \Pi_0$	$\Pi < \Pi_0$

We shall introduce an auxiliary value $z = \Pi_0-\Pi$ and find its probabilistic characteristics:

$z = \Pi_0 - \Pi$; $D_Z=D\Pi$.

Considering, that z has a normal distribution with parameters z and D_Z, one may obtain expression for the average value $\Delta\Pi$:

,

.

5) By taking, as the desirable profit, $\Pi_0= B - З_0$, one can show, how the financial risk changes depending on the parameters of safety of the system.

Having constructed the algorithm, and having determined the price of a single operation (it is presented in more detail in the main text of the article):

$Ц_{1оп} = 2\ 10^{-13}$ roubles

$DЦ_{1оп} =1.5 * 10^{-27}$,

one can evaluate reduction of economical risk (deficient profit) of cracking of cryptographic system depending on its reliability.

In case where cryptography is used, then the probability of cracking would be reduced considerably. The attacker can afford $O = З_{ВЗ}/Ц_{1оп}$ operations. Such evaluation of the number of operations is based on an assumption, that the attacker would not spend more efforts that those equal to the cost of information. Having calculated O and DO, let us assume, that the value O has normal distribution. Knowing the function $P(L, C)$ and probability of cracking of the algorithm with a key having length of L with the help of C operations, we can then calculate probability of cracking of the system with the key having the length L:

,

where $W_{ВЗ}(C)$ – probability density of normal distribution with parameters O and DO.

Using the value $P_{ВЗ}$ in the developed algorithm, it would be possible to find the dependency of the risk of getting the profit $\Pi_0=B-З_0$ on the length of key L, in which connection, the value of risk $ДП$ would be measured in money equivalent, with the account of probabilities of getting the profit, expenses and cracking of the cryptographic algorithm.

The works presents a method for evaluation of the risk of cracking of a cryptographic system, depending on the parameter of safety of the system (for example, length of key). The given method allows to evaluate the risk in money equivalent of the deficient profit, which allows to construct performance evaluations of the CPS for the enterprises, with the consideration of their specificity, and issue recommendations with the use of financial indexes, to the clients of CPS, heads and management of the companies.

The algorithm takes into account probabilistic nature of cracking of the code and economic processes (profit earning, expenses). This allows to increase objectivity of the evaluation.

The latest achievements in the field of risk-management and financial management [1][3-5] have been applied. This technique can be used at enterprises for evaluation of the required level of protection, when

selling and configuring the systems of cryptographic protection, as well as for by development of algorithms for evaluation of potential areas of application of codes.

[1] Вайсблат Б.И. Риск-Менеджмент. НФ ГУ-ВШЭ, 2004.

[2] Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. СПб.: ГУАП, 2004.

[3] Вайсблат Б.И. Математические модели анализа инвестиционных процессов. НФ ГУ-ВШЭ, 2008.

[4] Вайсблат Б.И. Инновационный финансовый менеджмент. НФ ГУ-ВШЭ, 2008.

[5] Грабовый П.Г. Риски в современном обществе М.: Аланс, 1994.

[6] Севрук В.Т. Банковские риски. М.: Дело Лтд., 1995.

[7] Рябко Б.Я., Фионов А.Н. Основы современной криптографии. М.: Научный мир, 2004.

Оценка эффективности внедрения систем криптографической защиты (СКЗ) становится всё более и более актуальной в связи с быстрым развитием технологий защиты и вскрытия таких систем. Во многих из существующих на сегодняшний день криптографических алгоритмов можно достаточно гибко выбирать длину ключа. С одной стороны есть рекомендованные длины, которые будут гарантированно безопасны, а с другой стороны растёт рынок маломощных устройств, для которых тоже необходима криптография. Для них часто встаёт вопрос экономии ресурсов, вследствие чего применение сложных алгоритмов неприемлемо, поскольку ведёт за собой существенное удорожание устройства. Особенно актуальна такая оценка сейчас, так как переплата за излишний уровень защиты нецелесообразна, хотя с другой стороны есть опасность применения ненадёжной системы.

Задачей настоящей статьи является разработка методики оценки экономической эффективности внедрения СКЗ, выраженной в денежном эквиваленте. Для этой оценки использовано понятия риска как среднего значения величины недополученной прибыли до желаемой [1]. Главным варьируемым параметром будем считать длину ключа, от которой зависит криптостойкость.

Выбрано именно это определение риска из-за наиболее понятных для предпринимателей результатов расчетов. Если объяснять эффективность криптографический системы в математических терминах человеку без математического образования, то ему будет сложно выбрать оптимальный вариант. Если дать финансовое обоснование, основанное на конкретной материальной выгоде этой системы для предпринимателя, то он сможет выбрать наиболее подходящий для него вариант. Системы, для которых рассчитана экономическая эффективность, получают существенное преимущество на рынке.

Существует несколько методов оценки ущерба от взлома. Все они используют три основные характеристики криптостойкость системы[2]:

$C_{кр}$ – математическое ожидание числа операций для взлома;

$DC_{кр}$ – дисперсия математического ожидание числа операций для взлома;

$P(L, C)$ – вероятность взлома алгоритма с длиной ключа L за C операций.

Зная эти характеристики, можно посчитать потери при взломе и время взлома. Но существующие методы не дают ответа на вопрос: какие будут материальные потери в случае взлома, так как взлом СКЗ имеет вероятностную природу, что никак не учитывается в этих методах. Возможно, что даже одного взлома будет достаточно, чтобы система не окупилась, так как прибыль, получаемая от нее, тоже является вероятностной величиной, и это необходимо учитывать в расчетах наряду с потерями от взлома.

Построим алгоритм для расчета риска. Если имеется некая информационная система, которая пусть даже косвенным образом способствует получению прибыли компании, то это является необходимым условием возникновения СКЗ.

Прибыль Π складывается из выручки, получаемой с помощью информационной системы и затрат на её использование $З$. Эти затраты суммируются из обязательных затрат $З_0$ (которые точно

будут потрачены, следовательно, их дисперсия равна нулю) и затрат, понесённых в результате взлома системы $З_{вз}$, того, что получит атакующий, успешно взломавший информационную систему. Обозначим за $\overline{В}$ среднее значение выручки с дисперсией DB. Величины $\overline{В}$, $П$, $З$ обязательно рассчитываются при финансовом планировании, так как компании необходимо знать, сколько она планирует потратить и получить.

Будем считать, что систему взломают с вероятностью $Р_{вз}$. Приведём формулы для расчета прибыли и риска.

1) Рассчитаем среднюю величину и дисперсию затрат:

Затраты	$З_0$	$З_0 + З_{вз}$
Вероятность	$1-Р_{вз}$	$Р_{вз}$

$$\overline{З} = З_0(1-Р_{вз}) + Р_{вз}(З_0 + З_{вз}),$$

$$DЗ = EЗ^2 - \overline{З}^2,$$

где, $EЗ^2 = З_0^2(1-Р_{вз}) + Р_{вз}(З_0 + З_{вз})^2$.

2) Найдём финансовый результат:

$$\overline{Q} = \overline{В} - \overline{З},$$

$$DQ = DB + DЗ + 2\rho\sqrt{DB \cdot DЗ},$$

где, ρ – коэффициент корреляции.

3) Учитывая, что $П$ является функцией от Q нетрудно получить выражения для среднего значения и дисперсии прибыли [3]:

$$\overline{П} = \int_0^\infty x \cdot W(x)dx = \overline{Q} \cdot \gamma\left(\frac{\overline{Q}}{\sqrt{DQ}}\right) + \sqrt{DQ} \cdot \beta\left(\frac{\overline{Q}}{\sqrt{DQ}}\right),$$

$$DП = \int_0^\infty x^2 \cdot W(x)dx - \overline{П}^2 = DQ \cdot \gamma^2\left(\frac{\overline{Q}}{\sqrt{DQ}}\right),$$

где $\gamma(t) = 0.5 + \Phi(t)$; $\Phi(t) = \frac{1}{2\pi}\int_0^t e^{-\frac{x^2}{2}}dx$ – функция Лапласа; $\beta(t) = \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$ – функция Гаусса.

4) Пусть необходимо получить прибыль в размере $П_0$. Тогда недополученная прибыль:

ΔП	0	$\Pi_0 - \overline{\Pi}$
если	$\overline{\Pi} >= \Pi_0$	$\overline{\Pi} < \Pi_0$

Введём вспомогательную величину z = $\Pi_0 - \Pi$ и найдём её вероятностные характеристики:

$$\overline{z} = \Pi_0 - \overline{\Pi}; \quad Dz = D\Pi.$$

Учитывая, что z имеет нормальное распределение с параметрами $\overline{z}$ и Dz, можно получить выражения для среднего значения $\Delta\overline{\Pi}$:

$$\overline{\Delta\Pi} = \int_0^{\infty} t \cdot \frac{1}{\sqrt{2\pi}\sqrt{Dz}} \cdot \exp(-\frac{(t-\overline{z})^2}{2Dz})dt = \overline{z} \cdot \gamma(\frac{\overline{z}}{\sqrt{Dz}}) + \sqrt{Dz} \cdot \beta(\frac{\overline{z}}{\sqrt{Dz}}),$$

$$\overline{\Delta\Pi} = (\Pi_0 - \overline{\Pi}) \cdot \gamma(\frac{(\Pi_0 - \overline{\Pi})}{\sqrt{D\Pi}}) + \sqrt{Dz} \cdot \beta(\frac{(\Pi_0 - \overline{\Pi})}{\sqrt{D\Pi}}).$$

5) Взяв в качестве желаемой прибыли $\Pi_0 = \overline{B} - З_0$, можно показать, как меняется финансовый риск в зависимости от параметров безопасности системы.

Построив алгоритм и определив стоимость одной операции. Более подробно это описано в основном тексте работы):

$Ц_{1оп} = 2\ 10^{-13}$ руб.

$DЦ_{1оп} = 1{,}5 * 10^{-27}$,

можно оценить снижение экономического риска (недополученной прибыли) взлома криптографической системы в зависимости от её надёжности.

Если используется криптография, то вероятность взлома сильно уменьшится. Атакующий может позволить себе $\overline{O} = З_{вз} / Ц_{1оп}$ операций. Такая оценка количества операций основывается на предположении, что атакующий не будет тратить сил больше, чем стоит эта информация. Рассчитав $\overline{O}$ и DO, положим, что величина O распределена по нормальному закону. Зная функцию $P(L, C)$ и вероятность взлома алгоритма с ключом длины L за C операций, можем рассчитать вероятность взлома системы с ключом длины L:

$$P_{вз} = \int_{\infty}^{+\infty} P(C, L) \cdot W_{вз}(C)dC,$$

где $W_{вз}(C)$ – плотность вероятности нормального распределения с параметрами $\overline{O}$ и DO.

Используя в разработанном алгоритме значение $P_{вз}$, можно найти зависимость риска получения $\Pi_0 = \overline{B} - З_0$ от длины ключа L, причём значение риска $\overline{\Delta\Pi}$ будет измеряться в денежном

эквиваленте, с учетом вероятностей получения прибыли, затрат и взлома криптографического алгоритма.

В работе приведён метод оценки риска взлома криптографической системы в зависимости от параметра безопасности системы (например, длины ключа). Данный метод позволяет оценить риск в денежном эквиваленте недополученной прибыли, что позволяет строить оценки эффективности СКЗ для предприятий с учётом их специфики и давать клиентам СКЗ, руководителям и менеджменту компаний, рекомендации с использованием финансовых показателей.

Алгоритм учитывает вероятностную природу взлома шифра и экономических процессов (получения прибыли, затрат). Это позволяет увеличить объективность данной оценки.

Применены последние достижения в области риск-менеджмента и финансового менеджмента [1][3-5]. Методика может использоваться на предприятиях для оценки необходимого уровня защиты, при продажах и конфигурировании систем криптографической защиты, а также при разработке алгоритмов для оценки потенциальных областей применения шифров.

[1] Вайсблат Б.И. Риск-Менеджмент. НФ ГУ-ВШЭ, 2004.

[2] Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. СПб.: ГУАП, 2004.

[3] Вайсблат Б.И. Математические модели анализа инвестиционных процессов. НФ ГУ-ВШЭ, 2008.

[4] Вайсблат Б.И. Инновационный финансовый менеджмент. НФ ГУ-ВШЭ, 2008.

[5] Грабовый П.Г. Риски в современном обществе М.: Аланс, 1994.

[6] Севрук В.Т. Банковские риски. М.: Дело Лтд., 1995.

[7] Рябко Б.Я., Фионов А.Н. Основы современной криптографии. М.: Научный мир, 2004.

Разработка генератора паролей на основе мнемонических формул

Шакирова Р.И.

Башкирский государственный аграрный университет
г.Уфа, Россия
Shakira.Sh@mail.ru

Development of a password generator on the basis of mnemonic formulas

Shakirova R.I.

Bashkir state agrarian university
Ufa, Russia
Shakira.Sh@mail.ru

Две серьезные проблемы авторизации посредством пароля напрямую связаны с пользователем и с тем, как он хранит свои пароли. Во-первых, если пользователям нельзя записывать пароли, то они в

большинстве случаев выбирают легкие пароли, которые намного легче взломать, чем сложные. Помимо этого пользователи склонны использовать одни и те же пароли в разных системах авторизации.

Пользователям невероятно трудно запоминать заранее заданные случайные пароли и пароли более высокого уровня сложности, выбранные ими по предписанию. В связи с этим возникает необходимость разработки программного обеспечения, позволяющего быстро и удобно создавать мнемонические пароли. В данной работе подробно рассматривается ряд трудностей, с которыми сталкиваются пользователи и администраторы систем авторизации, в которых применяются пароли. Также анализируются современные подходы, направленные на облегчение подобных трудностей, представлен новый метод управления паролями, обращенный к мнемоническим формулам для запоминания паролей.

Мнемонический пароль (МП) – это пароль, который легко вспомнить, используя мнемонический прием – скажем, создание пароля с использованием первых букв высказывания, которое легко запомнить, стихотворения или текста песни. Пароли, составленные из фраз по своей сложности схожи с паролями, составленными из случайных символов. МП имеют тот же недостаток, что и обычные пароли, а именно, что пользователи могут повторно использовать один и тот же пароль в разных системах авторизации. Кроме того, такие пароли часто создаются с использованием хорошо известных отрывков текста из знаменитых литературных произведений или текстов песен. Были разработаны словари для подбора паролей, содержащие большое кол-во таких мнемонических вариантов.

Мнемонические пароли повышенного уровня безопасности (МППУБ) – это пароли, образованные от простых слов, которые пользователь сможет легко запомнить, однако в этих паролях используются мнемонические замены, чтобы в итоге пароль получился более сложным.

Проблема, характерная исключительно для МППУБ, состоит в том, что не все пароли могут быть преобразованы с помощью этого метода, что ограничивает либо выбор доступных слов, либо качество сложности пароля. Злоумышленниками были разработаны различные словари для подбора паролей, основанные на преобразованиях.

Фразовые пароли являются наиболее приемлемым вариантом МП. Их легче запомнить, и они гораздо длиннее, что значительно повышает устойчивость пароля к атакам прямого подбора. Они более сложны потому, что в них используется верхний и нижний регистры, пробелы и специальные символы, например, знаки пунктуации и цифры.

Мнемоническая формула для запоминания паролей, или МФП – это мнемоническая техника, подразумевающая использование заранее заданной, легко вызываемой в памяти формулы для оперативного создания паролей, основанных на знании различной контекстной информации, доступной пользователю. При использовании хорошо продуманной МФП, получившийся пароль должен иметь следующие характеристики:

- кажущаяся случайной последовательность символов.
- сложность и длина пароля, достаточные для обеспечения устойчивости к взлому.
- легкость восстановления в памяти пользователем, который знает формулу и целевую систему авторизации.
- уникальность для каждого пользователя, класса доступа и системы авторизации.

Для данной работы будет использоваться следующий синтаксис формул:

- <X>: элемент, который полностью заменяется каким-либо известным объектом, обозначенным X.

- | : при применении в элементе, заключенном в угловые скобки, обозначает выбор значения по схеме ИЛИ.

- все другие символы являются константными.

Простая МФП содержит два элемента: пользователя и целевую систему, которая идентифицируется либо именем хоста, либо наиболее значимым октетом IP-адреса.

<user>!<hostname|lastoctet>

С помощью вышеприведенной МФП можно получить такой пароль, как:

- "intropy!intropy" для пользователя intropy в системе intropy.net

С помощью этой простой МФП-схемы получается достаточно длинный и легко запоминающийся пароль, содержащий специальный символ. Однако по этой схеме нельзя создавать действительно сложные пароли.

Рассмотрим усложненные МФП. Внеся некоторые изменения в рассмотренную выше простую МФП, можно значительно повысить сложность пароля. При наличии информации об авторизуемом пользователе и системе авторизации, можно использовать следующую МФП:

<u>!<h|n>.<d,d,...|n,n,...>

МФП содержит три элемента: <u> представляет первую букву имени пользователя, <h|n> представляет первую букву имени хоста или первую цифру первого октета адреса и <d,d,...|n,n,...> представляет первые буквы остальных компонентов имени домена или первые номера остальных октетов адреса, соединенные вместе. Эта МФП также содержит еще один специальный символ помимо восклицательного знака – точка между вторым и третьим элементами.

Используя рассмотренную выше МФП, можно получить такой пароль, как:

- "i!i.n" для пользователя intropy в системе intropy.net

Измененная МФП содержит два спец символа, благодаря чему ее можно отнести к паролям повышенной сложности, однако пароли все еще могут получиться разной длины, и могут не подойти той или иной системы авторизации, в которой реализована политика ограничения количества символов в пароле. Кроме того, рассмотренная МФП имеет повышенный уровень сложности, из-за чего она может представлять сложности для запоминания.

По причине того, что сложность МФП значительно возрастает при попытках построения формул, соответствующих первым трем условиям, рассмотренным выше, к МФП можно применить второй уровень мнемонических свойств. МФП по определению является мнемонической техникой, поскольку она обладает свойством, позволяющим пользователю восстанавливать в памяти пароль для каждой отдельной системы, если он помнит только МФП и обладает знанием информационного контекста в отношении себя и системы. Для запоминания самой МФП могут быть применены дополнительные мнемотехники. Этот дополнительный мнемонический уровень может применяться пользователем помимо собственно МФП.

Например, при наличии информации об авторизуемом пользователе и системе авторизации можно использовать адекватно сложную, длинную и легкую для запоминания МФП следующего вида:

<u>@<h|n>.<d|n>;

Данная МФП содержит три элемента: <u> представляет первую букву имени пользователя, <h|n> представляет первую букву имени хоста или первую цифру первого октета адреса, и <d|n> представляет последнюю букву суффикса имени домена или последнюю цифру последнего октета адреса. Эта видоизмененная МФП также содержит третий специальный символ в добавление к восклицательному знаку и точке: точку с запятой после последнего элемента.

С помощью приведенной выше МФП можно получить следующий пароль:

- "i@i.t;" для пользователя intropy в системе intropy.net

В отличие от рассмотренных ранее МФП, в вышеприведенной формуле использована вторичная мнемотехника, которая легче запоминается пользователем, поскольку формула читается естественным образом. Эту МФП можно запомнить как «пользователь–собачка–хост–точка-домен», что напоминает структурный формат адреса электронной почты.

Элементы повышенной сложности. Можно составить МФП более высокого уровня, используя усложненные элементы, которые повторяются, изменяются, чередуются или увеличиваются на заданное значение, в отличие от простых элементов, заменяемых некими статистическими значениями (например, именем пользователя или частью имени хоста). Однако стоит отметить, что чрезмерное использование элементов этого типа может привести к тому, что МФП не будет запоминаться пользователем, поскольку она станет слишком сложной для запоминания.

С помощью МФП можно создавать более длинные пароли, повторяя простые элементы. Н-р, такой элемент, как первая буква имени хоста, может быть использован дважды:

<u>@<h|n><h|n>.<d>;

Совсем необязательно, чтобы такие повторяющиеся элементы шли один за другим, т.е. они могут быть использованы в любой части МФП.

С помощью МФП можно создавать пароли повышенной сложности, если включить в нее переменные элементы. Например, создатель МФП может поставить "p:" или "b:" перед началом какого-либо элемента, чтобы указать, что система является персональной (personal) или бизнес-системой (business).

<p|b>:<u>@<h|n>.<d|n>;

Чтобы лучше проиллюстрировать данный пример, рассмотрим ситуацию, когда пользователь занимается системным администрированием большого количества объектов. В этом случае переменный элемент может обозначать администрируемый объект:

<x>:<u>@<hi|n>.<d|n>;

<x> может быть заменено на «p» в случае с персональной системой, «E» в случае, если система находится в домене управления Exxon-Mobil или «A», если система управляется ассоциацией Austin Hackers Association. Использование переменного элемента помогает предотвратить сходство паролей. Можно использовать подстановку символов «0:» или «1:» вначале формулы, чтобы разделять доступ администратора от доступа пользователя без привилегий.

Таким образом, включение дополнительного переменного элемента в МФП приведет к тому, что пароль станет более сложным и будет отражать класс доступа:

<0|1>:<u>@<hi|n>.<d|n>;

Переменные элементы не обязательно должны стоять в начале формулы, как в приведенных выше примерах, их можно поместить в любую часть МФП.

На базе приведенных выше мнемонических формул для запоминания паролей была написана программа в среде Borland Delphi7, позволяющая генерировать пароли на основе имени пользователя и названия системы авторизации. Алгоритм работы программы приведен на рисунке 1.

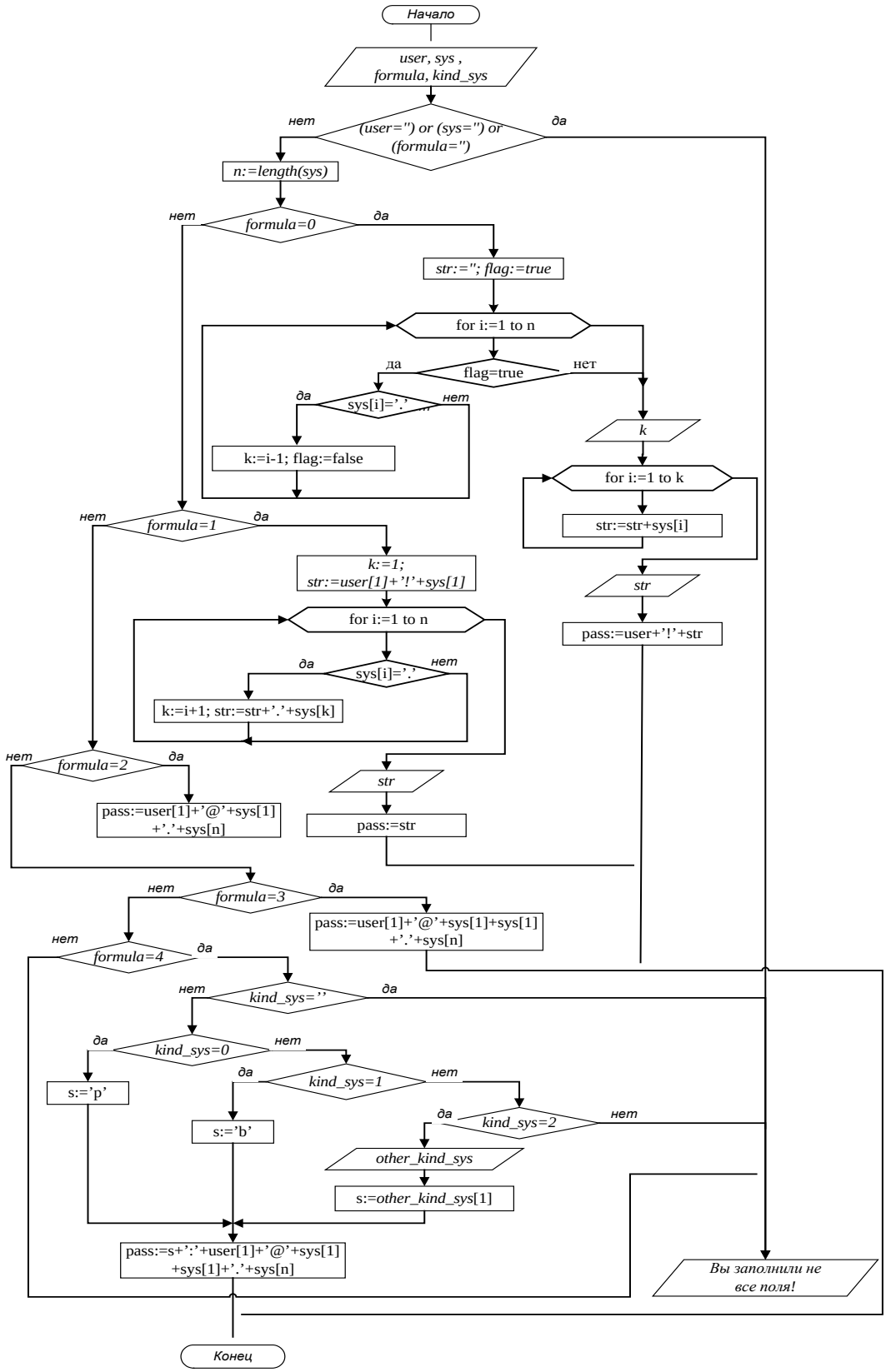


Рисунок 2 – Алгоритм работы программы

Интерфейс программы и пример ее работы представлен на рисунке 2.

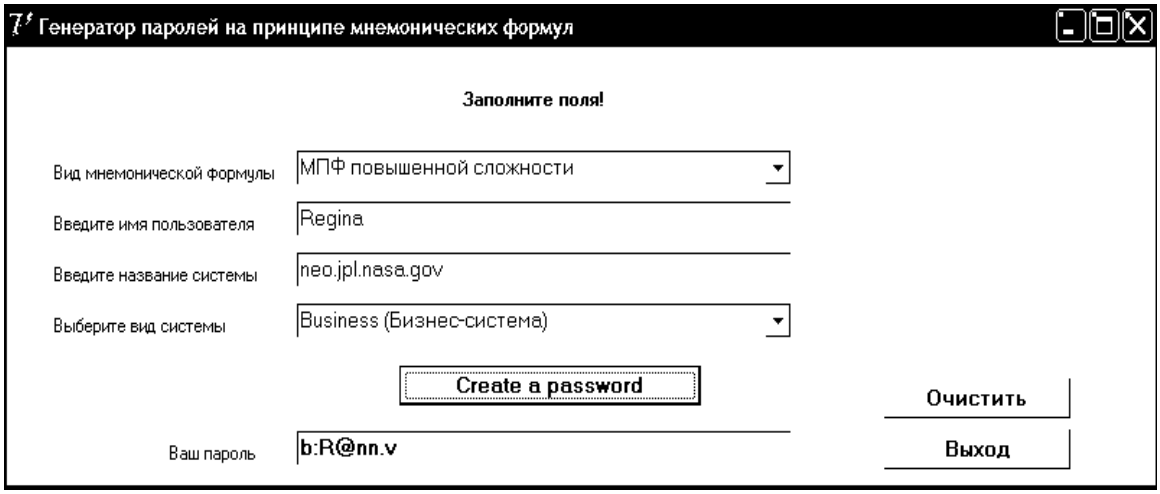


Рисунок 2 – Внешний вид программы с примером работы

Таким образом, МФП эффективно помогают избегать многих небезопасных ситуаций, связанных с выбором сложных паролей и их использованием. Однако стоит очень тщательно подходить к выбору степени сложности формул и их мнемонических характеристик, чтобы в итоге МФП получались достаточно защищенными, одновременно сохраняя легкость при воспроизведении в памяти. Если формулы становятся слишком сложными для запоминания, то проблемы, от которых пытались избавить пользователей с помощью МФП, могут возникнуть вновь.

Авторский указатель
The authors

1. Chrisina Draganova
2. Erdenebat Chuluun
3. Hamid Jahankhani
4. Imran Askerniya
5. Orhan Gemikonakli
6. Yoney Kirsal
7. Адамов Александр Семенович
8. Азизян Нина Ашотовна
9. Алексеев И.С.
10. Ануфриев Андрей Владимирович
11. Атапин А.В.
12. Базенков Д.Е.
13. Баринов Андрей
14. Босова Мария
15. Бочарникова Марина Владимировна
16. Бухаров Иван Владимирович
17. Вальгер Светлана
18. Гимазетдинов Марат Амирханович
19. Голованов Сергей Юрьевич
20. Гончаров Николай Олегович
21. Данилов В.О.
22. Дремлюга Роман Игоревич
23. Егоров Григорий Владимирович
24. Ермакова Лиана Магдановна
25. Ершов Дмитрий
26. Заводсков Андрей
27. Зорина Иннэса Викторовна
28. Ишемгулов Руслан
29. Калинин Антон
30. Киктенко Виталий Анатольевич
31. Кириченко Сергей
32. Князев Артём
33. Кожанов Евгений Александрович
34. Колосов Алексей Павлович
35. Копыстко Алексей Леонидович
36. Коромысов Сергей Юрьевич
37. Космачев Александр Валерьевич
38. Косолапова Елена Николаевна

1. Adamov Alexander
2. Alekseev I.S.
3. Anufrief Andrey
4. Atapin A.V.
5. Azizyan Nina
6. Barinov Andrey
7. Bazenkov D.E.
8. Bocharnikova Marina
9. Bosova Mariya
10. Bukharov Ivan
11. Chrisina Draganova
12. Chuvilo Oleg
13. Danilov V.
14. Dremluga Roman
15. Egorov Grigory
16. Erdenebat Chuluun
17. Ermakova Liana
18. Ershova Dmitry
19. Fathinurov Airat
20. Fayzullin R.
21. Gimazetdinov Marat
22. Golovanov Sergey
23. Goncharov Nikolay
24. Hamid Jahankhani
25. Imran Askerniya
26. Ishemgulov Ruslan
27. Kalinin Anton
28. Khalitova Kristina
29. Kiktenko Vitaliy
30. Kirichenko Sergey
31. Knyazev Artem
32. Kolosov Akexey
33. Kopytsko Alexey
34. Koromysov Sergey
35. Kosmachev Alexander
36. Kosolapova Elena
37. Kozhanov Eugene
38. Kraynov N.

39.	Крайнов Н.А.	39. Kukalo Ivan
40.	Кукало Иван	40. Kurnavina Taisiya
41.	Курнавина Таисия Сергеевна	41. Loginov Vladimir
42.	Логинов Владимир	42. Malyshev V.
43.	Малышев В.В.	43. Novoselov Nikolay
44.	Новоселов Николай Александрович	44. Olevskaya Ludmila
45.	Олевская Людмила Николаевна	45. Orhan Gemikonakli
46.	Осокин Д.В.	46. Osokin D.
47.	Парамонова Светлана Леонидовна	47. Paramonova Svetlana
48.	Печкуров Александр Владимирович	48. Pechkurov Alexander
49.	Приходько Максим Александрович	49. Prihodko Maxim
50.	Пустобаева Дарья	50. Pustobaeva Darya
51.	Рашевский Роман	51. Rashevsky Roman
52.	Речицкий Александр Сергеевич	52. Rechitsky Alexander
53.	Рой Константин Сергеевич	53. Roy Konstantin
54.	Рыжков Евгений Александрович	54. Ryzhkov Eugene
55.	Саварцов Алексей Васильевич	55. Saprykin Alexander
56.	Савельева Александра	56. Savartsov Alexey
57.	Сапрыкин Александр Сергеевич	57. Savelieva Alexandra
58.	Семенихина Варвара Сергеевна	58. Semenikhina Varvara
59.	Семенова Наталья Андреевна	59. Semenova Natalya
60.	Сергеева А.М.	60. Sergeeva A.M.
61.	Сергеева Елена	61. Sergeeva Elena
62.	Сидоров Михаил Владимирович	62. Shabanov Artem
63.	Смирнов Михаил	63. Shaimardanov Dmitry
64.	Снегурский Александр Владимирович	64. Shakirova Regina
65.	Сорокин Никита	65. Shalimov Mikhail
66.	Степина Алина Николаевна	66. Shkeda Artem
67.	Стуров А.С.	67. Sidorov Mikhail
68.	Тухтаманов Д.В.	68. Smirnov Mikhail
69.	Уртемеева М.А.	69. Snegursky Alexander
70.	Файзуллин Р.В.	70. Sorokin Nikita
71.	Фатхинуров Айрат	71. Stepina Alina
72.	Халитова Кристина Ибрагимовна	72. Sturov A.
73.	Чувило Олег	73. Tukhtamanov D.
74.	Шабанов Артем Владимирович	74. Urtemeeva M.
75.	Шаймарданов Дмитрий Ильфарович	75. Valger Svetlana
76.	Шакирова Регина	76. Yoney Kirsal
77.	Шалимов Михаил Александрович	77. Zavodskov Andrey
78.	Шкеда Артем	78. Zorina Inessa