ISSN 2225-5435

Вестник УрФО

БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

№ 4(14) / 2014

УЧРЕДИТЕЛЬ

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГЛАВНЫЙ РЕДАКТОР

ШЕСТАКОВ А. Л.,
д. т. н., проф., ректор ЮУрГУ

ОТВЕТСТВЕННЫЙ РЕДАКТОР

РАДИОНОВ А. А.,
д. т. н., проф., проректор ЮУрГУ

ВЫПУСКАЮЩИЙ РЕДАКТОР

СОГРИН Е. К.

ВЁРСТКА

ПЕЧЁНКИН В. А.

КОРРЕКТОР

БЫТОВ А. М.

Подписной индекс 73852 в каталоге «Почта России»

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Свидетельство **ПИ № ФС77-44941** от 05.05.2011

Издатель: ООО «Южно-Уральский юридический вестник»

Адрес редакции: Россия, 454080, г. Челябинск, пр. Ленина, д. 76

Тел./факс: (351) 267-90-65, 267-97-01

Электронная версия журнала в Интернете: **www.info-secur.ru, e-mail: urvest@mail.ru**

ПРЕДСЕДАТЕЛЬ РЕДАКЦИОННОГО СОВЕТА

БОЛГАРСКИЙ А. И., руководитель Управления ФСТЭК России по УрФО

РЕДАКЦИОННЫЙ СОВЕТ:

АСТАХОВА Л. В.,
зам. декана приборостроительного факультета ЮУрГУ, д. п. н., профессор кафедры безопасности информационных систем;

ГАЙДАМАКИН Н. А.,
д. т. н., проф., начальник Института повышения квалификации сотрудников ФСБ России;

ЗАХАРОВ А. А.,
д. т. н., проф., зав. каф. информационной безопасности ТюмГУ;

ЗЫРЯНОВА Т. Ю.,
к. т. н., доцент, руководитель цикла «Защита информации» кафедры ИТиЗИ УрГУПС;

КАРМАНОВ Ю. Т.,
д. т. н., директор НИИ ЦС ЮУрГУ;

КУЗНЕЦОВ П. У.,
д. ю. н., проф., зав. каф. информационного права УрГЮА;

МЕЛИКОВ У. А.,
к. ю. н., нач. отдела гражданского, семейного и предпринимательского законодательства Национального центра законодательства при Президенте Республики Таджикистан;

МЕЛЬНИКОВ А. В.,
д. т. н., проф., проректор ЧелГУ;

МИНБАЛЕЕВ А. В. (зам. отв. редактора),
зам. декана юридического факультета ЮУрГУ, д. ю. н., доцент, доцент кафедры конституционного и административного права;

СИДОРОВ А. И.,
д. т. н., проф., зав. каф. БЖД ЮУрГУ;

СКОРОБОГАТОВ А. А.,
заместитель начальника Управления ФСБ по Челябинской области;

СОКОЛОВ А. Н. (зам. отв. редактора),
к. т. н., доцент, зав. кафедрой безопасности информационных систем ЮУрГУ;

СОЛОДОВНИКОВ В. М.,
к. физ.-мат. наук, зав каф. БИиАС КГУ;

ТРЯСКИН Е. А.,
начальник специального управления ЮУрГУ.

В НОМЕРЕ

ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

КОБЯКОВ В. Ю., ЛУЧИНИН А. С.
Обнаружение ПЭМИ проводников и коннекторов при передаче по интерфейсу USB. 4

ЗУБОВ Я. М., ИЛЬИН И. И., МОСКВИН В. В.
Модель системы контроля и управления доступом на предприятии на базе Arduino 9

ЛУКЬЯНОВ Г. И., МИХАЙЛОВА У. В.
Эффективность применения СЗИ от утечки по акустическим каналам. 14

ШАБУРОВ А. С., РАШЕВСКИЙ Р. Б.
О практическом применении технологии vmware vshield app для обеспечения безопасности информационных систем персональных данных 19

ПОПОВ Е. Ф., ТЮКОВА А. А., ФУЧКО М. М., ЗАХАРОВ А. А.
Выявление нетипичных событий средствами статистического анализа 24

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

КОНДРАШИН Д. В., ГОРШЕНИН В. В.
Графическая аутентификация для Android устройств 28

МОИСЕЕВ А. М., МАМЫКИН А. В., МОСКВИН В. В.
Атака через USB. 32

ТОКАРЧУК Н. А., СЕРЕДКИНА Е. Д., ЗЮЛЯРКИНА Н. Д.
Протокол TCP как стеганографический контейнер. 36

ФОМИН И. П., МАТКИН И. А.
Технология аппаратной виртуализации в контексте компьютерной безопасности 40

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОРОКИНА С. В., ТИТОВ С. С.
Матроиды, двойственные к бинарным, и их схемы разделения секрета 44

СУРИНА А. А., ЗЮЛЯРКИНА Н. Д.
Рюкзачная криптосистема на основе прямого произведения диэдральных групп 48

ГОРЯИНОВ С. В., ИСАКОВА Г. С.
Связность второй окрестности в кореберно-регулярных графах Деза 53

ОРГАНИЗАЦИОННАЯ И ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

АСТАХОВА Л. В., ЕФРЕМОВ В. А., МИТЬКИН А. И.
Автоматизация многофакторной оценки кадровых уязвимостей информационной безопасности 57

ЛАПТЕВА Т. В., МИЩЕНКО Е. Ю., МАКАРОВА П. В.
Особенности составления трудовых договоров и соглашений о неразглашении информации, составляющей коммерческую тайну, на предприятиях, использующих DLP-системы 62

УЛЬЯНОВ Н. Л., АСТАХОВА Л. В.
Проблема кадровой безопасности в системе стандартов информационной безопасности Банка России 66

TECHNICAL MEANS AND METHODS OF INFORMATION PROTECTION

KOBYAKOV V. Y, LUCHININ A. S.
Detection of tempest conductors and connectors in the process of transmission through USB interface 4

ZUBOV Y. M., ILIIN I. I., MOSKVIN V. V.
Arduino based access monitoring and control systems 9

LUKYANOV G. I., MIKHAILOVA U. V.
The effectivenes of the implementation of information security system for prevetion of information leakage through acoustic links 14

SHABUROV A. S., RASHEVSKY R. B.
On practical implementation of vmware vshield app technology for ensuring security of personal data information systems 19

POPOV E., TYUKOVA A., FUCHKO M., ZAKHAROV A.
Identification of atypical events means of the statistical analysis..... 24

COMPUTER SECURITY

KONDRASHIN D. V., GORSHENIN V. V.
Graphic authentication for Android devices 28

MOISEEV A. M., MAMYKIN A. V., MOSKVIN V. V.
USB driven attac 32

TOKARCHUK N. A, SEREDKINA E. D., ZIULIARKINA N. D.
TCP protocol as a steganographic container 36

FOMIN I., MATKIN I.
Hardware virtualization technologies in the context of computer security..... 40

MATHEMATICAL METHODS IN INFORMATION SECURITY

SOROKINA S. V., TITOV S. S.
Matroids dual to binary ones and their secret separation schemes..... 44

SURINA A. A., ZIULIARKINA N. D.
Knapsack public key cryptosystem on the basis of direct product of dihedral groups 48

GORYAINOV V. S., ISAKOVA G. S.
Connection of the second neighbourhood in coadjoint regular Deza graphs 53

ORGANIZATIONAL AND LEGAL PROTECTION INFORMATION

ASTAKHOVA L. V., EFREMOV V. A. MITKIN A. I.
Automation of multifactorial estimation of personnel vulnerability of information security..... 57

LAPTEVA T. V., MISCHENKO E. Y., MAKAROVA P. V.
Features of employment contracts and non-disclosure agreements which comprise trade secrets at enterprises which use dlp systems 62

ULIANOV N. L., ASTAKHOVA L. V.
the problem of personnel security in the system of standards of information security of the bank of Russia 66

УДК 004. 056.5 + 004.35.031.4 + 004.5.056

Кобяков В. Ю., Лучинин А. С.

ОБНАРУЖЕНИЕ ПЭМИ ПРОВОДНИКОВ И КОННЕКТОРОВ ПРИ ПЕРЕДАЧЕ ПО ИНТЕРФЕЙСУ USB

В настоящее время огромное количество устройств обмениваются друг с другом по интерфейсу USB. Возможные утечки информации в литературе освещены недостаточно, чем и обоснован выбор темы для исследования. В статье кратко изложена структура интерфейса USB. Для проведения измерений выбрана проводная клавиатура Rapoo N2400 с низкоскоростным соединением USB. Экспериментальные исследования показали возможность перехвата информации за счет побочных электромагнитных излучений.

Ключевые слова: *информационная безопасность, побочные электромагнитные излучения, перехват информации, USB, клавиатура, защита информации.*

Kobyakov V. Y, Luchinin A. S.

DETECTION OF TEMPEST CONDUCTORS AND CONNECTORS IN THE PROCESS OF TRANSMISSION THROUGH USB INTERFACE

Currently a great number of devices are intercommunicating with each other through the USB interface. Data leakages are not properly highlighted which justifies the topic of the research. The article dwells on concise structure of the USB interface with the Rapoo N2400 keyboard with slow connection chosen for execution of measurements. The experiments have shown the possibility of information capturing by means of side electromagnetic radiation.

Keywords: *information security, side electromagnetic radiation, information capturing, USB, keyboard, information security.*

Выделение информативного сигнала из передаваемых данных было невозможно без изучения протокола USB, описанного в соответствующей спецификации [1]. Первоначально (в версиях 1.0 и 1.1) шина обеспечивала две скорости передачи информации: полная скорость FS (FullSpeed) — 12 Мбит/с и низкая скорость LS (LowSpeed) — 1,5 Мбит/с. В версии 2.0 и 3.0 определены ещё высокая скорость HS (HighSpeed) – 480 Мбит/с и супервысокая скорость SS (SuperSpeed) – 5 Гбит/с.

Все обмены информацией, далее транзакции, инициируются хостом. Транзакция состоит из двух-трех пакетов. При обмене данными используются пакеты четырех типов:

1) Маркерные пакеты – пакеты управления, передаются только хостом (рис. 1);
2) Пакеты данных – применяются для передачи полезной нагрузки, используются хостом и устройством (рис. 2);
3) Пакеты квитирования – подтверждение принятого пакета данных, используются хостом и устройством (рис. 3);
4) Пакеты начала кадра (SOF) – выдаются хостом с номинальной скоростью один каждую 1,00 мс±0.05 в полноскоростном соединении. Используется при передаче сообщений, размер которых больше максимальной полезной нагрузки пакета данных (рис. 4).

Практическое наблюдение сигнала производилось с помощью осциллографа, подключенного к дифференциальным парам. Экспериментально установлено, что информация передается младшим битом вперед в кодировке NRZI с добавлением нуля при шести подряд передаваемых единицах. Хост опрашивает устройство через каждые 8 мс пакетом со следующими данными:

[1 0 1 0 1 0 1 1] SYNC
[1 0 1 1]PID IN 10012
[0 0 0 1]Check PID 01102
[1 0 1 0 1 0 1] ADDR 00000012
[1 0 1 0] ENDP 00012
[0 0 1 1 0] CRC
[0 0] EOP

Поля SYNC и EOP не несут смысловой нагрузки, они необходимы для синхронизации и инициализации обмена данными. При передаче EOP (End of packet) обе дифференциальные пары на два такта переходят в нулевое состояние, это означает конец передачи пакета. Поле PID определяет тип пакета, поле Check – инверсионное представление поля PID, необходимо для контроля ошибок.ADDR – поле адреса функции (устройства), назначается хостом. На нулевой адрес должны откликаться все устройства. Поле ENDP – номер конечной точки функции, обеспечивает более гибкую адресацию. CRC – контрольная

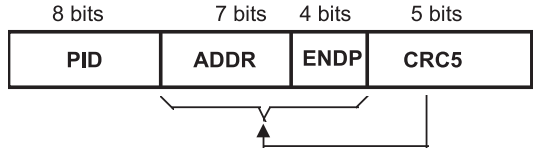


Рис. 1. Формат маркерного пакета

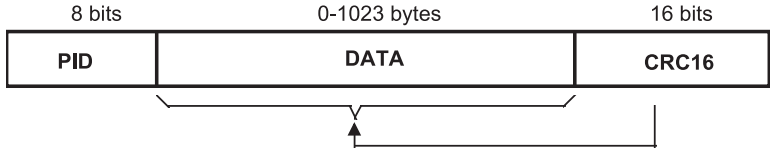


Рис. 2. Формат пакета данных

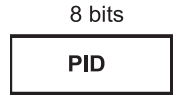


Рис. 3. Формат пакета квитирования

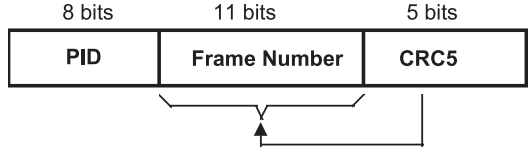


Рис. 4. Формат пакета начала кадра

сумма над полями ADDR и ENDP. В дальнейшем полями SYNC и EOP пренебрежём при описании пакетов, так как информации они не несут и присутствуют в пакетах любого типа.

Устройство отвечает через 8 битовых тактов ≈ 5,3 мс. Если у устройства нет ничего к передаче, то оно отправляет пакет квитирования об отсутствии нагрузки.

[0 0 1 1] PID NAK 10102 – устройство не может принимать данные или посылать данные.

[1 0 0 1] Check PID

Только в пакетах квитирования нет контрольной суммы. Контроль ошибок осуществляется полем Check.

Если у устройства есть что-то к передаче, то передается пакет данных. Передача информации о нажатии клавиши «a».

[1 0 1 0 1 0 1 1] SYNC.

[1 1 0 0] PID data1 – нечетный пакет данных

[1 0 0 0] Check PID

[0 1 0 1 0 1 0 1] DATA 0x00

[0 1 0 1 0 1 0 1] DATA 0x00

[0 1 1 0 1 0 1 0] DATA 0x04 код кнопки «a»

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 0 1 0 1 0 1 0] DATA 0x00

[1 1 1 1 1 1 0 0] CRC 0xCE

[1 0 1 0 0 0 0 1] CRC 0x78

Под поле данных в низкоскоростном соединении выделяется максимум 8 байт. Размер поля может быть меньше, но исследуемая клавиатура сконфигурирована следующим образом: первые 2 байта нулевые, следующий байт HID-кода клавиши [2], остальные 5 байт нулевые. Контрольная сумма вычисляется над полем данных. Информация о нажатии клавиши передается один раз. Продолжительность нажатия, регистр, раскладку, комбинации клавиш – всё вычисляет драйвер клавиатуры и определяет, что делать.

В случае если данные приняты без ошибок, то хост отправляет пакет квитирования о подтверждении приема.

[0 0 1 0] PID ACK 0010_2 – приемник принимает пакет данных, свободный от ошибок.

[0 1 1 1] Check

При одновременном нажатии коды клавиш будут передаваться последовательно во время опроса устройства. При отпускании одной из зажатых клавиш будут переданы HID коды клавиш, которые ещё зажаты в по-

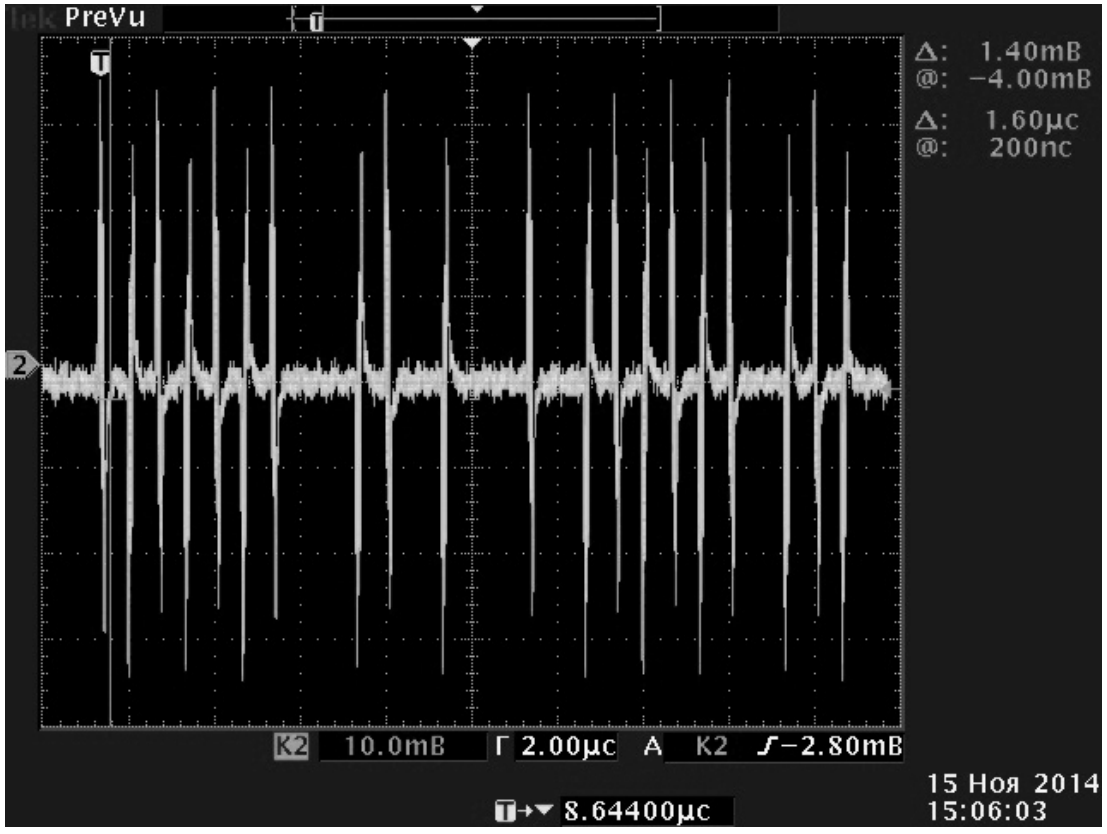


Рис. 5. Обнаруженный пакет данных, передаваемый по D+

рядке их нажатия. Максимальное число одновременно зажатых клавиш семь [3]. Нажатие восьмой клавиши будет проигнорировано. При отжатии последней клавиши передаются 8 нулевых байтов данных.

Для оценки возможности перехвата информации по каналу ПЭМИ, передаваемой по проводному низкоскоростному соединению, были проведены следующие эксперименты.

С помощью токосъемника ТИ2-3 и осциллографа Tektronix TDS 3054C делалась попытка пронаблюдать сигналы, циркулирующие по кабелю USB клавиатуры. Эксперимент не дал результата из-за недостаточной чувствительности осциллографа и хорошего качества кабеля (выполненного в виде витой пары).

Для повышения уровня сигнала была нарушена экранировка кабеля и токосъемник был подключен к одному из проводов сигнальной пары кабеля. В таком виде сигналы побочного излучения обнаруживаются успешно (рис. 5).

Уровень максимального импульсного скачка, образованного фронтом передаваемого импульсного сигнала, около 34 мВ. Уровень ниспадающего импульсного скачка 25–28 мВ. Данный разброс по амплитуде обусловлен разной длительностью переднего и заднего фронта информационных импульсов.

Есть две причины, по которым наблюдаемые импульсные скачки можно относить к побочным сигналам, излучаемым интерфейсом USB:

1. Длительность наблюдаемых возрастающих и ниспадающих импульсных скачков около 120–140 нс. Время нарастания/спадания импульсного сигнала в интерфейсе USB 110–140 нс.
2. Период повторения импульсных скачков около 650 нс – длительность импульса в интерфейсе 660 нс.

Для подавления побочного электромагнитного излучения в интерфейсе USB используется дифференциальная пара для передачи сигналов и экранирования кабеля. Подавление, обусловленное применением экранирования, было оценено экспериментально.

Экранированный кабель Belsis “Multimedia” Hi-Grade USB 2.0 High Speed Cable, со второго кабеля полностью сняты защитная оболочка и экранировка. Нагрузка 100 Ом, генератор N5181A (Agilent Technologies) излучал в линию синусоидальный сигнал амплитудой 1В. Прием вёлся с помощью анализатора спектра ESPI 3 (Rohde & Swartz). Зависимость мощности принятого сигнала от частоты изображена на рис. 6 и рис. 7.

Экранирование подавляет сигнал на 10–15 дБ. На частотах ниже 6 МГц уровень излучения меньше -115 дБм, для наблюдения излучения необходима более чувствительная аппаратура.

Экранированные кабели с применением витых пар позволили обнаружить излучение лишь на небольшом расстоянии. Амплитуды импульсных сигналов рис. 5, около 34 мВ лишь немного превышают порог чувствительности осциллографа. Дальность обнаружения можно увеличить, если применить более чувствительную аппаратуру.

Рассчитаем теоретически реализуемый порог чувствительности приемника, способного перехватить сигнал, излучаемый за счет побочного излучения кабеля и коннекторов USB интерфейса. Зададим параметры:

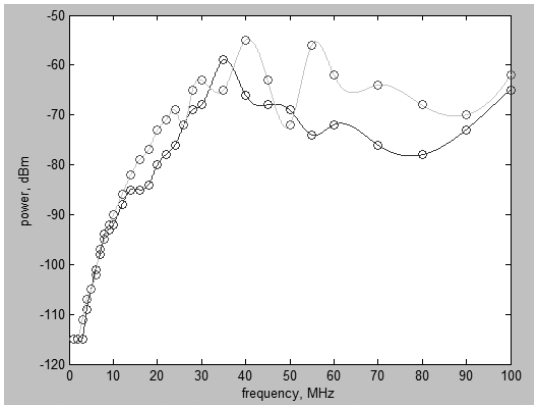


Рис. 6. Уровень ЭМИ при съеме информации токосъёмником ТИ2-3 в экранированном и неэкранированном кабеле

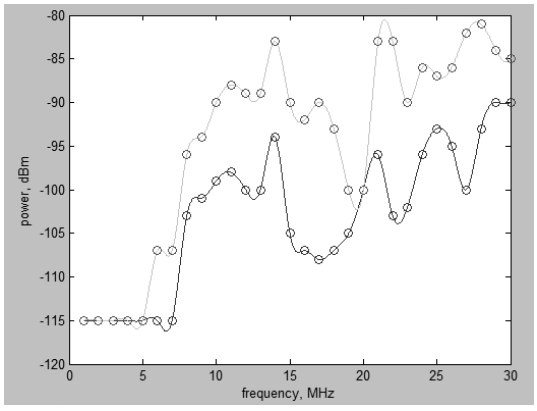


Рис. 7. Уровень ЭМИ в экранированном и неэкранированном кабеле USB на расстоянии 1 м, антенна АИР3-2

- R_a=50 Ом – выходное сопротивление антенны;
- F=10 дБ – коэффициент шума;
- K=10 дБ – требуемое отношение сигнал/шум на входе приемника;
- T=300 К – температура окружающей среды;
- $\tau_и$=120 нс – минимальная длительность ожидаемого импульсного скачка.

Минимальная мощность, необходимая для приема сигнала шумящим приемником (порог чувствительности):

$$P_{min} = F * K * k * T * \Delta f, \quad (1)$$

где $k = 1.38 * 10^{-23}$ Дж/К – постоянная Больцмана,

$$\Delta f = \frac{1}{\tau_и} = \frac{1}{120*10^{-9}} \approx 8.5 * 10^6 \text{Гц} \quad (2)$$

При условии согласования на входе приемника мощность собственных шумов и Э.Д.С. связаны соотношением

$$P_{min} = \frac{e_ш^2}{4*R_a}, \quad (3)$$

где, $e_ш$ – Э.Д.С. шумов, приведенных ко входу приемника.

Минимальное входное напряжение связанно с ЭДС шума:

$$U_{вх} = \frac{\sqrt{e_ш^2}}{2}. \quad (4)$$

Подставив числовые значения, найдем $e_ш^2$:

$$e_ш^2 = 4 * R_a * F * K * k * T * \Delta f \approx \approx 7.04 * 10^{-10} \text{ В}^2 \quad (5)$$

Подставив полученный результат в формулу 4, получим:

$$U_{вх} = \frac{\sqrt{e_ш^2}}{2} = \frac{\sqrt{7.04 * 10^{-10}}}{2} \approx \approx \frac{26.54 * 10^{-6}}{2} \approx 13.3 \text{ мкВ}$$

Полученной чувствительности хватит для того, чтобы перехватить передаваемую информацию по интерфейсу USB. Заданные исходные параметры приемника являются реальными для современной аппаратуры.

Полученные результаты позволяют уточнить требования к качеству экранировки кабеля и других элементов клавиатуры для исключения возможности перехвата информации в реальных устройствах [4].

Примечания

1. Спецификация по USB1.1 на русском языке // Сайт «Паяльник». URL: http://cxem.net/doc/comp/usb11.rar (дата обращения: 08.12.14)

2. USB Hid Keyboard Scan Codes // STIK elektro. URL: http://www.mindrunway.ru/IgorPlHex/USBKeyScan.pdf (дата обращения: 08.12.14)

3. Исупов. Л. Радиоснифер клавиатуры. Свежий подход к перехвату набираемого на клавиатуре текста // Хакер. 2006. № 08. с. 20 – 23. URL: http://xakep.ru/wp-content/uploads/2014/08/xa_08_2006_low.pdf?2bdec0 (дата обращения: 08.12.14)

4. Martin Vuagnoux, Sylvain Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards // EPFL, Lausanne, Switzerland. URL: http://www.usenix.org-events-sec09-tech-f ull_papers-vuagnoux.pdf (дата обращения: 08.12.14)

Кобяков Василий Юрьвич, студент, Уральский федеральный университет, (г. Екатеринбург). E-mail: kobyakov93@mail.ru.

Лучинин Александр Сергеевич, к. т. н., доцент, Уральский федеральный университет, (г. Екатеринбург).

Vasily Yurievich Kobyakov, student of Ural Federal University. E-mail: kobyakov93@mail.ru.

Aleksandr Sergeevich Luchinin, Cand. Sc. Engineering, Associate Professor of Ural Federal University.

УДК 681.51 + 004.056.5 + 004.382.7

Зубов Я. М., Ильин И. И., Москвин В. В.

МОДЕЛЬ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРЕДПРИЯТИИ НА БАЗЕ ARDUINO

Системы контроля и управления доступом (СКУД) – это эффективная контрольно-пропускная система, которая позволяет управлять безопасностью объекта и осуществлять контроль доступа. Целью работы является демонстрация возможности реализации модели СКУД на базе программно совместимого аналога Arduino, которая будет существенно более выгодной в коммерческом плане по сравнению с существующими промышленными аналогами.

Ключевые слова: *безопасность, инженерно-техническая защита информации, защита информации, предохранительные устройства и мероприятия, контроль территории, носимые устройства авторизации, RFID, токен, Arduino.*

Zubov Y. M., Iliin I. I., Moskvin V. V.

ARDUINO BASED ACCESS MONITORING AND CONTROL SYSTEMS

Access monitoring and control systems (ACS) are the effective control systems which enable to administrate the object's security and implement the access control. The aim of the work is to demonstrate the range of possibilities of the implementation of Arduino based ACS which is to be more profitable in terms of commercial success compared to the current industrial alternatives.

Keywords: *security, engineer and technical information security, information security, protective equipment and measures, territory control, portable authentication devices, RFID, token, Arduino.*

Вступление

Одним из направлений обеспечения информационной безопасности на предприятии или в организации является инженерно-техническая защита, в рамках которой используются системы контроля и управления доступом.

Перед проектирующим систему информационной защиты организации специалистом нередко ставится задача обеспечения для сотрудников защиты на некоторой территории, внутри которой возможен свободный обмен. В качестве элемента такой системы можно предложить устройства, разрабатываемые на базе плат Arduino.

RFID

Используемая для реализации системы технология Radio Frequency IDentification (радиочастотная идентификация – РЧИ) — это

метод удаленного хранения и получения информации путем передачи радиосигналов с помощью устройств, называемых RFID-метками [1, 2]. Данная технология является одной из тех, элементами которых являются носимые пользователями систем, построенных на этих технологиях, специальные высокотехнологичные идентификаторы – токены (англ. token).

Использованный нами архитектурный тип метки – «пассивная». Пассивные RFID-метки не имеют встроенного источника энергии. Чип, обеспечивающий работу метки, питается от индуцируемого в антенне сигналом запроса электрического тока.

Ниже приведён пример распределения характеристик РЧИ-меток по рабочим частотным диапазонам (Табл. 2).

Таблица 1. Пассивные RFID-метки

Функциональные возможности	Только прочтение/прочтение-запись
Частота	125KHz / 13.56MHz / 915 MHz / 2.45GHz прочтение-запись
Расстояние прочтения	До 6 м + (с установленной антенной)
Размеры	Разные, ~ 0,8 мм в диаметре
Вес	6–54 г
Память	До 16 Kbit
Срок эксплуатации	10 лет
Температурный режим	- 40 до + 70 по Цельсию

Таблица 2. Классификация RFID по диапазонам частот

Характеристика	**Низкие частоты (НЧ, LF) – 125–134 КГц**	**Высокие частоты (ВЧ, HF) – 13,56 МГц**	**Ультравысокие частоты (УВЧ, UHF) – 860–960 МГц**	**Микроволны (SHF) – 2,4 ГГц**
Максимальное расстояние считывания	от 3 до 70 см	от 3 до 100 см	от 10 см до 4 м	2–10 м
Скорость передачи данных радиометка-считыватель	около 9600 бит/с	до 64 кбит/с	до 128 кбит/с	до 128 кбит/с
Наличие антиколлизии	Есть, но не у всех микросхем	Есть	Есть	Есть
Объем памяти радиометки	32–1024 байта	8–16384 байт	64–1024 бит (ISO), 64 или 96 бит (EPC)	от 64 бит до 32 кбит

Сферы применения RFID

СКУД на основе РЧИ устанавливаются повсюду, где целесообразно оные устанавливать. Это территории, доступ на которые должен предоставляться строго ограниченному кругу лиц. Кроме того, RFID применяются при изготовлении европейских и американских паспортов, различных кредитных карт; в животноводстве, системах охраны автомобилей.

Пользовательский интерфейс системы

Далее описывается сценарий взаимодействия с системой (рис. 1). Сотрудник предприятия или предполагаемый злоумышленник, проходя на контролируемую территорию, предоставляет свою RFID-метку. Модуль системы, отвечающий за получение информации с RFID-метки, должен выполнить считывание и проанализировать полученные данные, используя базу данных системы, содержащую соответствия между записями на метках и сотрудниками, которым метки принадлежат. Если предоставленная метка зарегистрирована в базе, то система должна пропустить работника. В ином случае – опционально просигнализировать о неудаче авторизации.

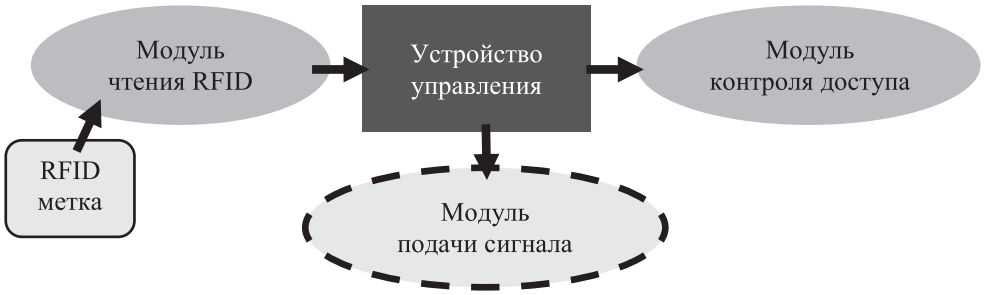


Рис. 1. Модульная диаграмма. Стрелками указаны пути обмена информацией между компонентами

Разработка модели

Устройством управления будет выступать плата Arduino с записанной в её контроллер программой. Чтением информации с RFID-метки займётся специальная схема RFID-RC522[7], а сигналы о работе модели системы будут подаваться при помощи светодиода и элементарного аудиоустройства (buzzer) [4]. Работу модуля контроля доступа будет исполнять сервомотор SG90 [5].

Arduino

Выбранная в качестве базы для разработки системы платформа Arduino обеспечена разработанным для использования именно с ней ПО [3].

Бесплатно распространяющаяся интегрированная среда разработки Arduino IDE 1.0.6 решает задачу удобных написания, компилирования и загрузки управляющего кода.

Для работы с модулем RFID-RC522 была задействована библиотека <MFRC522.h> [8]. Использование методов из объявленного в ней класса MFRC522 – это возможность считывания информации с RFID-меток. В данном случае мы определяем «своих» при помощи только UID–метки. Это четыре байта, при совпадении которых с записанными будет подаваться сигнал об успешной авторизации и производиться действия, символизирующие предоставление доступа.

Для управления сервомотором понадобилась поставляемая вместе с IDE <Servo.h>, содержащая, кроме прочих, описание класса Servo. Данный класс «подключается» к указываемому по номеру порту и позволяет при помощи предоставляемого им методов attach (int port) и write (int val) выбирать порт для работы с сервомотором и задавать положение ротора сервомотора соответственно.

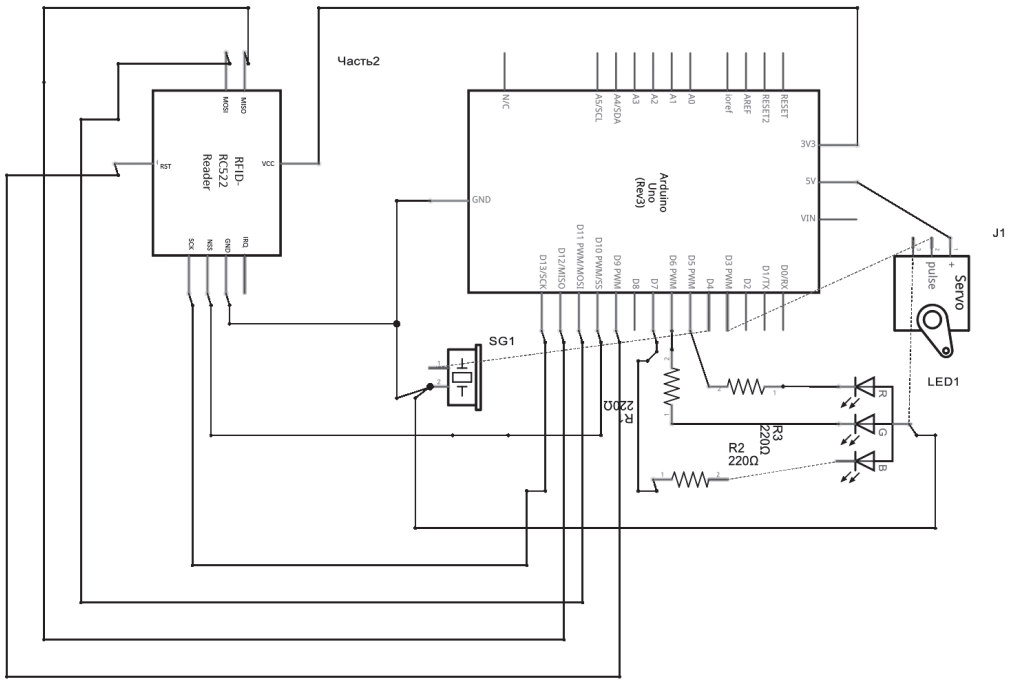


Рис. 2. Принципиальная схема

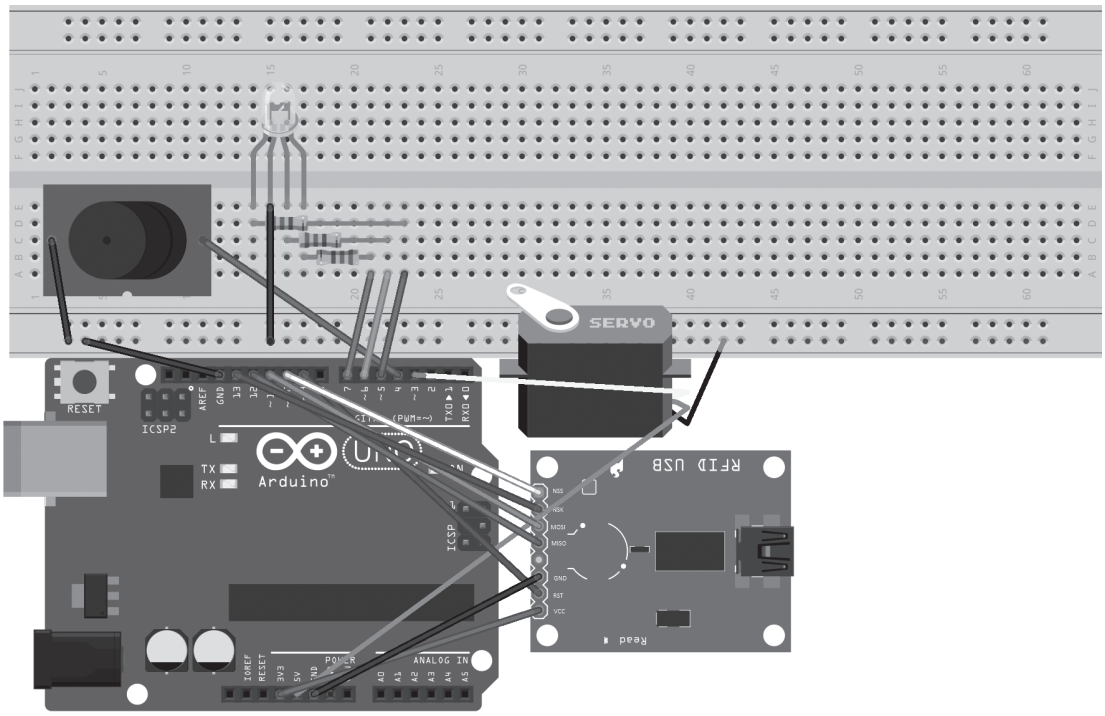


Рис. 3. Внешний вид результата сборки

Подведение итогов

По окончании процесса проектирования, сборки и тестирования можно подвести итог – подсчитать наши немодельные затраты и сравнить их с уктами, предлагаемыми на рынке. Под немодельными затратами понимаем реально обеспечивающие должную работу системы модули. В данном случае используемые нами компоненты не будут заменены, но система требует модуля контроля доступа. Примером может послужить магнитный замок.

Приведённые в таблице цены получены в процессе анализа рынка данных компонентов на момент выполнения работы и признаны авторами «умеренными».

Таблица 3. Список компонентов и цены

Обозначение	Кол-во	Тип	Свойства	Стоимость
LED1	1	RGB LED	4-контактный RGB светодиод с общим анодом	10–20 р. / шт.
R1, R2, R3	3	220Ωрезистор	Допуск ± 5% сопротивление 220Ω	30 р. / 50 шт.
SG1	1	Buzzer 12mm	Зуммер 12 мм	5 р. / шт.
Часть 1	1	Arduino Uno (Rev3)	Микроконтроллер платы на основе ATmega328	300–400 р. / шт.
Часть 2	1	RFID-RC522	Модуль чтения-записи RFID карт на частоте 13,56 Мгц	250–350 р. / шт.
				Итого: ~700 р.

Таблица 4. Коммерческие предложения

	RFID Proximity Entry Electric Door Lock	2000–4000 р.
	Hotel Rfid Lock Door	2500–5000 р.

Видеопрезентация: http://www.youtube.com/watch?v=miXkDGL3Dvc
Программный код: https://drive.google.com/folderview?id=0B-tk-VyBe4iWbnRfWXFvOXBPazg&usp=sharing

Вывод

Результатом нашей работы стала модель СКУД, не претендующая на статус прототипа готового коммерческого продукта. Данный программно-аппаратный комплекс не завершен, что делает затруднительным оценку результирующей стоимости нашего устройства. Но уже на основе имеющихся у нас данных можно сказать, что материальные затраты на техническую сторону реализации данной системы (предполагается написание комплекса программных решений, предоставляющих управление ею с помощью ПК) незначительные по сравнению с существующими промышленными аналогами. А труд, приложение которого необходимо для окончательной реализации всей СКУД, является студенческим, то есть бесплатным.

Примечания

1. Технология 13,56 МГц // Компания «ТерраЛинк». URL: http://idcards.ru/materials/technology/skud/hif.php (дата обращения: 08.12.14)

2. Принцип работы RFID // Группа компаний «Стиль Групп». URL: http://www.ms-keys.narod.ru/princip_proxi.htm (дата обращения: 08.12.14)

3. Arduino code tutorials and examples // Официальный сайт «Arduino». URL: http://arduino.cc/en/Tutorial/HomePage (дата обращения: 08.12.14)

4. Buzzer Arduino Example Code // [Персональный сайт Роба Фалуди]. URL: http://www.faludi.com/2007/04/23/buzzer-arduino-example-code/ (дата обращения: 08.12.14)

5. SG 90 9g Micro Servo // «Spark n' Go». URL: http://datasheet.sparkgo.com.br/SG90Servo.pdf (дата обращения: 08.12.14)

6. Уроки Fritzing // Блог «Амперка». URL: http://blog.amperka.ru/уроки-fritzing (дата обращения: 08.12.14)

7. Mifare RC522 RFID Модуль // Форум «Arduino.ru». URL: http://arduino.ru/forum/apparatnye-voprosy/mifare-rc522-rfid-modul (дата обращения: 08.12.14)

8. Arduino library for MFRC522 // Интернет-портал «GitHUB». URL: https://github.com/miguelbalboa/rfid (дата обращения: 08.12.14)

Зубов Яков Михайлович, студент, Курганский государственный университет. E-mail: wind069@gmail.com.

Ильин Иван Игоревич, студент, Курганский государственный университет. E-mail: illy1vann@gmail.com.

Москвин Владимир Викторович, ст. преподаватель КГУ.

Yakov Mikhailovich Zubov, student of Kurgan State University. E-mail: wind069@gmail.com

Ivan Igorevich Iliin, student of Kurgan State University. E-mail: illy1vann@gmail.com

Vladimir Viktorovich Moskvin, senior lecturer of Kurgan State University.

УДК 004.056 + 004.322 : 534 + 621.394/.396.019.3

Лукьянов Г. И., Михайлова У. В.

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ СЗИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ

В данной статье рассматривается анализ активного метода защиты информации на базе СЗИ «Соната-АВ». На основе проведенного анализа рассмотрены недостатки данной системы и предложены доработки с целью полной изоляции акустического канала.

Ключевые слова: *информация, безопасность, акустика, вибрация, защита информации, акустический канал.*

Lukyanov G. I., Mikhailova U. V.

THE EFFECTIVENES OF THE IMPLEMENTATION OF INFORMATION SECURITY SYSTEM FOR PREVETION OF INFORMATION LEAKAGE THROUGH ACOUSTIC LINKS

The article dwells on the analysis of the active method of information security based on information security system 'Sonata-AB'. On the basis of the analysis the authors consider disadvantages of the abovementioned system and propose improvements for the purpose of complete isolation of the acoustic link.

Keywords: *information, security, acoustics, vibration, information security, acoustic link.*

В общем комплексе мероприятий по обеспечению информационной безопасности одной из важнейших задач является защита акустической (речевой) информации. Оценка защищенности помещений от утечки по акустическому каналу состоит в определении коэффициентов звукоизоляции ограждающих конструкций в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц в выбранных контрольных точках [1].

Реализация защиты акустической информации осуществляется с помощью пассивных и активных методов. В случае если пассивные средства защиты помещений не обеспечивают требуемых норм по звукоизоляции, используются активные меры защиты, заключающиеся в создании маскирующих акустических и вибрационных помех с использованием виброакустической маскировки информационных сигналов. Акустическая маскировка эффективно используется для защиты речевой информации от утечки по всем каналам, а виброакустическая – по виброакустическому и оптико-электронному (акустооптическому) каналам. Обычно активная маскировка осуществляется посредством аддитивного зашумления источника электромагнитного сигнала, т. е. наложения на несущий полезную информацию сигнал маскирующего шумового сигнала определенной структуры.

В настоящее время выпускается большое количество различных систем активной виброакустической маскировки, успешно ис-

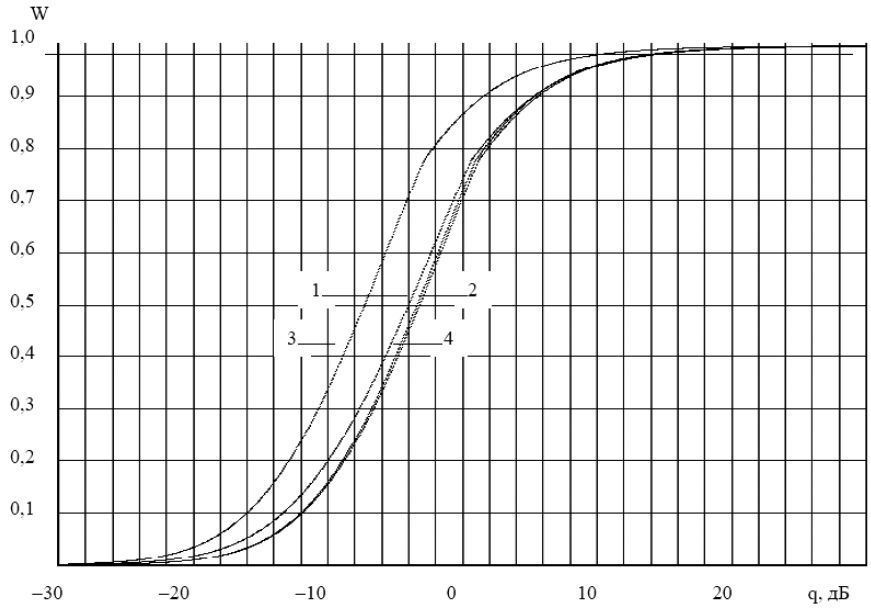


Рис. 1. Зависимость словесной разборчивости W от интегрального отношения сигнал/шум q в полосе частот 180…5600 Гц: 1 – «белый» шум; 2 – «розовый» шум; 3 – шум со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот; 4 – шумовая «речеподобная» помеха

пользуемых для подавления средств перехвата речевой информации. В основном эти системы используют генераторы прямошумовых помех различной структуры и генераторы амплитудно-модулированных и частотно-модулированных шумовых помех. К ним относятся: системы «Заслон», «Кабинет», «Барон», «Порог-2М», «Фон-В», «Шорох», VNG-006, ANG-2000, NG-101, «Эхо», «Соната-АВ» и т. д.

В системах акустической и виброакустической маскировки, как правило, используются шумовые помехи следующих видов [2]:

• «белый» шум (шум с постоянной спектральной плотностью в речевом диапазоне частот);

• «розовый» шум (шум с тенденцией спада спектральной плотности 3 дБ на октаву в сторону высоких частот);

• шум с тенденцией спада спектральной плотности 6 дБ на октаву в сторону высоких частот;

• шумовая «речеподобная» помеха (шум с огибающей амплитудного спектра, подобной речевому сигналу).

Анализ шумовых помех различных видов: белый шум, «розовый» шум, шум с тенденций спада спектральной плотности, шумовая «речеподобная» помеха с использованием метода Н. Б. Покровского приведен на рис.1 [3]. На рисунке приведены графики зависимости словесной разборчивости W от интегрального отношения сигнал/шум q в полосе частот 180…5600 Гц.

Рассмотрим одну из систем активной виброакустической маскировки. Система виброакустической и акустической защиты «Соната-АВ» модель 3М, разработанная и производимая НПО «Анна». Она является техническим средством защиты акустической речевой информации, обрабатываемой в выделенных помещениях до 1 категории включительно, от утечки по акустическому и виброакустическому каналам путем постановки помех в диапазоне частот 90. . .11200 Гц.

Системным признаком модели 3М аппаратуры «Соната-АВ» является построение по принципу «единый источник электрического шумового сигнала + электроакустические преобразователи» (рис. 2).

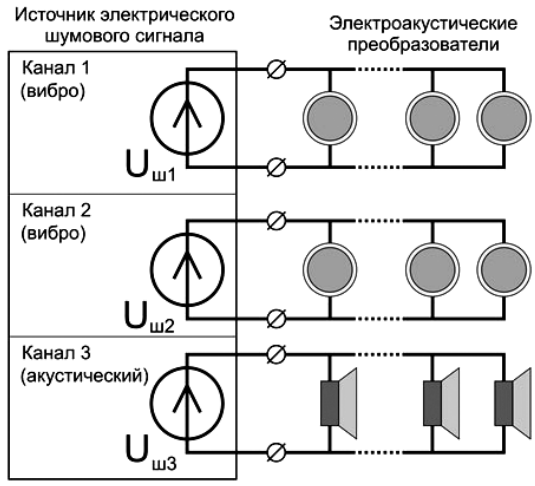


Рис. 2. Схема модели 3М аппаратуры «Соната-АВ»

Для проведения исследований использовали СЗИ «Соната-АВ» модель 3М. После установки системы виброакустической маскировки проводили оценку эффективности ее применения, основанную на результатах проведенных экспериментальных исследований.

При контроле защищенности речевой информации от виброакустической аппаратуры речевой разведки контрольными точками установки измерительного контактного микрофона (виброакустического датчика) являются внешние по отношению к источнику речевого сигнала поверхности различных ограждающих конструкций, инженерных коммуникаций и других предметов, которые находятся на разведопасных направлениях, а также возможные места на инженерных коммуникациях (строительных конструкциях и т. п.), доступных посторонним лицам.

Основным положительным следствием такого построения аппаратуры является более низкая стоимость системы при большом количестве излучателей, т. к. наиболее массовый элемент (излучатель) содержит только электроакустический преобразователь и является предельно простым устройством.

Для анализа возможностей системы проводилась запись голоса при варьировании двух параметров:

1) расположение источника шума относительно записывающего устройства;

2) расположение источника шума относительно источника акустического сигнала.

С использованием аудиоредактора AdobeAudition произведена обработка записей. Применялись фильтры шума, щелчков и другие функции по очистке звука (рис. 3). Для обработки результатов применялись методы теории планирования эксперимента.

По результатам обработки записей сделан вывод, что для полного зашумления акустического канала с помощью прибора Соната–АВ требуется применять сразу несколько октав шума. Иначе имеется возможность «вычистить» запись и разобрать речь (рис. 4–5).

Основными отрицательными следствиями такого построения аппаратуры являются:

• потенциально более высокое мешающее действие системы из-за отсутствия возможности регулировки интегрального уровня и корректировки спектра шума в каждом излучателе;

• относительно высокая стоимость системы при малом количестве и/или большом разнообразии типов нагрузок.

Для лучшей маскировки акустического канала требуются доработки данной системы. А именно создание возможности регулирования интегрального уровня и корректировку спектра шума каждого излучателя независимо друг от друга.

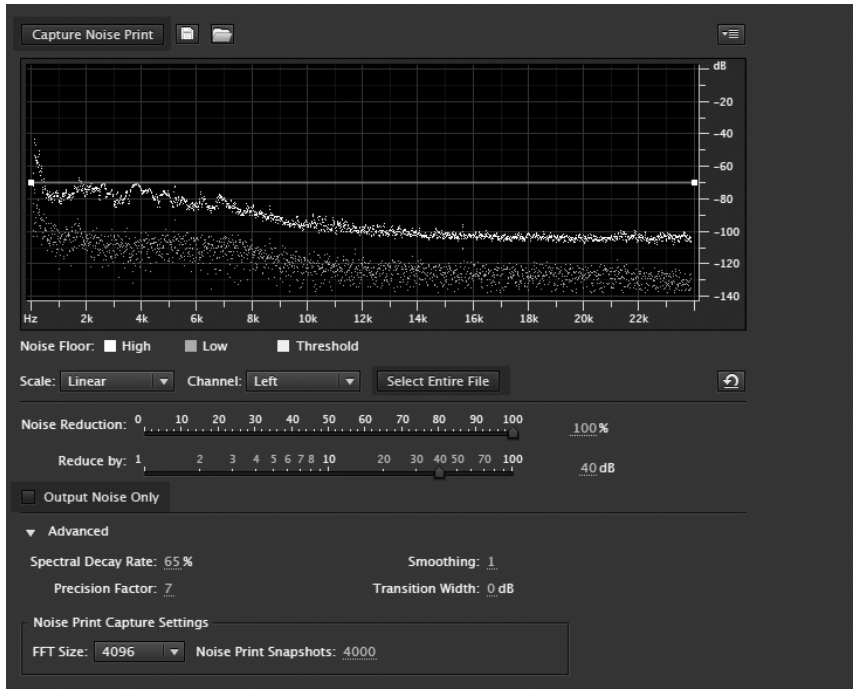


Рис. 3. Фильтр Noise Reduction

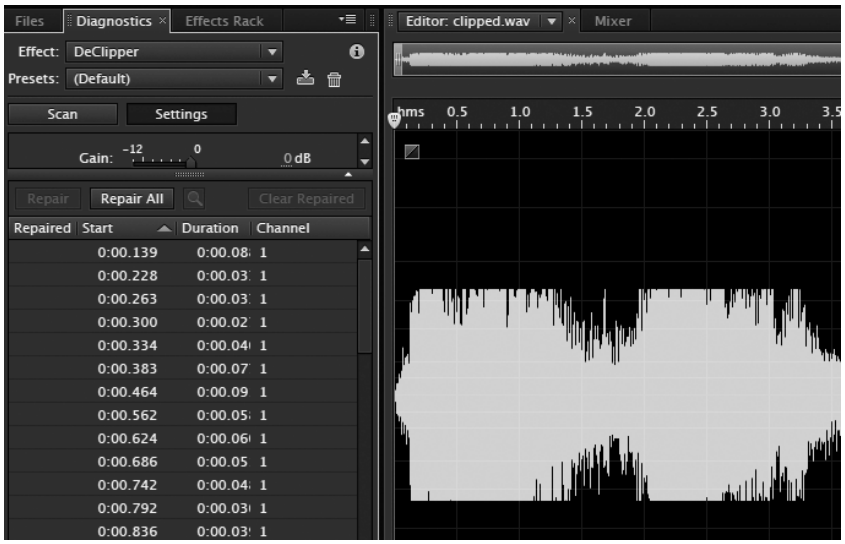


Рис. 4. Акустический канал до фильтрации.

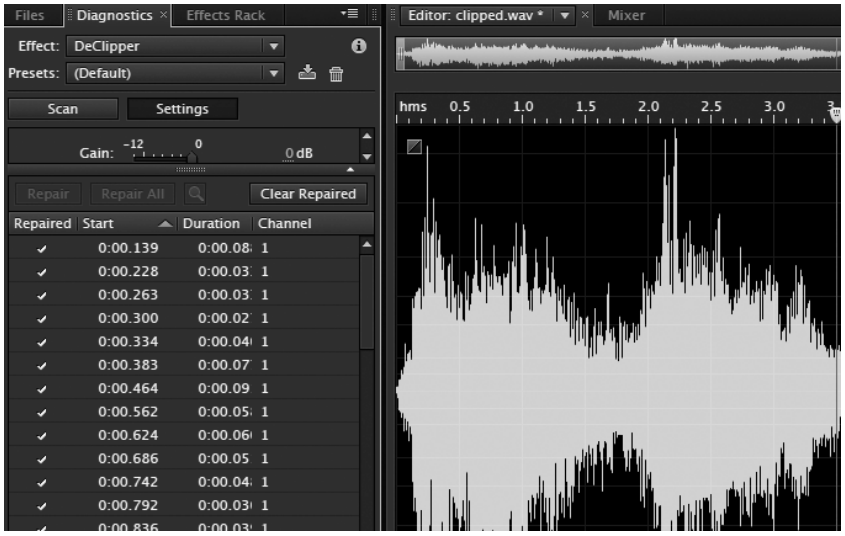


Рис. 5. Акустический канал после фильтрации.

Еще один минус применения всех систем активной виброакустической маскировки – это неблагоприятное воздействие на функциональное состояние человека, несмотря на выполнение медицинских норм. Излучения, испускаемые этими системами, вызывают ярко выраженные негативные психогенные воздействия [4].

В связи с этим на сегодняшний день перспективным подходом к решению задачи защиты информации от утечки по акустическим каналам является совершенствование структуры маскирующих помех и обеспечение соответствия этой структуры заданным требованиям. А также совершенствование методов защиты речевой информации при проектировании и строительстве объектов информатизации с целью снижения уровня излучения акустических и электромагнитных полей за пределами выделенного помещения за счет оптимального размещения и специального выбора конструктивных элементов, обеспечивающих экранирование электромагнитных волн и акустических полей.

Задача защиты информации от утечки по акустическим каналам может быть решена только при комплексном применении активных и пассивных СЗИ вместе с применением организационных мер.

Перспективной тенденцией развития данной области в будущем является не зашумление акустического канала, не воздействие на усилители микрофонов, а попытка точного определения местонахождения «жучков» и использование дистанционного воздействия для полного выведения их из строя.

Примечания

1. ГОСТ Р 50840-95. Методы оценки качества, разборчивости и узнаваемости.

2. Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации// Специальная техника. – 2000. – № 4 – С. 39–45.

3. Покровский Н. Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962.

4. Герасименко В. Г., Лаврухин Ю. Н., Тупота В. И. Методы защиты акустической речевой информации от утечки по техническим каналам. – М.: РЦИБ «Факел», 2008. – 258 с .

Лукьянов Георгий Игоревич, студент, Магнитогорский государственный технический университет. E-mail: decorsi@mail.ru

Михайлова Ульяна Владимировна, к. т. н., доцент, Магнитогорский государственный технический университет. E-mail: ylianapost@gmail.com

Georgy Igorevich Lukyanov, student of G.I. Nosov Magnitogorsk State Technical University. E-mail: decorsi@mail.ru

Uliana Vladimirovna Mikhailova, Cand. Sc. Engineering, associate professor of G.I. Nosov Magnitogorsk State Technical University. E-mail: ylianapost@gmail.com

УДК 004.422.8 + 004.738.056.5 + 342.2/.7 : 004.056

Шабуров А. С., Рашевский Р. Б.

О ПРАКТИЧЕСКОМ ПРИМЕНЕНИИ ТЕХНОЛОГИИ VMWARE VSHIELD APP ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются общие принципы работы семейства продуктов VMWare vShield App в части настройки и управления с использованием API. Приведен пример практического применения VMWare vShield App для сетевой защиты информационной системы персональных данных при реализации требований по защите среды виртуализации.

Ключевые слова: *информационная безопасность, авторизация, гипервизор, сетевая атака, информационная система персональных данных, среда виртуализации.*

Shaburov A. S., Rashevsky R. B.

ON PRACTICAL IMPLEMENTATION OF VMWARE VSHIELD APP TECHNOLOGY FOR ENSURING SECURITY OF PERSONAL DATA INFORMATION SYSTEMS

The authors dwell on general working principles of VMWare vShield App and settings and control with the use of API in particular. The authors give the examples of practical implementation of VMWare vShield App for network security of personal data information systems in the process of implementation of standards of virtualization security.

Keywords: *information security, authorization, hypervisor, network attack, personal data information systems, virtualization environment.*

Развитие корпоративных информационных систем в современных условиях предусматривает использование технологии виртуализации. Актуальность применения подобной технологии обусловлена, в первую очередь, необходимостью сокращения эксплуатационных расходов на информационную инфраструктуру. Вместе с тем, подобные инновации заставляют по-новому решать задачи защиты информации, размещаемой в облачном пространстве, а также предполагают выполнение требований по безопасности информации, регламентированных для различных информационных систем, в том числе информационных систем персональных данных (ИС ПДн) [1].

Уменьшение расходов на информационную инфраструктуру может осуществляться за счет размещения нескольких виртуальных серверов или рабочих станций на базе одного физического узла с установленным гипервизором. При этом применение виртуализации повышает гибкость и удобство развертывания и настройки новых узлов информационной инфраструктуры для сетевых инженеров и системных администраторов [2].

В связи со своей спецификой виртуальная инфраструктура требует несколько иных подходов к обеспечению информационной безопасности. Так, в случае обеспечения антивирусной защиты виртуальных серверов или рабочих станций использование классических антивирусных продуктов, предполагающих установку на каждый защищаемый узел, является нецелесообразным. Более рациональным будет использование антивирусного решения, устанавливаемого на гипервизор и выполняющего сканирование всех виртуальных серверов и рабочих станций, запущенных на физическом узле [3].

Применительно к обеспечению защиты от сетевых атак также более рациональным является использование решения, устанавливаемого на гипервизор. Такое решение позволит снизить использование аппаратных ресурсов физического узла, а также эффективно противостоять различным методикам сокрытия сетевого трафика.

На сегодняшний день лидером в области виртуализации является компания VMWare, имеющая широкую продуктовую линейку в области решений для виртуализации [4]. В целом обеспечение безопасности виртуальной инфраструктуры обеспечивается следующими программными продуктами: VMWare vShield Endpoint, VMWare vShield Edge и VMWare vShield App.

VMWare vShield Endpoint представляет собой специальные программные интерфейсы для организации антивирусной защиты виртуальной инфраструктуры на уровне гипервизора.

VMWare vShield Edge обеспечивает сетевую защиту виртуальной локальной сети, т. е. является аналогом аппаратного межсетевого экрана для виртуальной сети.

VMWare vShield App обеспечивает защиту отдельных виртуальных серверов или рабочих станций, а также групп серверов или рабочих станций средствами гипервизора, позволяя задавать правила фильтрации сетевого трафика.

Каждый из продуктов, входящих в состав продуктовой линейки VMWare vShield, имеет программный интерфейс управления (API) для настройки и управления [5].

API VMWare vShield App реализует модель взаимодействия REST, т. е. вызов тех или иных методов API, когда получение и передача данных выполняются с помощью HTTP-запросов. При этом поддерживаются четыре основных HTTP-метода: GET, POST, PUT, DELETE. Для обеспечения безопасности при работе с API используются защищенное соединение (SSL) и авторизация администратора.

В последней доступной на сегодняшний день версии API–5.5 для взаимодействия с программным интерфейсом необходимо отправить HTTP-запрос по URL-адресу https://<vsm-ip>/api/2.0/app/firewall/.

Организация взаимодействия с API предполагает прохождение процедуры авторизации, которая заключается в передаче пароля администратора в кодировке base64 в запросе. В соответствии с эталонной моделью HTTP-запросов в VMWare vShield API GET-запросы используются для получения текущей конфигурации и статистических данных, POST-запросы – для создания новых правил фильтрации, PUT-запросы – для изменения режима работы VMWare vShield App и DELETE-запросы – для удаления правил фильтрации (рис. 1).

В качестве примера рассмотрим виртуальный веб-сервер на базе UNIX-подобной операционной системы в составе ИС ПДн. Данный веб-сервер имеет два сетевых интерфейса, один из которых используется для доступа к веб-серверу из глобальной сети Ин-

```
   GET https://<vsm-ip>/api./2.0/app/firewall/
<dc-id>/config?list=config&precedence=DEFAULT
   Response Body:

      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312802020950"
timestamp="1312802020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default"
id="1340">
                     <action>block</action>
                     <logged>false</logged>
                     <notes></notes>
                     <source/>
                     <destination/>
                </layer3FirewallRule>
                <layer2FirewallRule disabled="false"precedence="default"
id="1341">
                     <action>allow</action>
                     <logged>false</logged>
                     <notes></notes>
                     <destination/>
                </layer2FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 1. Пример GET-запроса для получения правил, установленных по умолчанию, и ответ API на запрос

тернет, а второй – для подключения администраторов веб-сервера из внутренней сети. При этом основной задачей веб-сервера является взаимодействие по защищенному сетевому протоколу HTTPS для получения пользовательских данных из глобальной сети Интернет. Вместе с тем для обслуживания веб-сервера необходим удаленный доступ из локальной сети по протоколу SSH (рис. 2).

Для настройки правил фильтрации сетевого трафика в рассмотренном выше примере с двумя сетевыми интерфейсами предполагается воспользоваться API VMWare vShield App. На интерфейсе eth0 запретим всю сетевую активность, кроме входящих подключений по порту 443; на интерфейсе eth1 также запретим всю сетевую активность, кроме входящих подключений по порту 25.

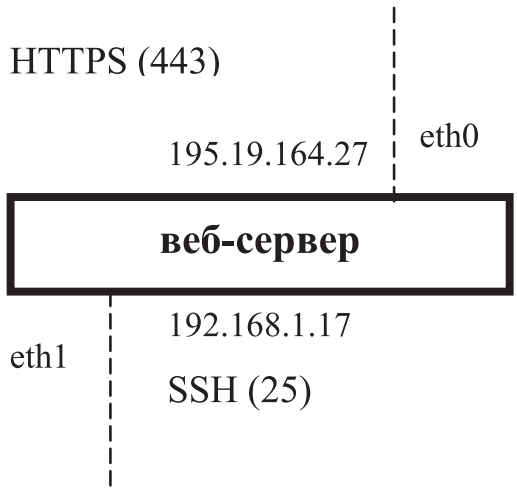


Рис. 2. Общая схема сетевых интерфейсов веб-сервера

Характерно, что поумолчанию весь сетевой трафик на обоих интерфейсах блокируется, т. е. VMWare vShield App работает в режиме «запрещено все, что явно не разрешено». Таким образом, для решения поставленной задачи достаточно создать дополнительные правила фильтрации сетевого трафика: для сетевого интерфейса eth0 необходимо разрешить входящие сетевые соединения по порту 443, а для сетевого интерфейса eth1 необходимо разрешить входящие сетевые соединения по порту 25.

Для добавления нового правила фильтрации сетевого трафика необходимо инициировать POST-запрос к API, в котором осуществить передачу нового правила, записанного в файле формата XML. После чего новое правило будет добавлено в список правил фильтрации VMWare vShield App (рис. 3).

Аналогичным образом добавляется правило для разрешения входящих сетевых соединений на интерфейс eth0 по порту 443.

```
      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312833020950"
timestamp="1312833020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default" id="0">
                      <name>AllowSSH</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows SSh traffic from ANY to eth1</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>25</portinfo>
                      </destination>
                </layer3FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 3. XML-файл с правилом фильтрации сетевого трафика для разрешения входящих сетевых соединений

```
   GET https://<vsm-ip>/api./2.0/app/firewall/
   <dc-id>/config?list=config&precedence=DEFAULT
     Response Body:
      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312802020950"
timestamp="1312802020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default"
id="1340">
                     <action>block</action>
                     <logged>false</logged>
                     <notes></notes>
                     <source/>
                     <destination/>
                </layer3FirewallRule>
                <layer3FirewallRule disabled="false"precedence="default"
id="1342">
                      <name>AllowSSH</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows SSH traffic from ANY to eth1</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>25</portinfo>
                      </destination>
                </layer3FirewallRule>
                <layer3FirewallRule disabled="false"precedence="default"
id="1343">
                      <name>AllowHTTPS</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows HTTPS traffic from ANY to eth0</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>443</portinfo>
                      </destination>
                </layer3FirewallRule>
                <layer2FirewallRule disabled="false"precedence="default"
id="1341">
                     <action>allow</action>
                     <logged>false</logged>
                     <notes></notes>
                     <destination/>
                </layer2FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 4. GET-запрос с ответом для получения конфигурации правил VMWare vShield App

После добавления двух новых правил фильтрации сетевого трафика запросим текущую конфигурацию правил VMWare vShield App посредством GET-запроса к API и убедимся в том, что новые правила фильтрации были добавлены в конфигурацию VMWare vShield App (рис. 4).

Очевидно, все новые правила фильтрации сетевого трафика были корректно добавлены в конфигурации правил фильтрации VMWare vShield App.

Таким образом, проведенный анализ основных принципов функционирования VMWare vShield App API, а также рассмотренный пример практического применения программного интерфейса управления для создания новых правил фильтрации сетевого трафика и изменения конфигурации правил VMWare vShield App позволяют создавать на их основе защищенные виртуальные структуры, в том числе и для информационных систем персональных данных.

Примечания

1. Екимов О. Б., Шабуров А. С., Исаков И. П., Мазунин П. В., Шляков А. Н. «О реализации требований по защите персональных данных в информационной системе пермского филиала ФГУП «РЧЦ ПФО» // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2013. – № 8. – С. 144–155.
2. Кусек К., Ван Ной В., Дэниел А.. Администрирование VMWare vSphere 5. СПб. : Питер, 2013.
3. Sarkar P. VMWare vCloud Security – PACKT Publishing – Bir-mingham, 2014.
4. Bittman T. J., Margevicius M. A., Dawson P.. Gartner Magic Quadrant for x86 Server Virtualization Infrastructure – Gartner Inc. – Stamford, 2014.
5. VMWare vShield API Programming Guide – VMWare Inc. – Palo Alto, 2014.

Шабуров А. С., к. т. н., доцент, Пермский национальный исследовательский политехнический университет. E-mail: shans@at.pstu.ru

Рашевский Р. Б. E-mail: oman@rashevskiy.com

Shaburov A. S., Perm National Research Polytechnic University, Cand. Sc. Engineering, associate professor. E-mail: shans@at.pstu.ru

Rashevsky R. B. E-mail: oman@rashevskiy.com

УДК 004.056.53

Попов Е. Ф., Тюкова А. А., Фучко М. М., Захаров А. А.

ВЫЯВЛЕНИЕ НЕТИПИЧНЫХ СОБЫТИЙ СРЕДСТВАМИ СТАТИСТИЧЕСКОГО АНАЛИЗА

В работе изучается вопрос о применимости алгоритмов статистического анализа для выявления нетипичных событий и состояний в различных информационных системах. Рассматривается возможность применения кластерного анализа для выявления нетипичных потоков трафика в сети передачи данных, а так же его эффективность при различной интерпретации характеристик потоков сетевого трафика.

Ключевые слова: *статистический анализ, кластерный анализ, сети передачи данных, выявление аномалий, система обнаружения вторжений.*

Popov E., Tyukova A., Fuchko M., Zakharov A.

IDENTIFICATION OF ATYPICAL EVENTS MEANS OF THE STATISTICAL ANALYSIS

In this paper we study the question of the applicability of statistical analysis to detect unusual events and conditions in various information systems. The possibility of using cluster analysis to identify unusual traffic flows in a data network, as well as its effectiveness in different interpretations of the characteristics of network traffic flows.

Keywords: *statistical analysis, cluster analysis, data transmission networks, detection of anomalies, system of detection of invasions.*

ВВЕДЕНИЕ

В условиях быстрого развития информационных технологий постоянно разрабатываются новые методы атак на информационные системы, что требует непрерывного совершенствования средств защиты информации. Так как предусмотреть все способы атак на информационную систему зачастую не представляется возможным, оптимальным решением является выявление нетипичных событий и состояний системы.

Для выявления отклонений необходимы показатели, которые отображают типичное состояние информационной системы и могут выступать в качестве эталона для сопоставления с данными, обрабатываемыми в реальном времени. Применение алгоритмов статистического анализа к данным, собранным в период штатного функционирования, позволяет выделить статистические показатели, при сравнении с которыми можно выявить нетипичные события и состояния, являющиеся потенциально опасными для информационной системы.

В данной работе изучается вопрос о применимости алгоритмов статистического анализа, для выявления нетипичных событий и состояний на примере потоков трафика в сетях передачи данных. Рассматривается эффективность применения результатов кластерного анализа в реальном времени при различной интерпретации характери-

стик потоков сетевого трафика. По результатам применения кластерного анализа к потокам трафика в сети передачи данных оценивается возможность применения используемого метода для выявления нетипичных событий и состояний в различных подсистемах и элементах информационной инфраструктуры.

СБОР И ИНТЕРПРЕТАЦИЯ СТАТИСТИЧЕСКИХ ДАННЫХ

Сложность применения статистического анализа в данном контексте заключается в том, что применяемые алгоритмы должны быть адаптированы для обработки данных в реальном времени и должны производить интеллектуальный анализ, учитывающий не только текущее состояние системы или состояния за короткий промежуток времени. Наиболее ценными являются данные, собранные за длительные периоды штатного функционирования, которые являются необходимыми для наиболее точного выявления типичных событий и состояний системы. [1]

Для обработки характеристик, собранных за длительный период, важно применять алгоритмы статистического анализа, не только адаптированные для обработки большого количества данных, но и способные учитывать степень устаревания, что является необходимым для адаптации к изменениям в информационной системе. Наиболее оптимальными являются алгоритмы, которые способны производить анализ не только на базе набора статистических данных, но и с учетом предыдущих результатов работы алгоритмов статистического анализа.

События и состояния могут рассматриваться как объекты, обладающие рядом характеристик. Полученные объекты могут быть использованы в качестве статистических единиц для таких алгоритмов статистического анализа, как алгоритмы кластеризации. Рассмотрим применение статистического анализа для выявления нетипичных состояний на примере.

Наиболее удобным для рассмотрения является пример применения статистического анализа к потокам трафика в сети передачи данных. Для сбора информации о потоках трафика могут использоваться сенсоры, базирующиеся на протоколе NetFlow. Подобные сенсоры позволяют получить следующие характеристики:

- IP-адреса отправителя и назначения;
- протоколы сетевого и транспортного уровня;
- номера портов (TCP/UDP), позволяющие определить используемый протокол прикладного уровня;
- время;
- объем переданных данных;
- средний размер пакетов данных.[2]

Полученные характеристики необходимо адаптировать для применения кластерного анализа.

IP-адрес не может применяться для кластерного анализа в чистом виде, так как не характеризует никаких особенностей потока трафика, и данные, передаваемые на различные адреса, могут быть предназначены для работы с одним и тем же сервисом. Например, таким как поисковик Google, который обеспечивает балансировку нагрузки за счет соответствия своему основному доменному имени ряда различных IP-адресов, что не всегда возможно отслеживать автоматически в процессе кластерного анализа.[3]

Но за счет адреса назначения можно выявить ряд особенностей потока трафика, например, выявить для внутренней или для внешней сети предназначен поток трафика, что является важной характеристикой в процессе анализа. Так же, опираясь на адрес отправителя, можно выявить какие устройства или какая группа пользователей располагаются в данной подсети, определив из какой подсети инициирован поток трафика.

Протокол прикладного уровня, который определяется номерами портов, является одной из ключевых характеристик, которая может быть интерпретирована различным образом. Можно разделять статистические единицы на множество классов, считая потоки данных каждого из протоколов прикладного уровня отдельными классами. Так же, протоколы прикладного уровня могут быть разделены на классы по их функциональному предназначению:

- получение информации с веб-сайтов;
- передача файлов;
- мгновенный обмен сообщениями;
- потоковая передача данных;
- удаленное управление;
- и т.д.

При сравнении потоков сетевого трафика, относящихся к различным классам, было выявлено, что остальные характеристики, такие как объем передаваемых данных, дли-

тельность передачи данных, средний размер пакета зависит от класса потока трафика, определенного по функциональному предназначению протокола прикладного уровня. И характеристики потоков сетевого трафика различных протоколов прикладного уровня, относящихся к одному классу, имеют сходство намного большее, чем в случае с протоколами, относящимся к разным классам. [4]

ПРИМЕНЕНИЕ СТАТИСТИЧЕСКОГО АНАЛИЗА

Необходимо выделить единицу потока трафика, к которой будет применяться статистический анализ. В данном контексте статистической единицей могут являться:

- поток трафика от уникального отправителя уникальному получателю за весь период передачи данных (период активности сессии);
- поток трафика от уникального отправителя уникальному получателю за заданный промежуток времени.

Анализ потока за полный период передачи данных между двумя узлами предоставляет наиболее точную характеристику природы трафика и является наиболее ценным для статистического анализа. Но статистика, составленная на базе информации о сетевом трафике, переданном за полный период активности сессии, может быть использована для обнаружения нетипичных потоков данных, только после завершения сессии, что значительно увеличивает время реакции системы.

При использовании в качестве статистических единиц сегментов, выделенных из общего потока, ограниченных небольшими промежутками времени, например интервалами в 30 секунд, снижается точность статистического анализа, но появляется возможность использования результата статистического анализа для обнаружения нетипичных действий в реальном времени, с максимальным временем реакции равным выбранному интервалу времени для статистической единицы.[5]

Каждую отдельную статистическую единицу можно представить в виде точки, расположенной в многомерном пространстве, каждое из измерений которого представляет собой одну из характеристик потока трафика. Применение алгоритма кластеризации позволит выявить области с высокой концентрацией точек и объединить их в кластеры. В результате работы алгоритмы будут получены кластеры, отображающие наборы характеристик, свойственные потокам сетевого трафика, передаваемого при штатном функционировании системы.[6]

На базе результатов вычислений могут быть выделены правила, описывающие значения ряда характеристик, свойственные для полученных кластеров, которые могут стать эталонными для определения типичности потоков трафика. Наличие правил, описывающих типичные потоки трафика, открывает возможность производить в реальном времени контроль, лежат ли значения характеристик текущих потоков трафика в рамках типичных для данной информационной системы.

ВЫВОДЫ

В результате исследования было выявлено, что интерпретация статистических единиц, как объектов обладающих рядом характеристик, позволяет адаптировать статистические данные о событиях и состояниях различных подсистем для анализа с применением алгоритмов кластеризации. Необходимым и достаточным для применения кластерного анализа является наличие исчисляемых характеристик событий или состояний. На эффективность алгоритмов кластеризации влияет равномерность распределения и зависимость характеристик статистических единиц.

Было определено, что по результатам кластерного анализа может быть разработан ряд правил, определяющий типичные значения характеристик статистической единицы, которые могут быть применены для выявления нетипичных событий или состояний в реальном времени без необходимости повторного применения алгоритмов статистического анализа.

На примере применения кластерного анализа для выявления нетипичных потоков трафика в сети передачи данных обнаружена зависимость эффективности алгоритмов кластеризации от интерпретации характеристик статистических единиц. Определено, что классификация статистических единиц по характеристикам, не имеющим числового значения, может оказывать высокое влияние на эффективность кластерного анализа, при условии зависимости от них значений исчисляемых характеристик.

Примечания

1. Babenko G. V., Belov S. V. Identification of network abnormalities using methods of statistical analysis //European researcher – 2011. – Т. 1. – №. 5.

2. Claise D. Cisco Systems NetFlow Services Export Version 9 // IETF RFC 3954 URL: http://www.ietf.org/rfc/rfc3954 (датаобращения 08.12.2014)

3. Barroso L. A., Dean J., Holzle U. Web search for a planet: The Google cluster architecture //Micro, Ieee. – 2003. – Т. 23. – №. 2. – С. 22-28.

4. Soysal M., Schmidt E. G. Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison //Performance Evaluation. – 2010. – Т. 67. – №. 6. – С. 451-467.

5. Костенко С. А. Технология применения многомерного шкалирования и кластерного анализа // Фундаментальные исследования. – 2012. – №. 11. – С. 927-930.

6. Дюран Б., Оделл П. Кластерный анализ //М.: Статистика. – 1977. – Т. 15.

Попов Евгений Фёдорович, аспирант, Тюменский государственный университет. E-mail: efpopov@gmail.com

ТюковаАлександра Александровна, аспирант, Тюменский государственный университет. E-mail: tyukovaaa@kbinform.ru

Фучко Михаил Михайлович, аспирант, Тюменский государственный университет. E-mail: mikhalich@russia.ru

Захаров Александр Анатольевич, д.т.н., профессор ТюмГУ

Popov Evgeniy Fedorovich, graduate Tyumen State University. E-mail: efpopov@gmail.com

Tyukova Aleksandra Aleksandrovna, graduate Tyumen State University. E-mail: tyukovaaa@kbinform.ru

Fuchko Mikhail Mikhailovich, graduate Tyumen State University. E-mail: mikhalich@russia.ru

Zakharov Alexander Anatolevich, professor Tyumen State University

УДК 004.056.53 + 004.451

Кондрашин Д. В., Горшенин В. В.

ГРАФИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ДЛЯ ANDROID УСТРОЙСТВ

Целью данной работы является разработка собственного программного продукта, реализующего надежную графическую аутентификацию для мобильной операционной системы Android. Приложение должно быть устойчиво, к самым распространенным видам атак, в частности к атаке подглядывания из-за плеча. В итоге было создано приложение AlphaLocker, которое сейчас доступно для скачивания в Google Market. Имеется уже около 500 скачиваний из разных стран мира. В данные момент ведется доработка приложения с учетом полученных комментариев.

Ключевые слова: *информационная безопасность, аутентификация, схема треугольника, мобильные операционные системы, Android, графический пароль.*

Kondrashin D. V., Gorshenin V. V.

GRAPHIC AUTHENTICATION FOR ANDROID DEVICES

The aim of the article is to develop individual software which implements reliable graphical authentication for Android mobile operating system. The application is to be resistant to the most common types of attacks and spying over the shoulder attack in particular. As a result, the AlphaLocker application was created and is now available for download in Google Market. There have already been about 500 downloads from various countries all over the world. At the moment the application is being debugged taking into account comments received.

Keywords: *information security, authentication, delta network, mobile operating systems, Android, picture password.*

Сейчас сложно представить человека, не имеющего смартфона или планшетного компьютера. В связи с этим объем и важность информации, хранимой на мобильных устройствах, стремительно растут. И, следовательно, необходимы средства для защиты хранимой информации и самого устройства от несанкционированного доступа.

Наиболее логичным и простым решением данной проблемы является использование надежной схемы аутентификации в системе.

Наиболее распространенным методом аутентификации в компьютерной системе является механизм, основанный на том, что пользователь вводит имя пользователя и текстовый пароль. Однако у этой схемы можно выделить ряд недостатков.

Например, буквенно-цифровые пароли обеспечивают высокую безопасность, если

они сложны. Однако многие пользователи испытывают трудности в запоминании случайных строк символов.

Поэтому становятся возможными атаки по словарю или атаки полного перебора. Другой недостаток символьного пароля заключается в том, что такая схема аутентификации не решает так называемую проблему «подглядывания из-за плеча». Заключается она в следующем: если во время ввода пароля злоумышленник имеет возможность увидеть или снять на видео процесс ввода пароля, то он без труда сможет повторить его позже.

В рамках данной работы речь пойдет о другой альтернативе текстовым паролям - графической аутентификации. Графические пароли имеют ряд преимуществ.

Использование изображений в качестве паролей делает невозможной атаку по словарю частично из-за большого пространства паролей и, главное, потому что не существует доступных для поиска словарей для графической информации. И наконец, некоторые схемы графической аутентификации позволяют решить проблему «подглядывания из-за плеча».

Целью данной работы является разработка собственного программного продукта, реализующего надежную графическую аутентификацию для одной из наиболее популярных мобильных операционных систем – Android.

При выборе метода аутентификации было решено использовать *схему треугольника*, так как она наиболее понятна для пользователя и одновременно устойчива к подглядыванию через плечо. При входе система будет случайным образом выбирать размещение N изображений. При установке пароля пользователь выбирает M изображений из базы размера N. При входе система случайным образом выбирает и рассеивает по экрану K изображений из базы, среди которых ровно 3 парольных. Пользователь должен найти выбранные парольные изображения и выбрать область внутри невидимого треугольника, созданного этими 3 изображениями.

Учитывая, что приложение ориентировано для использования на планшетных компьютерах и смартфонах, схема была несколько изменена с целью адаптации под мобильные устройства.

• Использовались легко запоминаемые графические изображения в виде латинских строчных и прописных букв.

• Изображения выводятся на экран в дискретной сетке.

• Уменьшение количества выводимых на экран изображений за счет разбиения раунда на два этапа и опционального задания количества успешно пройденных раундов (в первой половине раунда пользователь должен выбрать изображение внутри парольного треугольника, во второй половине – вне треугольника).

• Также для усложнения подбора пароля количество ошибок при вводе пароля ограничено, после чего происходит блокировка устройства.

• Площадь парольного треугольника не должна превышать 1/3 экрана.



Рис. 1. Первая половина раунда

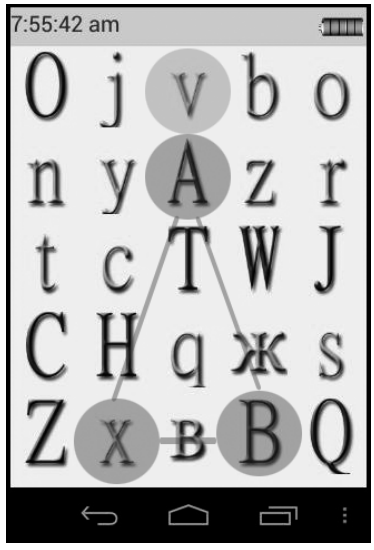


Рис. 2. Вторая половина раунда



Рис. 3. Выбор графического пароля

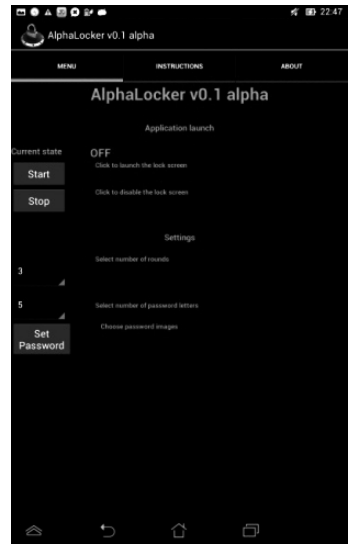


Рис. 4. Меню настройки

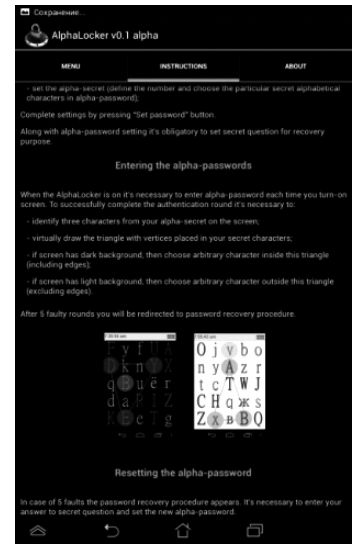


Рис. 5. Вкладка Instuctions

При такой реализации вероятность пройти один раунд наудачу приближенно равняется 0,016, причем при увеличении количества раундов она уменьшается экспоненциально.

Количество возможных паролей есть «биномиальный коэффициент». В нашем случае при N = 52, M = 5 число возможных паролей равно 2598960. При этом реализация приложения допускает всего 5 ошибок, что делает атаку полным перебором на данное приложение практически невозможной.

В случае подглядывания из-за плеча понадобится около 700 полноценных записей входа в систему, чтобы определить пароль пользователя. То есть если пользователь будет входить в систему каждый день в среднем по 10 раз, включая выходные и праздники, злоумышленнику придется подсматривать за ним почти 2 месяца.

Следующим шагам для создания надежного приложения был анализ ОС Android, в частности пришлось столкнуться со следующими проблемами:

• Запуск приложения при блокировке экрана.

• Не системное приложение не может перехватить нажатие кнопки Home.

• Не системное приложение не может перехватить двойное нажатие/удерживание кнопки Home, вызывающее менеджер задач.

• Блокировка остальных аппаратных кнопок.

Для решения первой и последней проблем достаточно переопределить соответствующие обработчики системных событий.

Решением второй проблемы являлось написание собственного системного загрузчика приложений (Launcher) и его установка в систему. Для этого при установке приложения пользователь должен согласиться с изменением загрузчика по умолчанию. После чего, если экран заблокирован, то вызывается наш загрузчик, который не позволяет закрыть приложение нажатием кнопки Home. После входа пользователя в систему, управление передается стандартному загрузчику android и система функционирует как обычно.

Для решения третьей проблемы при вызове менеджера задач приложение автоматически выбирает себя текущей задачей, после чего посылает сообщение о закрытии менеджера.

Последним этапом в разработке приложения было создание максимально удобного для пользователя интерфейса (вывод заряда батареи, уведомлений о пропущенных звонках и смс, отображение времени на экране блокировки и другое).

А также создание меню настроек, в котором пользователь может включить или отключить блокировку экрана приложением, установить количество раундов и парольных картинок. Здесь же происходит установка или изменение пароля. При первом запуске пользователь может беспрепятственно установить пароль и настройки для восстановления пароля. Для смены пароля потребуется ввести подтверждение старого пароля. Также стоит отметить, что изменение количества раундов или парольных изображений происходит только при смене пароля.

Для удобства пользователя в меню существует вкладка “Instructions”, которая содержит описание всех необходимых от пользователя действий по настройке приложения и аутентификации в системе.

В итоге было разработано приложение AlphaLocker, которое реализует схему треугольника для экрана блокировки операционной системы Android.

Далее был проведен ряд тестов, чтобы убедиться, что разработанное приложение действительно обеспечивает надежную защиту устройства и хранимой на нем информации.

Приложение доступно в Google Market по ссылке:

https://play.google.com/store/apps/details?id=com.AlphaLocker

или на официальном сайте:

http://alphalocker.bloolocker.com/

Примечания

1. Sobrado L., Birget, J. Graphical Passwords // The Rutgers Scholar, Rutgers University, Camden New Jersey. – 2002. - 4.
2. Jansen W., Gavrila S., Korolev и др. Picture Password: A Visual Login.
3. Technique for Mobile Devices // NIST Report - NISTIR7030. – 2003.
4. Голощапов А. Л. Google Android. Создание приложений для смартфонов и планшетных ПК. 2-е издание // БХВ-Петербург, 2013.
5. Рето Майер. Android 4. Программирование приложений для планшетных компьютеров и смартфонов // М.: Эксмо, 2013

Кондрашин Дмитрий Вячеславович, студент, Челябинский государственный университет. E-mail: dimon-280894@mail.ru

Горшенин Владимир Викторович, ст. преподаватель, Челябинский государственный университет.

Dmitry Vyacheslavovich Kondrashin, student of Chelyabinsk State University. E-mail: dimon-280894@mail.ru

Vladimir Viktorovich Gorshenin, senior lecturer of Chelyabinsk State University.

УДК 004.056.5 + 004.5 : 004.6

Моисеев А. М., Мамыкин А. В., Москвин В. В.

АТАКА ЧЕРЕЗ USB

USB – очень распространённый последовательный интерфейс передачи данных. За последние десятилетия этот стандарт успешно завоевал мир благодаря своей универсальности – различные устройства, работающие с USB, могут подключаться к одному и тому же разъему. В этом году за месяц до ежегодной хакерской конференции Black Hat USA был анонсирован доклад Карстена Ноля под названием «BadUSB – об аксессуарах, обратившихся во зло». В нем была описана уязвимость, которая не подлежит обнаружению стандартными средствами защиты. В данной статье мы хотели бы показать, что вовсе необязательно модифицировать уже существующие, а можно разработать свои устройства для проведения атаки через USB-интерфейс.

Ключевые слова: *информация, безопасность, уязвимости, информационная безопасность, инженерно-техническая защита информации.*

Moiseev A. M., Mamykin A. V., Moskvin V. V.

USB DRIVEN ATTACK

USB is a very common serial data interface. Over the past decades the aforementioned standard has successfully conquered the world due to its versatility: different devices operating with USB can connect to the same port. This year, a month before the annual hacker conference Black Hat USA Karsten Noll report entitled 'BadUSB. On accessories enquired with evil' was announced. It has described vulnerability that is not subject to detection by standard means of protection. In this article the authors would like to show that it is not necessary to modify the existing devices, one can develop personal device for an attack through the USB interface.

Keywords: *information, security, vulnerability, information security, engineer and technical information security.*

Интерфейс USB применяется в огромном количестве самых различных устройств, начиная с персональных компьютеров и заканчивая телевизорами. Этот стандарт имеет несколько версий. Причем устройства новых версий совместимы с интерфейсами старых версий, и наоборот (прямая и обратная совместимость).

Различных типов USB-устройств выделяется достаточно много: flash-накопители, USB-cdrom'ы, мыши, клавиатуры, игровые контроллеры, сетевые карты и множество других. Каждое такое устройство относится к определенному классу, согласно спецификации, определяющей функциональность этого устройства.

Примерами таких классов являются: звуковые карты, сетевые карты, устройства HID, веб-камеры, принтеры и прочие. Более подробно с классами устройств можно ознакомиться на сайте http://www.usb.org/developers/defined_class.

Классов устройств существует достаточно много. Наиболее известными и распро-

страненными среди этих классов являются HID, или «устройства человеческого интерфейса» – клавиатуры, мыши, джойстики, контроллеры беспроводной связи (Bluetooth/Wi-Fi), внешние устройства памяти и т. д. USB-HID не требуют установки специальных драйверов и могут работать сразу после подключения к ПК (Plug&Play). Реализовано это за счёт наличия драйверов в составе самой ОС.

Функциональность каждого устройства обеспечивает программно-управляемый USB-контроллер причем для различных классов может применяться один и тот же контроллер, с различной прошивкой. Именно USB-контроллер «сообщает» ПК о том, какое устройство к нему подключено.

Уязвимость «BadUSB», описанная в докладе Карстена Нолла, основывается на том, что при наличии соответствующей прошивки любое устройство может «маскироваться» под устройство другого класса и выполнять его функции.

С первого взгляда может показаться, что публикация этой уязвимости приведет к очередной эпидемии, ведь каждый желающий сможет реализовать её без каких-либо проблем. На самом деле проблем достаточно, и самая главная и очевидная проблема – в выборе оборудования. Для USB-устройств производители используют специальное ПО с закрытым исходным кодом. Чтобы преодолеть эту проблему, нужно прибегнуть к back-инжинирингу, чем и занялись специалисты Адам Коудил и Брэндон Уилсон, которые рассказали в совместном докладе на ежегодной конференции Derby Con об успешной прошивке контроллера Phison 2303 (2251-03). В итоге им удалось создать альтернативную прошивку, имитирующую клавиатуру.

В данной статье мы хотели бы показать, что проведение back-инжиниринга готового устройства – это не единственный способ реализации атаки через USB. Вместо того чтобы модифицировать заводское, можно достаточно просто разработать своё специализированное устройство для проведения данного вида атаки. Для этого необходимо воспользоваться практически любым микроконтроллером с аппаратной поддержкой USB. Мы остановились на наиболее широко распространенном микроконтроллере STM32F103C8 европейской фирмы STMicroelectronics. Принципиальная схема разработанного нами устройства, изображена на рис. 1.

Данный микроконтроллер имеет 32-битную архитектуру ARM Cortex M-3 с тактовой

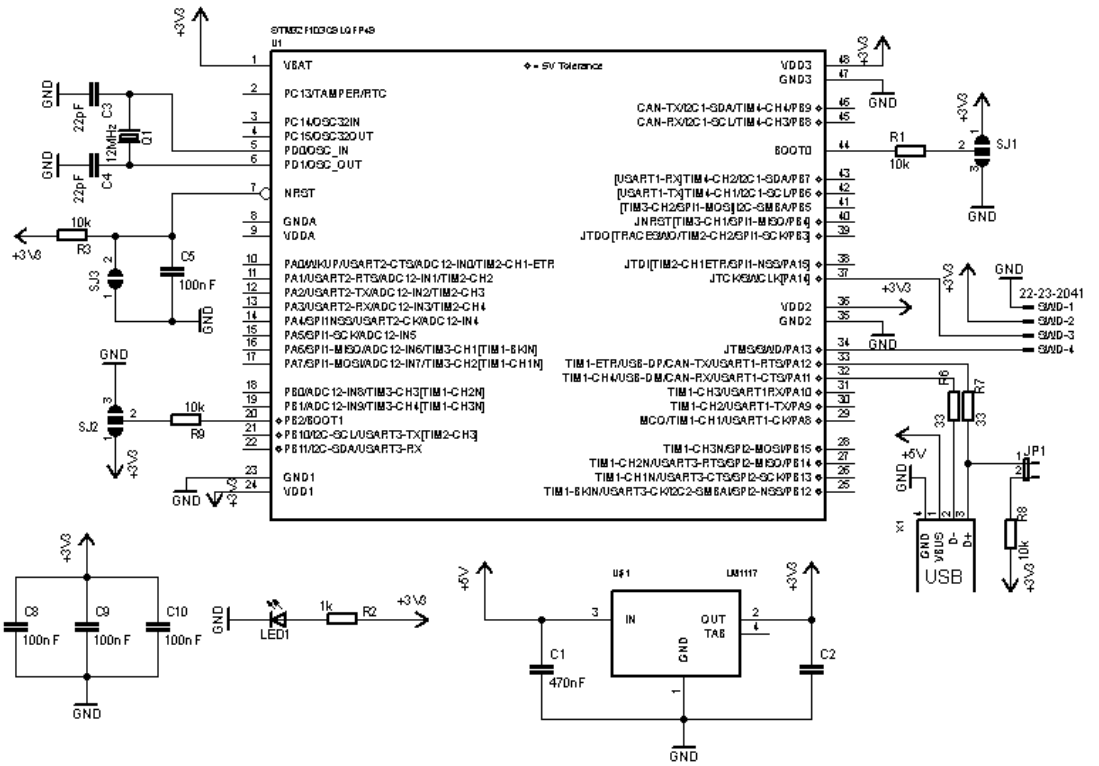


Рис. 1. Схема устройства

частотой до 72 МГц, 64 кБ программной памяти и 20 кБ оперативной памяти. Также он поддерживает следующие интерфейсы: CAN, I2C, SPI, USART и, конечно, USB.

Прошить его можно несколькими способами: через специализированные отладочные порты JTAG/SWD и программатор-отладчик (нами использовался ST-Link/v2), либо воспользовавшись простым USB-UART (COM-UART) адаптером, поскольку данный микроконтроллер содержит в памяти встроенный загрузчик.

Прежде всего необходимо определиться с HID-классом устройства. Для целенаправленной атаки на ПК лучше всего подойдет эмулирование клавиатуры, поскольку с помощью неё доступно выполнение большинства функций операционной системы. Вся информация, необходимая для поддержки функционирования HID-устройств, заложена в дескрипторах. Кроме того, можно привести небольшой список аналогичных векторов атак, основывающихся на других HID-устройствах:

• эмулирование сетевой карты и подмен/анализ пакетов данных. Предоставляет широчайшие возможности для атак типа «Man in the middle»;

• эмулирование флэш-накопителя совместно с клавиатурой с целью заражения ОС и подключенных уязвимых микроконтроллеров или модификации bios.

Дескриптор – это описание свойств устройства, а также функций, выполнение которых оно поддерживает. Он определяет способы обмена информацией, режимы работы и подходящий для устройства драйвер. Управлением шины занимается хост, поэтому HID-устройство не может инициировать передачу данных самостоятельно, оно лишь опрашивается хостом. Поэтому в описании дескриптора должна быть указана частота опроса. Считывание дескриптора производит требование GET_DESCRIPTOR. Ниже приведена таблица стандартных дескрипторов.

Так как Device дескриптор определяет само устройство, то он всегда один, а дескрипторов Configuration, Interface и Endpoint может быть несколько. Это связано с тем, что устройство может быть составным и иметь различные параметры электропитания. Дескрипторы, перечисленные в данном абзаце, являются обязательными, все остальные – необязательные (могут быть не заданы).

Отдельно выделяют Report дескриптор. ПК и USB-устройство обмениваются данными с помощью пакетов заранее определенного формата (report пакет). Различных типов пакетов может быть много, каждый – для выполнения своей задачи. Так как у данного дескриптора достаточно строгий формат, а ошибки в нем недопустимы, можно автоматизировать процесс его настройки с помощью утилиты «Usb Hid Demonstrator» от STMicroelectronics.

Для того чтобы наше устройство не вызывало подозрений у пользователя, такие параметры как VendorID, ProductId, а также серийный номер и производитель, могут быть скопированы с реального устройства.

В нашем случае использовался лишь микроконтроллер, но с добавлением к нему новых устройств его функционал можно значительно расширить – к примеру, flash-накопитель, который может нести в одном из разделов вирус, загружаемый в систему.

На данный момент каких-либо способов защиты от атак данного типа, кроме использования доверенных устройств, не существу-

Таблица 1

Код	Тип описания
0	DEVICE (устройство)
1	CONFIGURATION (конфигурация)
2	STRING (строка)
3	INTERFACE (интерфейс)
4	Зарезервировано
5	ENDPOINT (точка)
6	DEVICE_QUALIFIER (устройство для другой скорости)
7	OTHER_SPEED_CONFIGURATION (конфигурация для другой скорости)
8	INTERFACE_POWER

ет, но производители могут следовать определенным рекомендациям, чтобы значительно уменьшить вероятность их реализации в будущем:

1) Разделить USB-порты в ПК в зависимости от класса устройства. Таким образом, к примеру, выполнение функций клавиатуры USB-накопителем станет невозможным;

2) Контролирование классов устройств на программном уровне. Своеобразный USB-фаервол, проверяющий соответствие класса устройства и выполняемых им функций;

3) Подпись прошивок производителем устройства и проверка цифровой подписи ОС при подключении. ОС просто заблокирует устройство с модифицированной прошивкой.

Примечания

1. Чекунов, Д. Программисту USB-устройств. Часть 1. Знакомство с USB / Д. Чекунов // Современная электроника. – 2004. - № 1. – С. 68–71.

2. Чекунов, Д. Программисту USB-устройств. Часть 2. Стандартные требования USB / Д. Чекунов // Современная электроника. – 2004. - № 2. – С. 70–75.

3. Чекунов, Д. Программисту USB-устройств. Часть 3. Стандартные дескрипторы USB / Д. Чекунов // Современная электроника. – 2005. - № 1. – С. 72–77.

4. Defined 1.0 Class Codes [Электронный ресурс]. - Usb.org. Режим доступа: www.usb.org/developers/defined_class, свободный. – Загл. с экрана.

Моисеев Алексей Михайлович, студент, Курганский государственный университет E-mail: mamykin.av@bk.ru

Мамыкин Андрей Владимирович, студент, Курганский государственный университет. E-mail: mamykin.av@bk.ru

Москвин Владимир Викторович, ст. преподаватель, Курганский государственный университет.

Aleksey Michailovich Moiseev, student of Kurgan State University. E-mail: mamykin.av@bk.ru

Andrey Vladimirovich Mamykin, student of Kurgan State University. E-mail: mamykin.av@bk.ru

Vladimir Viktorovich Moskvin, senior teacher of Kurgan State University.

УДК 004.057.4 + 004.056

Токарчук Н. А., Середкина Е. Д., Зюляркина Н. Д.

ПРОТОКОЛ TCP КАК СТЕГАНОГРАФИЧЕСКИЙ КОНТЕЙНЕР

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Отличительной особенностью стеганографии по сравнению с криптографией является то, что стеганография не скрывает содержимое сообщения, а скрывает сам факт передачи. При этом контейнером для сообщения может быть, например, изображение, видеофайл или аудиофайл. В данной работе рассматривается метод сетевой стеганографии, в котором в качестве контейнера для хранения стеганографического сообщения используются TCP-сегменты.

Ключевые слова: *информация, безопасность, защита информации, компьютерная безопасность, стеганография.*

Tokarchuk N. A, Seredkina E. D., Ziuliarkina N. D.

TCP PROTOCOL AS A STEGANOGRAPHIC CONTAINER

Steganography is the science of secure information transfer by means of secrecy of the fact of the transfer. In comparison with cryptography the distinctive feature of stagnography is that it does not hide the message content but hides the fact of transmission. When this happens an image, a video, or an audio file can be a container for a message. The authors dwell on the method of network steganography which uses TCP-segments as containers for steganographic messages.

Keywords: *information, security, information security, computer security, teganography.*

Основная идея

Впервые использование TCP-сегментов и механизма RTO для передачи стеганографических сообщений было предложено учеными из Варшавского университета в работе «Retransmission steganography and its detection» в 2009 году [1].

Механизм RTO (Retransmission Timeout) подразумевает повторную отправку пакетов, которые были повреждены или утеряны. Для отслеживания потери пакетов используется метод обработки ошибок ARQ (Automatic repeat request).

Когда TCP передает сегмент, содержащий данные, он помещает его копию в очередь повторной передачи и запускает таймер. При получении подтверждения для данного сегмента он удаляется из очереди. Если подтверждение не получено до окончания действия таймера, сегмент отправляется повторно [2].

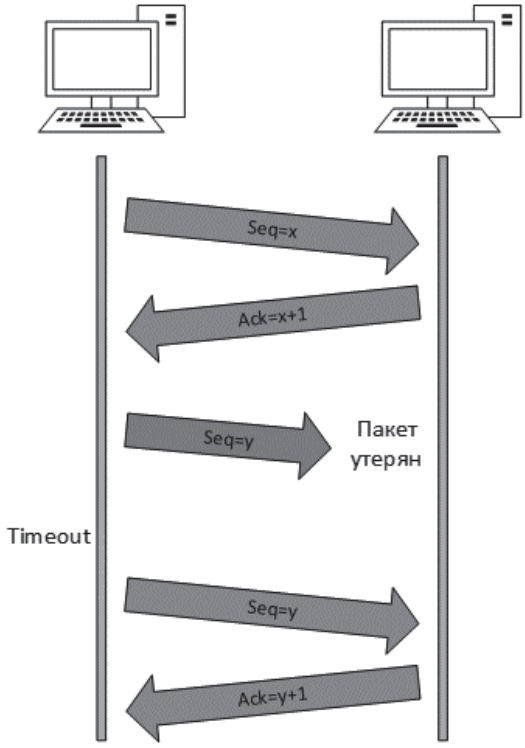


Рис. 1. Механизм RTO

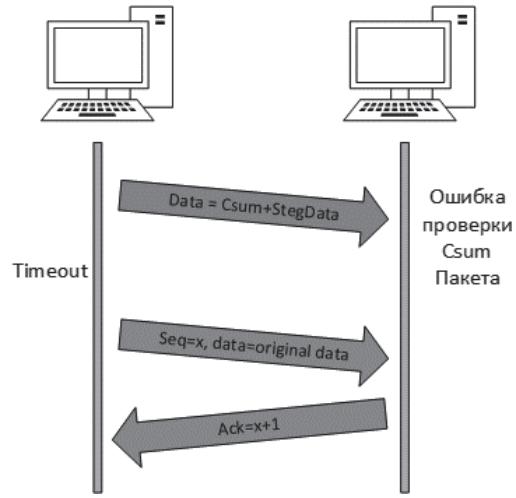


Рис. 2. Идея передачи стеганограмм

Мы реализовали свою идею использования механизма RTO для передачи стеганографических сообщений, которая заключается в паразитном использовании оригинальных сегментов с флагом PSH:

1) при отправке пользователем сегмента с некоторой вероятностью создается стеганографическая структура, состоящая из контрольной суммы стеганографического сообщения и непосредственно самого сообщения. Размер созданной стеганографической структуры должен соответствовать размеру поля данных в оригинальном сегменте;

2) получатель принимает сообщение, но из-за несовпадения контрольной суммы сегмент отбрасывается, а из данных извлекается стеганографическая структура и отправляется на проверку;

3) обработчик извлекает из стеганографической структуры контрольную сумму и сообщение, сам подсчитывает для сообщения контрольную сумму и сравнивает ее с извлеченной. При совпадении сумм сообщение считается принятым, иначе отбрасывается;

4) по истечении времени timeout отправитель передает сегмент, содержащий оригинальные данные;

5) получатель отправляет подтверждение.

Реализация

В данной работе мы взяли исходный код ядра Linux версии 3.17.1, который распространяется по лицензии GNU GPL v2 (https://www.kernel.org). Данная лицензия разрешает использовать исходный код для изучения, модифицирования и свободного распространения.

За основу мы взяли стек TCP/IP v4, реализация которого находится в файлах с префиксом «tcp_».

Механизмы отправки, приема и повторной передачи описаны в файлах tcp_input.c, tcp_output.c, tcp_ip_v4.c, tcp.c. Для реализации описанной идеи мы изменили данные файлы, как описано ниже.

Так как данные при отправке и приеме сообщений передаются от уровня к уровню (application, transport, network, link), то для исключения постоянного копирования данных и служебной информации в реализации протокола TCP ядра linux существует основная структура sk_buff (определена в заголовочном файле skbuff.h) [3].

В структуре sk_buff мы определили указатель на хранение оригинального сообщения, которое будет заменяться стеганографическими данными: unsigned char *stored_data.

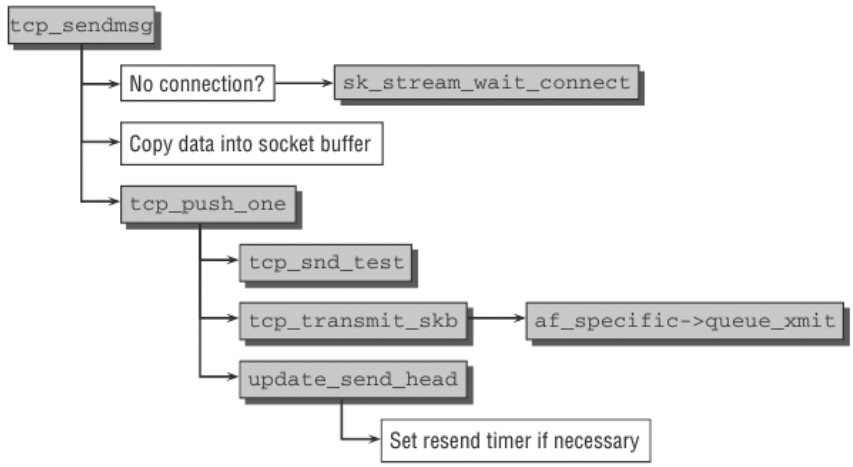


Рис. 3. Стек вызовов функций отправки сообщения

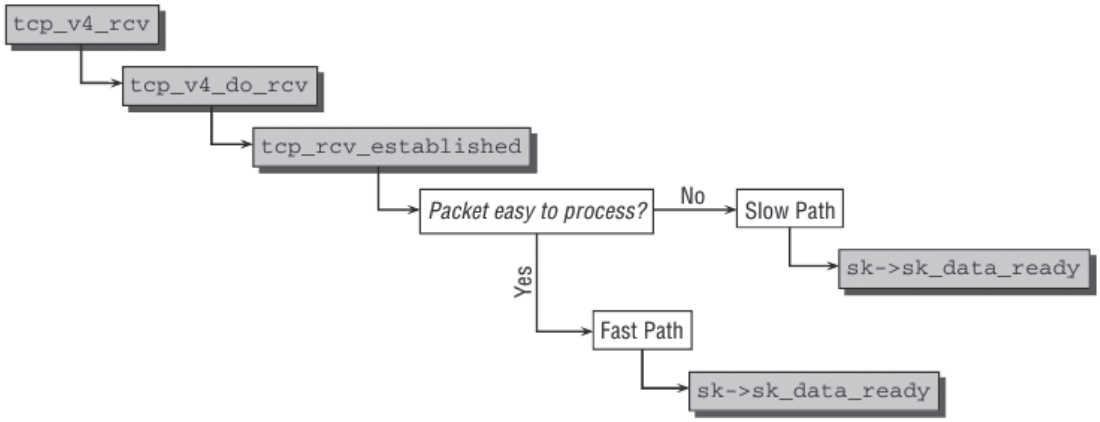


Рис. 4. Стек вызовов функций приема сообщения

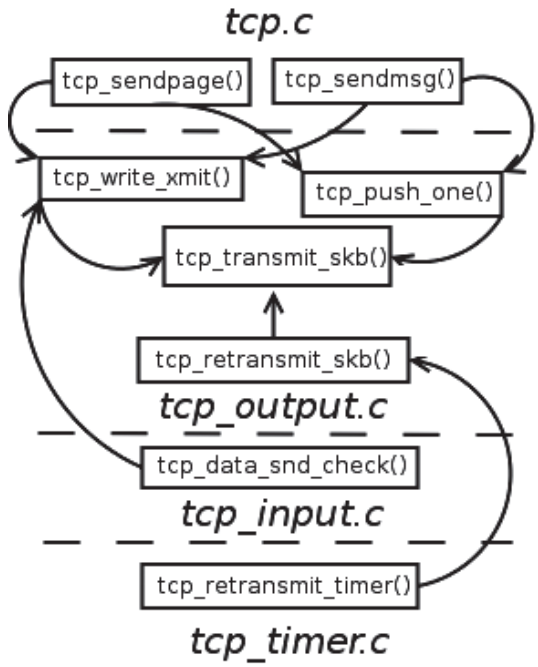


Рис. 5. Диаграмма работы механизма отправки сообщений протокола TCP

Для того чтобы модифицировать функции приема и передачи сообщений, рассмотрим, как они работают (рис. 3, рис. 4).

Так как протокол TCP является протоколом с гарантированной передачей данных, механизм отправки данного протокола является достаточно сложным. Чтобы правильно выбрать функцию отправки для модификации, рассмотрим диаграмму работы механизма отправки (рис. 5) [4].

Как видно из рис. 5, основной функцией для модификации отправки является функция tcp_transmit_skb(). В данной функции мы реализовали алгоритм отправки стеганографических сообщений.

Основной функцией приема является функция tcp_v4_rcv(). Мы модифицировали ее, добавив обработчик стеганографических сообщений.

Так как механизм RTO использует для повторной отправки функцию tcp_transmit_skb(), дополнительных изменений делать не нужно.

При модификации протокола важно сохранять его функциональность, чтобы не происходило потери пакетов. Потерей стеганографических пакетов на начальной стадии можно пренебречь.

Заключение

Описанная в данной работе реализация позволяет скрывать факт передачи сообщений, маскируясь под поврежденные сегменты, тем самым не изменяя логику работы TCP протокола. Однако данный метод не может полностью защитить от перехвата и подмены пакетов. Повысить защищенность передаваемых данных можно добиться использованием стеганографии в совокупности с криптографическими методами. В дальнейшем предполагается работа в данном направлении.

Примечания

1. Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission Steganography Applied, Poland: Warsaw University of Technology , 2010.

2. Transmission control protocol. Darpa internet program. Protocol specification. Defense Advanced Research Projects Agency, 1981.

3. Mauerer, W. Professional Linux® Kernel Architecture, Wiley Publishing, Inc, 2008.

4. How the Linux TCP output engine works // David S. Miller's Linux Networking Homepage. URL: http://vger.kernel.org/~davem/tcp_output.html (дата обращения 16.11.2014)

Токарчук Никита Александрович, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: nikita@tokarch.uk

Середкина Евгения Дмитриевна, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: vremendm@gmail.com

Зюляркина Наталья Дмитриевна, к. ф-.м. н., доцент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: toddeath@yandex.ru

Nikita Aleksandrovich Tokarchuk, student of South Ural State University. E-mail: nikita@tokarch.uk

Evgeniya Dmitrievna Seredkina, student of South Ural State University. E-mail: vremendm@gmail.com

Natalia Dmitrievna Ziuliarkina, Cand. Sc. Physics and Mathematics, associate professor of South Ural State University. E-mail: toddeath@yandex.ru

УДК 004.056.57

Фомин И. П., Маткин И. А.

ТЕХНОЛОГИЯ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ В КОНТЕКСТЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Технология аппаратной виртуализации предоставляет широкие возможности для программистов. Многие из этих возможностей интересны в контексте компьютерной безопасности. Целью данной работы является исследование технологии аппаратной виртуализации и выявление ее возможностей, применимых для решения задач в сфере компьютерной безопасности. В частности интересна возможность применения аппаратной виртуализации в руткитах. В результате проделанной работы были исследованы следующие возможности аппаратной виртуализации: контроль обращения к портам ввода вывода, возможность контроля таблицы страниц, а так же контроль обработки прерываний. Был разработан прототип руткита, использующего эти возможности для скрытного функционирования в системе и сбора информации.

Ключевые слова: *аппаратная виртуализация, руткит, гипервизор.*

Fomin I., Matkin I.

HARDWARE VIRTUALIZATION TECHNOLOGIES IN THE CONTEXT OF COMPUTER SECURITY

Tehnologiya hardware virtualization provides great opportunities for programmers. Many of the features of interest in the context of computer security. The aim of this work is to investigate hardware virtualization technology and the identification of its possible application to solve problems in the field of computer security. Particularly interesting possibility of using hardware virtualization rootkits. As a result of this work have been investigated following hardware virtualization: control access to ports of the output, the ability to control the page table, as well as control interrupt handling. Developed a prototype rootkit using these opportunities for covert operation of the system and gather information.

Keywords: *hardware virtualization, rootkit, hypervisor.*

На данный момент наиболее широкое распространение на рабочих станциях имеют две технологии аппаратной виртуализации: IntelVMXв процессорах семейства x86 от Intel, а так же AMD-V в процессорах AMDAthlon, которые появились в 2006 году.

Перед производителями процессоров были поставлены следующие требования:

1. Изоляция — каждая виртуальная машина должна иметь доступ только к тем ресурсам, которые были ей назначены. Она не должна иметь возможности повлиять на работы как монитора, так и других ВМ.

2. Эквивалентность — любая программа, исполняемая под управлением ВМ, должна демонстрировать поведение, полностью иден-

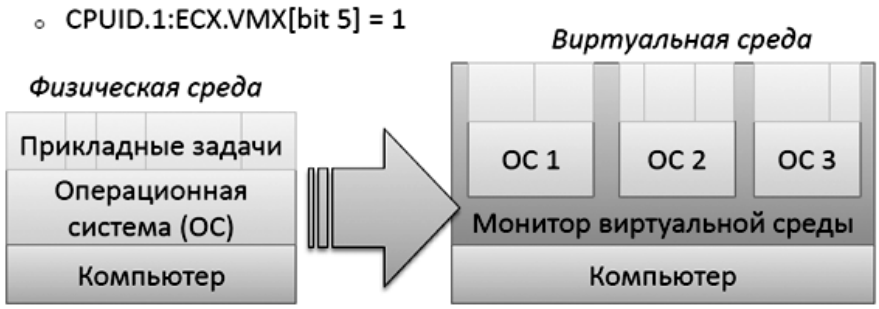


Рис. 1. Компьютер без гипервизора и с гипервизором

тичное её исполнению на реальной системе, за исключением эффектов, вызванных двумя обстоятельствами: различием в количестве доступных ресурсов (например, ВМ может иметь меньший объём памяти) и длительностями операций (из-за возможности разделения времени исполнения с другими ВМ).

3. Эффективность — в оригинальной работе условие сформулировано следующим образом: «статистически преобладающее подмножество инструкций виртуального процессора должно исполняться напрямую хозяйским процессором, без вмешательства монитора ВМ». Другими словами, значительная часть инструкций должна симулироваться в режиме прямого исполнения.

Идея работы аппаратной виртуализации заключена в работе монитора виртуальных машин (VMM) или гипервизора. Гиппервизор — это некий код имеющий уровень привилегий более высокий, чем уровень привилегий операционной системы, а так же неограниченный доступ к аппаратным ресурсам компьютера. При включении гипервизора на машине, все действия операционной системы начинают контролироваться гипервизором. Схематично это изображено на рис. 1.

Из этого следует, что аппаратная виртуализация предоставляет программистам широкий спектр воздействия на систему в самом привилегированном режиме. Это предоставляет очень мощную возможность для сокрытия вредоносного программного обеспечения.Так, с одной стороны, гипервизор, выполняющий функции монитора виртуальных машин, повышает сервисные возможности компьютера и снижает его эксплуатационные расходы. Благодаря монитору виртуальных машин на одном компьютере может быть одновременно запущено несколько ОС в разных виртуальных машинах. Но, с другой стороны, гипервизор можно негласно внедрить как программную закладку несущую угрозу информационной безопасности.



Рис. 2. Схема внедрения нелегитимного гипервизора

Далее рассмотрим интересные в контексте компьютерной безопасности возможности аппаратной виртуализации. Аппаратная виртуализация предоставляет средство контроля обращений к портам, то есть контролируются команды типа IN, INS/INSB/INSW/INSD, OUT, OUTS/OUTSB/OUTSW/OUTSD. Суть этого заключается в перехвате управления гипервизором в случае выполнения операций с портами из непривилегированного режима (в данном контексте привилегированным является режим работы гипервизора, а непривилегированный — пользовательский и режим ядра операционной системы). Из этого следует возможность контроля за операциями ввода и вывода, а также способ контроля взаимодействия программного кода с аппаратным обеспечением. Сказанное выше к примеру предоставляет возможность перехвата управления гипервизором в случае нажатия клавиши. В последствии в зависимости от логики работы гипервизора это событие можно обработать разными способами: можно сохранять нажатую клавишу, подменять код нажатой клавиши, либо скрывать нажатие клавиш. По такому принципу был разработан прототип руткита, представляющий драйвер режима ядра, который после загрузки в систему устанавливает гипервизор, регистрирует обработчики и использует специализированную команду для запуска гипервизора. Суть работы заключается в следующем: при регистрации гипервизора есть способ установить контроль обращений к портам ввода вывода путем установки определенного бита в единицу. Далее указывается гипервизору номер порта для контроля, в данном случае это порт с номером 0x60. В случае, если после установки контроля за портом, отвечающим за клавиатуру, пользователь станет вводить с клавиатуры какие-либо символы, управление перейдет к гипервизору, который сохраняет код нажатой клавиши и возвращает управление пользователю. Все это происходит незаметно для пользователя и антивирусных средств, так как гипервизор напрямую работает с процессором. Схематично этот процесс можно изобразить блок схемой (Рис. 3).

Контроль прерываний. Суть контроля прерываний заключается в перехвате гипервизором управления в случае прерываний, а также установка своих обработчиков для обработки прерываний. Данное средство позволяет перехватывать все виды прерываний, как программные, так и аппаратные. Например, мы имеем способ контроля исключений при обращении к выгруженной странице памяти. Эта возможность предоставляет нам интересный способ контроля операций обращения к памяти. Механизм этого состоит в отключении некоторых областей памяти путем выставления определенных битов, отвечающих за их работу, в нуль. Это вызывает, в случае обращения к соответствующим страницам, возникновение аппаратного прерывания, так как происходит обращение к недоступной памяти. После этого управление получает гипервизор. Подобная функциональность была реализована в прототипе руткита, для обеспечения сокрытия

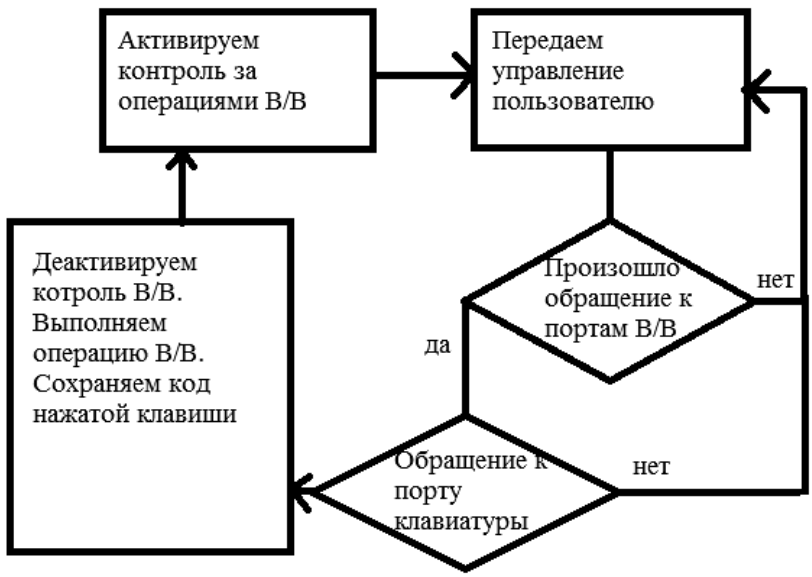


Рис. 3. Блок-схема алгоритма перехвата

руткита в системе. То есть, сокрытие происходит в том случае, если обращение на чтение к области памяти руткита происходит не из кода руткита, а за его пределами. Реализовано это было следующим образом. В гипервизоре устанавливается поддержка контроля прерываний. Далее в таблице страниц, обнуляется бит присутствия соответствующих страниц, чтобы при обращении к областям памяти, где расположен руткит, происходило прерывание, и управление получал гипервизор. В случае возникновения исключения управление передается обработчику гипервизора, в котором происходит проверка, какая операция вызвала исключение. Если это была операция чтения или записи, проверяется адрес инструкции, вызвавшей исключение. Если инструкция принадлежит коду руткита, то выставляется флаг трассировки в гипервизоре, так же бит присутствия страниц руткита вновь выставляется в единицу и управление передается коду, вызвавшему исключение. Далее благодаря установленному флагу трассировки, после выполненной инструкции управление вновь получает гипервизор, который снова устанавливает соответствующие биты присутствия страниц в нули, чтобы не пропустить последующие обращения к областям памяти руткита, снимается флаг трассировки и управление передается пользовательскому процессу. Если инструкция чтения / записи принадлежит не коду руткита, то необходимо скрыть код руткита от нежелательных действий. В данном случае происходит сохранение кода руткита в буфер и заполнение соответствующих руткиту областей памяти нулями. Далее происходит установка бита присутствия страниц в единицу, установка флага трассировки и передача управления вызвавшему исключение коду. После выполнения вызвавшей исключение инструкции код, вызвавший данную инструкцию, получит нули, и управление вновь перейдет к гипервизору, который вновь выставит биты присутствия в нули и снимет флаг трассировки. В случае если была инструкция передачи управления, то биты присутствии выставляются в единицу, выставляется флаг трассировки и управление получает руткит. Таким образом, блокируется внешнее воздействие на код руткита, не мешая деятельности руткита.

В заключении скажем, что поставленные задачи в данной работе были выполнены. В ходе работы были рассмотрены и изучены две интересные возможности аппаратной виртуализации в контексте компьютерной безопасности. Рассмотренные задачи и реализованные прототипы руткита впоследствии могут иметь применение для написания средств обнаружения руткитов. В будущем планируется рассмотрение других интересующих возможностей аппаратной виртуализации. А также планируется рассмотрение методов противодействия этому и написание антируткита.

Примечания

1. Intel® 64 and IA-32 Architectures Software Developer's Manual: в 3 т. //ОфициальныйсайтIntel. URL: http://http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-vol-1-manual.pdf

2. Gerhart. Примеры использования функциональности аппаратной виртуализации процессоров Intel для реализации Anti-VmDetect для Vmware[электронный ресурс]. – Электронные текстовые данные. - Режим доступа http://www.securitylab.ru/analytics/427855.php, свободный.

3. Методика обнаружения нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации [Текст] :автореф. дис. ... канд. техн. наук : 05.13.19 / И. Ю. Коркин. - М., 2011. - 21 с. : ил. - Библиогр.: с. 20-21

4. Александр Самойленко. Технологии аппаратной виртуализации[электронный ресурс]. – Электронные текстовые данные. – Режим доступа http://www.ixbt.com/cm/virtualization-h.shtml, свободный.

Фомин Игорь Павлович, студент, Челябинский государственный университет. E-mail: kraken_pro@mail.ru

Маткин Илья Александрович, ст. преподаватель, Челябинский государственный университет

Fomin Igor Pavlovich, student, Chelyabinsk State University. E-mail: kraken_pro@mail.ru

Matkin Ilya Alexandrovich, senior lecturer, Chelyabinsk State University

УДК 004.056 + 519.151 + 004.072.4

Сорокина С. В., Титов С. С.

МАТРОИДЫ, ДВОЙСТВЕННЫЕ К БИНАРНЫМ, И ИХ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Необходимость защиты информации от хищения или несанкционированной модификации порождает необходимость распределения прав доступа к ней. Грамотное разграничение доступа к информации подразумевает, что неразрешённая группа участников не получает никакой информации о секрете, а любая разрешённая – может его однозначно восстановить. В данной статье высказана гипотеза, которая в этой статье будет проверяться на примере матроида Фано, а затем в ходе дальнейших исследований и на других матроидах.

Ключевые слова: *информационная безопасность, матроиды, цикл матроида, базис матроида, идеальная схема разделения секрета, структура доступа.*

Sorokina S. V., Titov S. S.

MATROIDS DUAL TO BINARY ONES AND THEIR SECRET SEPARATION SCHEMES

The need to protect information from theft or unauthorized modification necessitates the sharing of rights of access to it. Proper differentiation of access to information means that the group of unpermitted participants gets no information about the secret, and any permitted one can restore it. The article dwells on the hypothesis which is going to be proved on the example of Fano matroid, as well as in the course of further research and other matroids.

Keywords: *information security, matroids, matroid cycle, matroid basis, ideal secret separation scheme, access structure.*

Реализация структур доступа на основе схем разделения секрета в настоящее время осуществляется на основе матроидов. Другими словами, по идеальной схеме разделения секрета можно построить матроид. Вопрос, можно ли, имея матроид, построить по нему схему разделения секрета, остаётся открытым до сих пор.

Мы предполагаем, что это возможно, и для этих целей рассматриваем матроид Фано, представимый как векторный над конечным полем GF(2), иначе говоря, бинарный матро-

ид. По нашей гипотезе, матрица идеальной схемы разделения секрета будет представлять собой матрицу циклов двойственного матроида. Для подтверждения этой гипотезы построим схему разделения секрета по матроиду Фано.

Матроид – это такая пара (X, I), где X – конечное множество, называемое **носителем матроида**, а I – некоторое множество подмножеств X, называемое семейством **независимых множеств**, то есть $I \in 2^X$. При этом должны выполняться следующие условия:

1) $\varnothing \in I$;

2) если $A \in I$ и $B \subset A$, то $B \in I$;

3) если $A, B \in I$ и $|A| > |B|$,
то $\exists x \in A \setminus B : B \cup \{x\} \in I$.

База матроида — максимальное по включению независимое множество.

Зависимое множество — подмножество носителя матроида, не являющееся независимым.

Матроид представим над полем F, если он изоморфен некоторому векторному матроиду над этим полем. Если матроид представим над любым полем, его называют регулярным. Матроид, который является представимым над двухэлементным полем $GF(2)=\{0,1\}$ (полем называют множество элементов, на котором определены две операции: сложение и умножение, даже если эти операции не являются обычными операциями сложения и умножения, а также вычитание и деление – на любой ненулевой элемент), называется бинарным матроидом. Матроид, представимый над полем $GF(3)=\{0,1,2\}$ из трёх элементов, называется тернарным матроидом.

Цикл матроида — минимальное по включению зависимое множество. Семейство циклов часто обозначается буквой C.

Двойственным матроидом называется матроид, носитель которого совпадает с носителем данного матроида, а базы – дополнения баз данного матроида до носителя, т. е. $X^*=X$, а множество баз двойственного матроида – это множество таких B^*, что $B^*=X\setminus B$, где B – база данного матроида.

Предположим, что матрица G идеальной схемы разделения секрета с матроидом M определяется двойственным матроидом M* через список его циклов как список его зависимых множеств. Следовательно, если матроид M представим над конечным полем F, то M* задаёт порождающую матрицу G линейного над полем F кода с проверочной матрицей H, задаваемой циклами матроида M, этот код и есть код этой СРС.

Для проверки этой гипотезы рассмотрим бинарный матроид на примере матроида Фано.

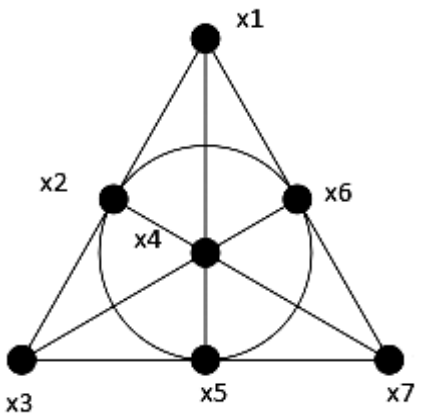


Рис. 1. Матроид Фано

Для матроида Фано носителем матроида является семиэлементное множество $X=\{x_1, \ldots, x_7\}$, элементы которого можно параметризовать битами (элементами поля $GF(2)=\{0,1\}$):

1) $\vec{i} = (1,0,0) = x_1$;
2) $\vec{j} = (0,1,0) = x_3$;
3) $\vec{k} = (0,0,1) = x_7$;
4) $\vec{i} + \vec{j} = (1,1,0) = x_2$;
5) $\vec{j} + \vec{k} = (0,1,1) = x_5$;
6) $\vec{i} + \vec{k} = (1,0,1) = x_6$;
7) $\vec{i} + \vec{j} + \vec{k} = (1,1,1) = x_4$.

Выпишем циклы матроида Фано, состоящие из 3 элементов (см. рис. 1, на котором трёхэлементные циклы соответствуют отрезкам и окружности):

1) x_1, x_2, x_3;
2) x_3, x_5, x_7;
3) x_1, x_6, x_7;
4) x_2, x_4, x_7;
5) x_6, x_4, x_3;
6) x_5, x_4, x_1;
7) x_2, x_5, x_6.

и циклы, состоящие из четырёх элементов:

1) x_2, x_3, x_6, x_7;
2) x_1, x_3, x_7, x_4;
3) x_1, x_2, x_5, x_7;
4) x_1, x_2, x_4, x_6;
5) x_1, x_3, x_5, x_6;
6) x_4, x_5, x_6, x_7;
7) x_2, x_3, x_4, x_5.

Если записать все вершины ($x_1, x_2, x_3, x_4, x_5, x_6, x_7$) матроида Фано в строчку, а под ними записывать все циклы, ставя единицу напротив вершины, через которую данный цикл проходит, и нуль в противном случае, то получится таблица циклов матроида Фано.

Таблица 1

№ строки	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	1	1	1	0	0	0	0
2	0	0	1	0	1	0	1
3	1	0	0	0	0	1	1
4	0	1	0	1	0	0	1
5	0	0	1	1	0	1	0
6	1	0	0	1	1	0	0
7	0	1	0	0	1	1	0
8	0	1	1	0	0	1	1
9	1	0	1	1	0	0	1
10	1	1	0	0	1	0	1
11	1	1	0	1	0	1	0
12	1	0	1	0	1	1	0
13	0	0	0	1	1	1	1
14	0	1	1	1	1	0	0

Данная таблица представляет собой матрицу H, в которой строка 1 дополняется строкой 13; строка 2–11; строка 3–14; строка 4–12; строка 5–10; строка 6–8 и строка 7–9.

Мы выбираем в качестве базиса множество (x_1, x_3, x_7), поскольку элементы x_1, x_3, x_7 образуют знакомый всем базис $\{i, j, k\}$ векторного пространства. И если добавить к базису элемент x_2, то увидим, что во множестве $\{x_1, x_2, x_3, x_7\}$ содержится единственный трёхэлементный цикл $\{x_1, x_2, x_3\}$, а цикла в цикле быть не может. Если мы добавим к базе элемент x_4, то получим $\{x_1, x_3, x_4, x_7\}$ – цикл, который уже есть в таблице циклов, а цикл не может быть базисом. Если мы добавим к базе элемент x_5, то получим $\{x_1, x_3, x_5, x_7\}$, где содержится единственный трёхэлементный цикл $\{x_7, x_5, x_3\}$, а если добавим x_6, то получим $\{x_1, x_3, x_6, x_7\}$, где содержится единственный трёхэлементный цикл $\{x_1, x_6, x_7\}$, а цикла в цикле быть не должно. Таким образом, $\{x_1, x_3, x_7\}$ – базис матроида Фано, следовательно, ранг матроида Фано равен трём. Составим таблицу схемы разделения секрета по нашему базису.

Под **разделением секрета** понимают любой метод распределения секрета среди группы участников, каждому из которых достается доля секрета. Секрет потом может воссоздать только разрешённая коалиция участников, а неразрешённая коалиция никакой информации о секрете не получает.

Сопоставим $x_1 \to S_1$, $x_2 \to S_2$, $x_3 \to S_3$ и так далее и выразим через базис остальные элементы, получив $S_2=S_1+S_3$, $S_5=S_3+S_7$, $S_6=S_1+S_7$, $S_4=S_1+S_3+S_7$.

Построим таблицу схемы разделения секрета (СРС), перебрав все возможные сочетания базиса (в левой части таблицы), т.е. элементов S_1, S_3, S_7. Поскольку поле двоичное, а базис состоит из 3 элементов, то вариантов сочетаний будет всего 8. Заполним правую часть таблицы для всех элементов матроида: S_1 берём из левой части таблицы; S_2 вычисляем как S_1+S_3; S_3 снова берём из левой части таблицы; S_4 вычисляется как $S_1+S_3+S_7$; S_5 – это S_3+S_7; S_6 – S_1+S_7; S_7 берём из левой части таблицы. Все операции сложения выполняются по модулю 2.

Таблица 2

S_1	S_3	S_7	S_1	S_2	S_3	S_4	S_5	S_6	S_7
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	1	1	1
0	1	0	0	1	1	1	1	0	0
0	1	1	0	1	1	0	0	1	1
1	0	0	1	1	0	1	0	1	0
1	0	1	1	1	0	0	1	0	1
1	1	0	1	0	1	0	1	1	0
1	1	1	1	0	1	1	0	0	1

Для подтверждения того, что таблица СРС матроида Фано является матрицей циклов матроида, двойственного матроиду Фано, построим таблицу, в которой перечислим все базы и кобазы матроида Фано.

Таблица 3

Базы	Кобазы	Базы	Кобазы	Базы	Кобазы
$\{x_1, x_2, x_4\}$	$\{x_3, x_5, x_6, x_7\}$	$\{x_5, x_6, x_1\}$	$\{x_2, x_3, x_4, x_7\}$	$\{x_2, x_3, x_6\}$	$\{x_1, x_4, x_5, x_7\}$
$\{x_1, x_2, x_5\}$	$\{x_3, x_4, x_6, x_7\}$	$\{x_1, x_3, x_5\}$	$\{x_2, x_4, x_6, x_7\}$	$\{x_2, x_3, x_7\}$	$\{x_1, x_4, x_5, x_6\}$
$\{x_1, x_2, x_6\}$	$\{x_3, x_4, x_5, x_7\}$	$\{x_1, x_3, x_7\}$	$\{x_2, x_4, x_5, x_6\}$	$\{x_3, x_4, x_5\}$	$\{x_1, x_2, x_6, x_7\}$
$\{x_1, x_2, x_7\}$	$\{x_3, x_4, x_5, x_6\}$	$\{x_2, x_4, x_6\}$	$\{x_1, x_3, x_5, x_7\}$	$\{x_3, x_4, x_7\}$	$\{x_1, x_2, x_5, x_6\}$
$\{x_2, x_3, x_4\}$	$\{x_1, x_5, x_6, x_7\}$	$\{x_1, x_4, x_7\}$	$\{x_2, x_3, x_5, x_6\}$	$\{x_3, x_4, x_1\}$	$\{x_2, x_5, x_6, x_7\}$
$\{x_2, x_3, x_5\}$	$\{x_1, x_4, x_6, x_7\}$	$\{x_1, x_5, x_6\}$	$\{x_2, x_3, x_4, x_7\}$	$\{x_1, x_5, x_7\}$	$\{x_2, x_3, x_4, x_6\}$
$\{x_2, x_4, x_6\}$	$\{x_1, x_2, x_3, x_7\}$	$\{x_3, x_5, x_6\}$	$\{x_1, x_2, x_4, x_7\}$	$\{x_4, x_5, x_7\}$	$\{x_6, x_1, x_2, x3\}$
$\{x_4, x_5, x_6\}$	$\{x_7, x_1, x_2, x_3\}$				

Если к каждой базе добавлять поочерёдно элементы из списка соответствующих кобаз, то получатся циклы матроида, двойственного матроиду Фано:

1) $\{x_1, x_2, x_5, x_7\}$;
2) $\{x_2, x_3, x_4, x_5\}$;
3) $\{x_1, x_3, x_5, x_6\}$;
4) $\{x_1, x_2, x_4, x_6\}$;
5) $\{x_2, x_3, x_6, x_7\}$;
6) $\{x_1, x_3, x_4, x_7\}$;
7) $\{x_4, x_5, x_6, x_7\}$.

Если выписать из правой части таблицы 2 те элементы, значение которых равно единице, и обозначить их не S_1, S_2 и т. д., а x_1, x_2 и т. д., то мы получим те же самые циклы матроида, двойственного матроиду Фано.

Таким образом получается, что таблица 2 представляет собой выколотый код Рида – Маллера схемы разделения секрета. В то же время эта таблица является матрицей G, т. е. матрицей циклов матроида, двойственного матроиду Фано.

Если дальнейшая проверка гипотезы на матроидах, представимых как векторные над $GF(3)$ и $GF(q)$, а также на других матроидах, о возможности построения идеальной схемы разделения секрета по циклам двойственного матроида подтвердит её справедливость, то задачу можно будет считать решённой.

Примечания

1. Алексейчук А. Н., Бояринова Ю. Е. Модулярная схема разделения секрета над кольцом гауссовых целых чисел // Реєстрація, зберігання і обробка даних. - Т. 9, № 1, 2007. – С. 87–99.

2. Аникевич Е. А., Еремеев М. А., Корниенко А. А. Высокоскоростные алгоритмы и протоколы криптографической защиты информационных ресурсов железнодорожного транспорта // Известия Петербургского университета путей сообщения. – Вып. 2. – СПб.: ПГУПС, 2004. – С. 85–88.

3. Асанов М. О., Баранский В. А., Расин В. В. Дискретная математика: графы, матроиды, алгоритмы. - Ижевск: НИЦ «Регулярная и хаотическая динамика, 2001. – 288 с.

4. Введение в криптографию / под общ. ред. В. В. Ященко. - СПб.: Питер, 2001. - 288 с.

Сорокина Светлана Викторовна, аспирант, Уральский государственный университет путей сообщения, г. Екатеринбург. E-mail: sorokina@ifsusu.ru

Титов Сергей Сергеевич, д. ф.-м. н., профессор, Уральский государственный университет путей сообщения. E-mail: stitov@usaaa.ru

Svetlana Viktorovna Sorokina, PhD student of Ural State University of Railway Transport, Yekaterinburg. E-mail: sorokina@ifsusu.ru

Sergey Sergeevich Titov, PhD Physics and Mathematics, Professor of Ural State University of Railway Transport. E-mail: stitov@usaaa.ru

УДК 512.54 + 003.26 + 004.056.55

Сурина А. А., Зюляркина Н. Д.

РЮКЗАЧНАЯ КРИПТОСИСТЕМА НА ОСНОВЕ ПРЯМОГО ПРОИЗВЕДЕНИЯ ДИЭДРАЛЬНЫХ ГРУПП

В статье рассматривается задача о мультипликативном рюкзаке с использованием диэдральных групп. Предложена математическая модель рюкзачной системы на основе прямого произведения диэдральных групп, которая оказалась криптостойкой к атаке методом полного перебора. Приведен пример выполнения шифрования/дешифровки сообщения с использованием предложенной математической модели.

Ключевые слова: *криптосистема, рюкзачная схема, группа, порождающий элемент, мультипликативный рюкзак.*

Surina A. A., Ziuliarkina N. D.

KNAPSACK PUBLIC KEY CRYPTOSYSTEM ON THE BASIS OF DIRECT PRODUCT OF DIHEDRAL GROUPS

The article deals with the problem of multiplicative knapsack with dihedral groups. A mathematical model of knapsack system based on direct product of dihedral groups is proposed; it was proved to be cryptographically resistant to the full enumeration method attack. The authors give examples of the encryption/decryption of key message with the use of proposed mathematical model.

Keywords: *cryptosystem, knapsack system, group, generating element, multiplicative knapsack.*

Усовершенствование технических средств требует постоянных изменений параметров системы, отвечающей за конфиденциальность информации. В связи с этим часто стали использоваться криптосистемы с открытым ключом: криптосистемы, основанные на задаче факторизации (RSA) и задаче нахождения дискретного логарифма (схема Эль-Гамаля). Но возникающие сложности при их использовании вынуждают искать задачи достаточно гибкие и позволяющие вводить новые варианты для преодоления криптографических слабостей.

Рюкзачные схемы очень удобны для иллюстрации основных идей криптографии с открытым ключом. Задача об укладке рюкзака является NP-полной, следовательно, созданная на ее основе система будет лучше и

быстрее, чем системы на основе целочисленной факторизации и дискретного логарифмирования.

Идея мультипликативного рюкзака была предложена в 1988 Масакацу Мории (Masakatu Morii) и Масао Касахара (Masao Kasahara). Мультипликативный рюкзак использует точно такую же функцию шифрования, как и у аддитивной рюкзачной схемы Меркля – Хеллмана.

Алгоритм построения открытого ключа

1. Выбирается n взаимно простых чисел ($p_1, p_2, \ldots, p_n$).

2. Выбирается некоторое простое число q, такое, что q-1 раскладывается на маленькие простые множители так, что

$$q > \prod_{i=1}^{n} p_i \qquad (1)$$

3. Выбирается некоторый примитивный корень $b(\mathrm{mod}\ q)$.

4. Затем находятся такие a_i $(1 < a_i < q-1)$, что: $p_i = b^{a_i} \pmod q$. a_i – дискретный логарифм от p_i по основанию $b(\mathrm{mod}\ q)$.

Зашифрованное сообщение будет выглядеть так:

$$S = \sum_{i=1}^{n} x_i \cdot a_i,$$

где x_i – n-битный вектор исходного сообщения.

Дешифрование происходит по следующей формуле:

$$S' = b^S \bmod q,$$

так как $b^S = b^{\sum x_i a_i} = \prod b^{x_i a_i} = \prod b_i^{x_i} \bmod q.$

Последнее равенство – результат условия (1).

Закрытым ключом является (b, q), открытый ключ – a_i. Затем можно легко найти соответствующий x, начинающийся с S', используя тот факт, что числа p_i взаимно простые [6]. Это очень важно, так как в общем случае задача о произведении подмножеств NP-полная.

Для рюкзака Мории – Касахара в настоящее время неизвестно эффективного способа взлома.

Задачу о мультипликативном рюкзаке можно модифицировать, взяв в качестве элементов рюкзака элементы прямого произведения диэдральных групп.

Пусть D_{2n} – *диэдральная группа порядка* $2n$, такая, что $D_{2n} = a, b$, где $a^2 = e$, $b^n = e$, и выполняется соотношение

$$a^{-1}ba = aba = b^{-1}. \qquad (2)$$

Если $d = a^x b^y$ – элемент диэдральной группы D_{2n}, существует алгоритм нахождения показателей x и y.

Математическая модель рюкзачной системы на основе прямого произведения диэдральных групп

Пусть $G = a, b = D_{2n}$ – диэдральная группа.

Тогда можно рассмотреть следующую рюкзачную систему, основанную на вычисления в диэдральной группе.

Генерация ключей

1. Сообщение шифруется двоичной последовательностью (можно использовать двоичные ASCII-коды символов латинского алфавита). Затем последовательность разбивается на блоки, длина которых равна количеству элементов в рюкзаке.

2. Секретный ключ задается следующим образом:

2.1. для группы $D_{2(q-1)}$

$$g_1' = \begin{pmatrix} \alpha_1 & 0 & \ldots & \ldots \\ 0 & \alpha_1^{-1} & \ldots & \ldots \\ \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & 0 & 1 \end{pmatrix}, \quad g_1'' = \begin{pmatrix} 0 & 1 & \ldots & \ldots \\ 1 & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & 0 & 1 \end{pmatrix}, \ldots, g_n' = \begin{pmatrix} 1 & 0 & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \alpha_n & 0 \\ \ldots & \ldots & 0 & \alpha_n^{-1} \end{pmatrix}, g_n'' = \begin{pmatrix} 1 & 0 & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots \\ \ldots & \ldots & 0 & 1 \\ \ldots & \ldots & 1 & 0 \end{pmatrix}$$

где: $b_1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1^{-1} \end{pmatrix}$, $b_2 = \begin{pmatrix} \alpha_2 & 0 \\ 0 & \alpha_2^{-1} \end{pmatrix}$, $a_1 = a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и так далее.

Для удобства вычислений можно выбрать $\alpha_1 = \alpha_2 = \ldots = \alpha_n$.

2.2. для группы $D_{2(q+1)}$

$$g_1^{'}=\begin{pmatrix} a & b & \dots & \dots \\ \alpha b & a & \dots & \dots \\ \dots & \dots & \dots & 0 \\ \dots & \dots & 0 & 1 \end{pmatrix},\ g_1^{''}=\begin{pmatrix} 0 & 1 & \dots & \dots \\ 1 & 0 & \dots & \dots \\ \dots & \dots & \dots & 0 \\ \dots & \dots & 0 & 1 \end{pmatrix},\dots,g_n^{'}=\begin{pmatrix} 1 & 0 & \dots & \dots \\ 0 & \dots & \dots & \dots \\ \dots & \dots & c & d \\ \dots & \dots & \alpha d & c \end{pmatrix},g_n^{''}=\begin{pmatrix} 1 & 0 & \dots & \dots \\ 0 & \dots & \dots & \dots \\ \dots & \dots & 0 & 1 \\ \dots & \dots & 1 & 0 \end{pmatrix}$$

Таких матриц получается столько, сколько элементов в рюкзаке.

3. Формируется рюкзак-ловушка $(\delta_1^{'},\delta_1^{''},\delta_2^{'},\delta_2^{''},\dots)$, который и является открытым ключом.

При этом $\delta_i^{'},\delta_i^{''}$ формируются следующим образом: $\delta_i^{'}=\left(g_i^{'}\right)^x$, $\delta_i^{''}=\left(g_i^{''}\right)^x$, где $x\in GL_{2n}(q)$. При этом x подбирается такой, что матрица будет иметь не диагональный вид, а общий.

Алгоритм шифрования

1. Блоки открытого текста, которые представлены в виде матрицы, возводятся в соответствующую степень (0 – получаем единичную матрицу, или 1 – получаем саму матрицу).

2. Перемножаем те матрицы, которые возводили в степень 1:

$$S=\prod_{i=1}\delta_i^{k_i}$$

Алгоритм дешифровки

1. Вычисляем $\gamma_i=\left(\delta_i^{k_i}\right)^{x^{-1}}$. Получим матрицу, которая будет иметь диагональный вид.

2. Разбиваем матрицу на блоки 2×2. Каждый блок будет элементом диаэдральной группы.

3. Относительно каждого блока применяем алгоритм нахождения показателей в диэдральной группе, при этом учитывая четность n. Таким образом, находится матрица исходного текста.

Пример 1. Рассмотрим группу $G=GL_2(5)$ и выберем в ней элементы

$$b=\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix},\ a=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

где α – примитивный элемент поля F_5, $\alpha=2$, $\alpha^{-1}=3$.

Тогда элементы секретного ключа задаются следующим образом:

$$g_1^{'}=\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ g_1^{''}=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ g_2^{'}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},\ g_2^{''}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Заметим, что $\left\langle g_1^{'},g_1^{''},g_2^{'},g_2^{''}\right\rangle$ является прямым произведением подгрупп $G'=\left\langle g_1^{'},g_1^{''},g_2^{'},g_2^{''}\right\rangle=\left\langle g_1^{'},g_1^{''}\right\rangle\left\langle g_2^{'},g_2^{''}\right\rangle$

Выберем в качестве маскирующего изоморфизма сопряжение посредством $x\in GL_4(5)$:

$$x=\begin{pmatrix} 2 & 0 & 0 & 2 \\ 4 & 3 & 2 & 4 \\ 3 & 1 & 3 & 3 \\ 3 & 4 & 3 & 4 \end{pmatrix}.\ \text{Заметим, что } x^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 0 \\ 0 & 2 & 4 & 0 \\ 2 & 3 & 2 & 1 \end{pmatrix}.$$

Вычислим набор $((g_1^{'})^x,(g_1^{''})^x,(g_2^{'})^x,(g_2^{''})^x)$, который будет являться открытым ключом:

$$(g_1^{'})^x=\begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 0 & 1 & 4 \\ 1 & 2 & 4 & 1 \\ 3 & 3 & 2 & 4 \end{pmatrix},\ (g_1^{''})^x=\begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix},\ (g_2^{'})^x=\begin{pmatrix} 4 & 0 & 3 & 1 \\ 2 & 0 & 2 & 2 \\ 2 & 4 & 3 & 2 \\ 2 & 0 & 2 & 0 \end{pmatrix},(g_2^{''})^x=\begin{pmatrix} 1 & 2 & 0 & 4 \\ 0 & 3 & 0 & 4 \\ 0 & 2 & 1 & 4 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

Зашифруем в данной системе сообщение OK (0100111101001011).

Так как у нас рюкзак размером 4 x 4, то делим двоичный код сообщения на блоки по 4 символов: (0100), (1111), (0100), (1011). Далее следуем алгоритму шифрования, указанному выше.

В итоге получим зашифрованные блоки S_i:

$$S_1 = (g_1')^0 (g_1'')^1 (g_2')^0 (g_2'')^0 = \begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix} \qquad S_2 = (g_1')^1 (g_1'')^1 (g_2')^1 (g_2'')^1 = \begin{pmatrix} 4 & 2 & 3 & 0 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix}$$

$$S_3 = (g_1')^0 (g_1'')^1 (g_2')^0 (g_2'')^0 = \begin{pmatrix} 4 & 2 & 3 & 3 \\ 4 & 2 & 4 & 4 \\ 1 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \end{pmatrix} \qquad S_4 = (g_1')^1 (g_1'')^0 (g_2')^1 (g_2'')^1 = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 3 & 3 & 4 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 4 & 4 \end{pmatrix}$$

Для дешифровки сообщения S найдем элемент γ:

$$\gamma_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ \gamma_2 = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}, \ \gamma_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}, \ \gamma_4 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

Получили блочно-диагональные матрицы.

Применяя соответствующие алгоритмы, описанные выше, находим показатели элементов диэдральной группы:

$$b' = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}, \quad (b^2)' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$x = 1, b' = ab^y \Rightarrow (b')^{-1} = a^{-1}b' = b^y$$

$$a^{-1}b' = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}^y, \text{ откуда } y=1.$$

Тогда элемент сообщение, соответствующее элементу γ_1, дешифруется как (0100).

Аналогично дешифруем сообщения, соответствующие γ_2, γ_3, γ_3, и получаем сообщения (1111), (0100), (1011). Выписываем сообщения в строчку и по таблице двоичных кодов символов латинского алфавита находим соответствующие буквы. При этом учитываем, что в таблице 1 символ представлен восьмиразрядной двоичной записью:

$$(0100111101001011) \rightarrow (01001111 \,|\, 01001011) \rightarrow \text{OK}.$$

Примечания

1. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory, V. TI-22, 1977, pp. 644–654.

2. Саломаа А. Криптография с открытым ключом // М.: Мир, 1995. С. 318.

3. Hellman M. E. The Mathematics of Public-Key Cryptography // Scientihc American, V. 241, № 8, Aug 1982, pp.146–157.

4. Merkle R. C., Hellman M. E. Hiding information and signatures in Trapdoor Knapsack // IEEE Transactions on Information Theory, V. 24, № 5, Sep. 1978, pp. 525–530.

5. Харин Ю. С., Берник В. И., Матвеев Г. В. Математические основы криптологии : учебное пособие // Мн.: БГУ, 1999. С. 319.

6. Henk C. A. van Tilborg. Encyclopedia of Cryptography and Security // Science, 2005, 697 p.

7. Harris M. E. Finite groups containing an intrinsic 2-component of Chevalley type over field of odd order // Transactions of the American math.soc. V. 272, № 1, 1982, pp. 1–65.

Сурина Альфия Адгамовна, аспирант, Южно-Уральский государственный университет,(г. Челябинск). E-mail: dallila87@mail.ru

Зюляркина Наталья Дмитриевна, к. ф.-м. н., доцент, Южно-Уральский государственный университет,(г. Челябинск).

Alfiya Adgamovna Surina, PhD student of South Ural State University. E-mail: dallila87@mail.ru

Natalia Dmitrievna Ziuliarkina, Cand. Sc. Physics and Mathematics, associate professor of South Ural State University.

УДК 519.175.1

Горяинов С. В., Исакова Г. С.

СВЯЗНОСТЬ ВТОРОЙ ОКРЕСТНОСТИ В КОРЕБЕРНО-РЕГУЛЯРНЫХ ГРАФАХ ДЕЗА

В работе классифицированы кореберно-регулярные графы Деза с несвязной второй окрестностью. В целом решена классическая задача комбинаторики и теории графов, в частности, перечисление комбинаторных объектов с заданными свойствами. Изучение графов Деза представляет интерес в связи с тем, что графы Деза имеют диаметр 2 и являются естественным обобщением сильно регулярных графов. Для данного класса графов проблема проверки изоморфизма представляется потенциально сложной. Предложенный в работе подход, возможно, позволит обобщить полученные результаты.

Ключевые слова: *теория графов, графы Деза, кореберно-регулярные графы, графы с несвязной второй окрестностью, изоморфизм графов.*

Goryainov V. S., Isakova G. S.

CONNECTION OF THE SECOND NEIGHBOURHOOD IN COADJOINT REGULAR DEZA GRAPHS

The article classifies coadjoint regular Deza graphs with unconnected second neighborhood. The authors solve the classical problem of combinatorics in general and graph theory in particular; they implement the transfer of combinatorial objects with specified properties. Studying of Deza graphs is of high interest due to the fact that they have the diameter of 2 and are a natural generalization of strongly regular graphs. For this class of graphs the problem of testing isomorphism seems potentially complicated. The approach proposed in the article may allow generalizing the results.

Keywords: *theory of graphs, Deza graphs, coadjoint regular graphs, graphs with unconnected second neighborhood, isomorphism of graphs.*

Задача, изучаемая в данной работе, является классической для многих областей дискретной математики - задача существования объектов с заданными комбинаторными свойствами. Изучаемые в работе графы представляют интерес в алгебраической и алгоритмической теории графов и могут быть рассмотрены с различных точек зрения.

В 1998 году в работе [3] впервые было рассмотрено естественное обобщение понятия сильно регулярного графа - графы Деза. Авторы указали на базовые соотношения в графах Деза и предложили несколько конструкций.

Сильно регулярные графы интересны для изучения как минимум с двух точек зрения.

С одной стороны, сильно регулярные графы образуют класс графов, для которых особенно сложна задача проверки изоморфизма графов. Это связано с высоким уровнем внутренней симметрии и особенностями метрических соотношений в графе. С другой стороны, для изучения сильно регулярных графов могут применяться алгебраические методы, в частности, матричный анализ. Так, за исключением тривиальных случаев, матрица смежности сильно регулярного графа имеет ровно 3 различных собственных значения. Отметим, что задача перечисления сильно регулярных графов на данный момент не решена.

Графы Деза имеют схожие метрические соотношения, и поэтому задача проверки изоморфизма для данного класса графов потенциально сложна.

В ряде исследований было выяснено, что графы Деза наследуют некоторые свойства сильно регулярных графов. Например, в [1] показано, что вершинная связность графа Деза, полученного из сильно регулярного графа с помощью инволюции, совпадает с валентностью.

Однако данное обобщение приводит и к потере части свойств. Например, в [2] было показано, что существует граф Деза, имеющий сколь угодно большое число различных собственных значений.

Одним из методов изучения графов Деза является наложение свойств и, как следствие, получение структурных ограничений на граф, классификация графов с заданными свойствами.

Особого внимания заслуживает работа [4], в которой получены соотношения для графов Деза без 3-коклик, описаны некоторые свойства и в частных случаях получена классификация таких графов.

В работе [5] классифицированы реберные графы Деза.

В настоящей работе классифицированы все графы Деза с несвязной второй окрестностью.

Для начала рассмотрим связность окрестности в сильно регулярном графе. В следующем абзаце приводится теорема, описывающая связные сильно регулярные графы с несвязной второй окрестностью.

Теорема. Если в связном сильно регулярном графе Γ хотя бы одна из вершин имеет несвязную вторую окрестность, то Γ – это полный многодольный граф.

Доказательство:

Возьмем $x \in V(\Gamma)$ с несвязной второй окрестностью. Пусть $u,v \in \Gamma_2(x)$ - произвольные вершины из второй окрестности. Вершины x и v не смежны, значит имеют μ общих соседей, причем все эти соседи находятся в $\Gamma(x)$, то есть вершина v имеет ровно μ соседей в $\Gamma(x)$, аналогично вершина u имеет ровно μ соседей в $\Gamma(x)$.

Покажем, что u и v имеют одних и тех же μ соседей в $\Gamma(x)$.

Пусть сначала вершины u и v лежат в разных компонентах связности $\Gamma_2(x)$. В этом случае u не смежна с v, и вершины u и v имеют μ общих соседей. u и v лежат в разных компонентах связности $\Gamma_2(x)$, следовательно, общих соседей могут иметь только в $\Gamma(x)$, но каждая из вершин u и v имеет ровно μ соседей в $\Gamma(x)$, отсюда следует, что это одни и те же μ соседей в $\Gamma(x)$, то есть любые две вершины из разных компонент связности $\Gamma_2(x)$ (x) имеют одних и тех же μ соседей в $\Gamma(x)$.

Покажем, что любые две вершины v_1, v_2 из одной компоненты связности в $\Gamma_2(x)$ имеют одних и тех же μ соседей в $\Gamma(x)$. Рассмотрим вершину u из другой компоненты связности. Так как v_1 и u из разных компонент связности, то по доказанному они имеют одних и тех же соседей в $\Gamma(x)$. Аналогично, v_2 и u имеют одних и тех же μ соседей в $\Gamma(x)$. Отсюда v_1 и v_2 имеют одних и тех же μ соседей в $\Gamma(x)$.

Далее сделаем разбор случаев.

Если $k = \mu$, то граф Γ – полный многодольный граф.

Допустим теперь, $k \neq \mu$, то есть $\mu < k$, и в $\Gamma(x)$ есть вершины, не смежные с любой вершиной из $\overline{\Gamma}(x)$. Рассмотрим такую вершину y. Тогда y может иметь соседей, кроме вершины x, только в $\Gamma(x)$. Всего в $\Gamma(x)$ находится k вершин, следовательно, кроме у в $\Gamma(x)$ находится $k - 1$ вершин, но вершина у имеет всего k соседей, таким образом соседями вершины у являются вершина x и указанные выше $k - 1$ вершин. Так как $x \sim y$, и они имеют $k - 1$ общих соседей, следовательно, $\lambda = k - 1$. Воспользуемся следующим равенством $k(k - 1 - \lambda) = (n - k - 1)\mu$. Получим, что либо $\mu = 0$, либо $n = k + 1$, из чего следует, что граф Γ - либо дизъюнктное объединение клик (что противоречит условию связности), либо клика, что противоречит условию сильной регулярности, т. е. в случае $\mu < k$ получили противоречие. ■

В работе результат был обобщен для кореберно-регулярных графов Деза, соответственно, далее приводятся формулировка и

доказательство основного результата данной работы.

Теорема. Если в кореберно-регулярном точном графе Деза Γ существует вершина с несвязной второй окрестностью, то Γ изоморфен реберному расширению полного многодольного графа.

Доказательство:

Пусть (n,k,b,a) – параметры кореберно-регулярного точного графа Деза Γ. Заметим, что $a < b$, иначе Γ – сильно регулярный. Пусть μ – число общих соседей двух несмежных вершин, тогда имеет место два случая:

1) $a = \mu$;

2) $b = \mu$.

1) $a = \mu$

Пусть u – вершина, вторая окрестность которой несвязна, тогда все вершины из $\Gamma_2(u)$ имеют одних и тех же μ общих соседей в $\Gamma(u)$. Обозначим через M множество из μ вершин. Так как $a = \mu < b \leq k$, то M - это строгое подмножество в $\Gamma(u)$, то есть $\Gamma(u)\backslash M$ не пусто. Заметим, что вершина из $\Gamma(u)\backslash M$ не имеет соседей в $\overline{\Gamma}(u)$, следовательно, смежна со всеми остальными вершинами в $\Gamma(u)$, кроме самой себя, то есть $b = k - 1$.

Пусть $A_1, A_2, \ldots$ – компоненты связности графа $\Gamma_2(u)$. Покажем, что это клики размера $k - \mu + 1$.

Рассмотрим компоненту произвольную компоненту A_i. Пусть в ней найдется пара несмежных вершин, но тогда найдется пара несмежных вершин x_1, x_2 на расстоянии 2, следовательно, x_1, x_2 имеют μ общих соседей в $\Gamma(u)$ и еще как минимум одного в $\Gamma_2(u)$. Противоречие с кореберной регулярностью. Отсюда следует, что коребер нет, значит A_1 – это клика. В силу условия регулярности, A_1 будет содержать $k - \mu + 1$ вершину.

Заметим, что множество $\Gamma(u)\backslash M \cup \{u\}$ – это также клика размера $k - \mu + 1$. Таким образом, граф Γ можно представить как t клик $(t \geq 3)$ размера $k - \mu + 1$, каждая вершина из этих клик смежна с каждой из μ вершин из множества M.

Пусть x – вершина из некоторой клики K размера $k - \mu + 1$, а y – вершина из множества M. Посчитаем количество общих соседей вершин x и y. Внутри клики K эти вершины имеют $k - \mu$ общих соседей, а внутри множества M имеют $k - (n - \mu)$ общих соседей (все соседи вершины y в множестве M). Таким образом, всего вершины x и y имеют $k - \mu + k - (n - \mu) = 2k - n$ общих соседей. Поскольку вершина y имеет как минимум двух соседей в других кликах, и эти вершины не являются соседями x, то число общих соседей x и $y \leq k - 2$, а значит равно $a = \mu$, то есть $2k - n = \mu$, отсюда $k - \mu = n - k$.

Таким образом, размер каждой клики равен $n - k + 1$, но эти клики - это подграфы в $\Gamma_2(u)$, а в $\Gamma_2(u)$ всего $n - k - 1$ вершина. Противоречие.

2) $b = \mu$

В данной ситуации возможно 2 случая:

2.1) $b = \mu = k$

Если $b = \mu = k$, тогда антиокрестность вершины u, объединенная с вершиной u, – это коклика, а окрестность – кореберно-регулярный граф Деза Γ, у которого $b = \mu$. Продолжая рекурсивно этот процесс, получим, что граф Γ является полным многодольным графом.

2.2) $b = \mu < k$

Если $b = \mu < k$, тогда $\Gamma(u)\backslash M$ не пусто, и любая вершина x из $\Gamma(u)\backslash M$ имеет соседей только в $\Gamma(u)$, отсюда вершины u и x имеют $k - 1$ общего соседа, и $b = \mu = k - 1$, отсюда $\Gamma(u)\backslash M$ содержит только одну вершину, а $\overline{\Gamma}(u)$ будет состоять из объединения изолированных ребер. Тогда $\overline{\Gamma}(u)$, объединенная с вершиной u, – это объединение изолированных ребер, а окрестность – кореберно-регулярный граф Деза Γ, у которого снова $b = \mu$. Получаем ситуацию, аналогичную случаю 2.1. Далее, продолжая рекурсивно этот процесс, получим, что граф Γ - реберное расширение полного многодольного графа.

Основной результат данной работы состоит в том, что кореберно-регулярные графы Деза с несвязной второй окрестностью исчерпываются полными многодольным графами с размером доли больше двух и их 2-кликовыми расширениями.

Примечания

1. Гаврилюк А. Л., Горяинов С. В., Кабанов В. В. О вершинной связности графов Деза // Тр. Ин-та математики и механики УрО РАН. Екатеринбург, 2013. Т. 19, № 3. С. 94–104.

2. Гаврилюк А. Л., Шалагинов Л. В. О графах Деза с 4-мя различными собственными значениями // Тезисы Международной (43-й Всероссийской) молодежной школы-конференции. Екатеринбург, 2012. С. 20–23.

3. Erickson M., Fernando S., Haemers W. H., Hardy D. and Hemmeter J. Deza graphs: a generalization of strongly regular graphs // J. Comb. Designs. 1999. Vol. 7, P. 359–405.

4. Ермакова Г. М. Две задачи алгебраической теории графов // Автореферат диссертации на соискание ученой степени кандидата ф.-м. н., УрО РАН, Екатеринбург, 2009.

5. Кабанов В. В., Митянина А. В. Реберные точные графы Деза // Тр. ИММ УрО РАН, 18:1 (2012), 165–177.

Горяинов Сергей Викторович, преподаватель, Институт математики и механики Уральского отделения Российской академии наук, г. Екатеринбург. E-mail: 44g@mail.ru

Исакова Галина Сергеевна, студент, Челябинский государственный университет, г. Челябинск. E-mail: carleink@gmail.com

Viktor Sergeevich Goryainov, lecturer of Institute of Mathematics and Mechanics of Ural Branch of Russian Academy of Science, Yekaterinburg. E-mail: 44g@mail.ru

Galina Sergeevna Isakova, student of Chelyabinsk State University, Chelyabinsk. E-mail: carleink@gmail.com

УДК 005.95/. 96 : 004.056 + 331.108.26 : 004.056

Астахова Л. В., Ефремов В. А., Митькин А. И.

АВТОМАТИЗАЦИЯ МНОГОФАКТОРНОЙ ОЦЕНКИ КАДРОВЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье представлены результаты автоматизации многофакторной оценки кадровых уязвимостей информационной безопасности, которая была разработана на основании основных этапов жизненного цикла деятельности по обеспечению кадровой безопасности организации. Разработанный программный продукт позволяет: при приёме на работу обращать внимание не только на профессиональные компетенции соискателя, но и на его личностные характеристики; после его утверждения на должность – поддерживать должный уровень профессиональных знаний; при увольнении – корректно оценить его психологическое состояние.

Ключевые слова: *информация, безопасность, кадровая безопасность, кадровые уязвимости, техническая защита информации, оценка, психология и т. п.*

Astakhova L. V., Efremov V. A. Mitkin A. I.

AUTOMATION OF MULTIFACTORIAL ESTIMATION OF PERSONNEL VULNERABILITY OF INFORMATION SECURITY

The article represents results of automation of multifactorial estimation of personnel vulnerability of information security which has been developed on the basis of the main stages of the life cycle of the activity aimed at ensuring personnel security of organizations. The abovementioned developed software allows to pay attention not only on professional competences of the applicant, but also on his personal characteristics; after the applicant's approval for the position the software allows to maintain the adequate level of professional knowledge and in case of his dismissal – to correctly assess his psychological state.

Keywords: *information, security, personnel security, personnel vulnerability, technical information security, estimation, psychology, etc..*

Введение. Актуальность проблемы

В процессе обеспечения информационной безопасности мы должны руководствоваться не только профессиональными компетенциями, но и психологическим состоянием человека, потому что вопросы безопасности систем большей частью есть вопросы человеческих отношений и человеческого поведения (1). Поэтому в сфере информационной безопасности утечка информации в подавляющем большинстве случаев происходит по вине сотрудников. Вопросы автоматизации оценки личностных качеств кандидата на вакантную должность для обеспечения информационной безопасности организации уже рассматривались нами в одной из публикаций (2). Однако кроме личностных качеств важны и профессиональные компетенции сотрудника, причем не только на этапе приема на работу, но и в процессе работы. А личностные качества сотрудника важны еще и при увольнении. В связи с этим есть необходимость в многофакторной оценке кадровых уязвимостей информационной безопасности.

Программный продукт для многофакторной оценки уязвимостей

Для реализации названных выше целей нами была написана программа на языке программирования C# с использованием SQL. Она состоит из двух основных модулей, пользовательского и администраторского, разделение на модули осуществляется системой логинов и паролей (рис. 1).

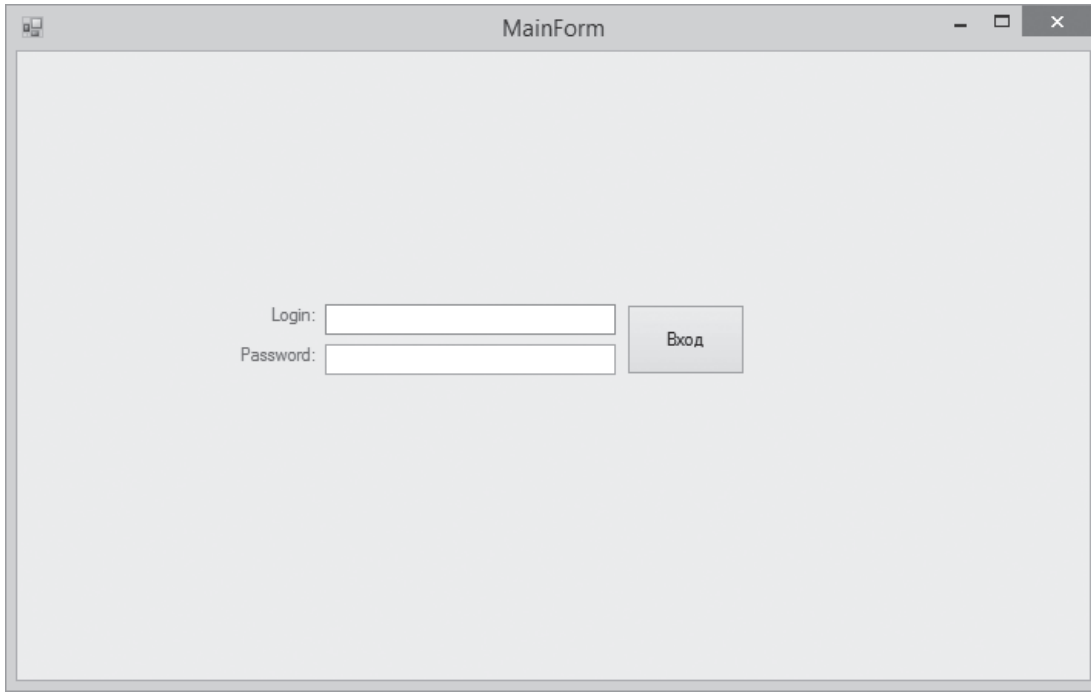


Рис. 1. Система логинов и паролей

При вводе логина и пароля, соответствующего пользователю, программа предоставляет ему возможность выбрать этап деятельности (прием на работу или работа), а затем – один из тестов, доступных для него, и начать тестирование (рис. 2). Результаты тестирования будут надёжно защищены от посторонних лиц.

При вводе логина и пароля, соответствующего администратору, программа предоставляет куда больше возможностей. Администраторы могут редактировать тесты, редактировать и просматривать информацию о пользователях, могут начать тестирование с соискателем либо работником по принципу собеседования, а также увидеть рекомендации специалиста по защите информации сотруднику службы управления персоналом для процесса увольнения того или иного сотрудника.

В окне редактирования тестов имеется возможность добавлять и удалять тесты, редактировать вопросы в них, присваивать определенные тесты определённым работникам фирмы в зависимости от их положения и присваивать тесту комментарий, в котором описаны правила оценивания теста (рис. 3).

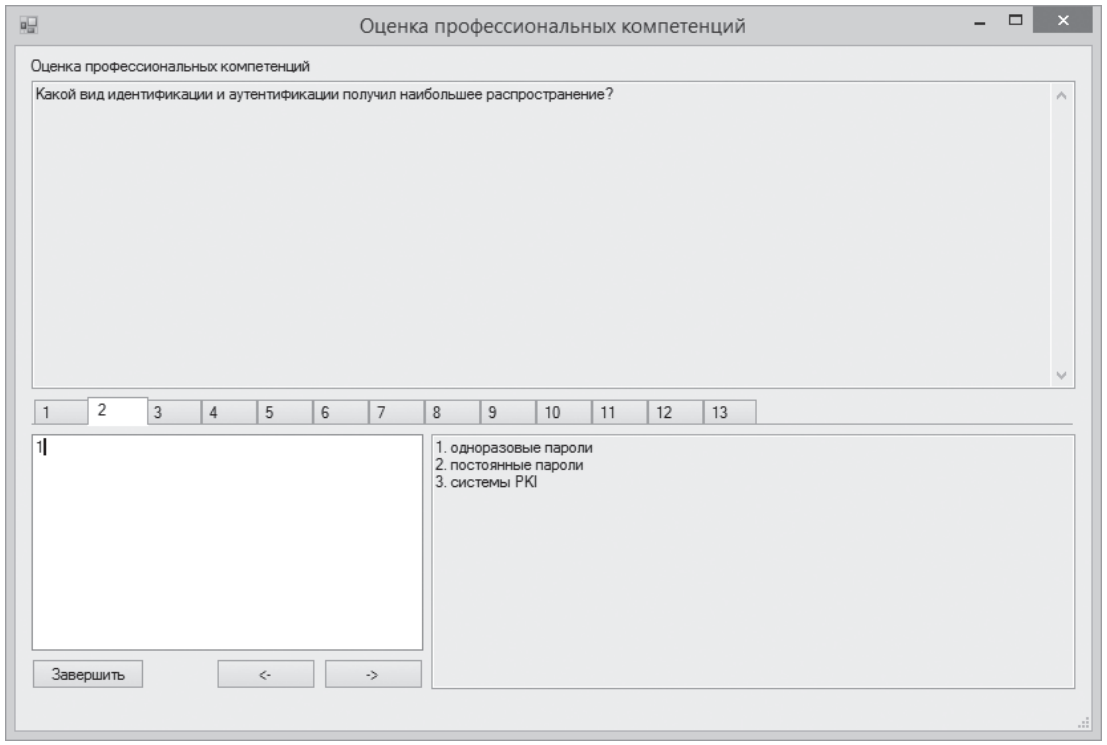


Рис. 2. Окно тестирования

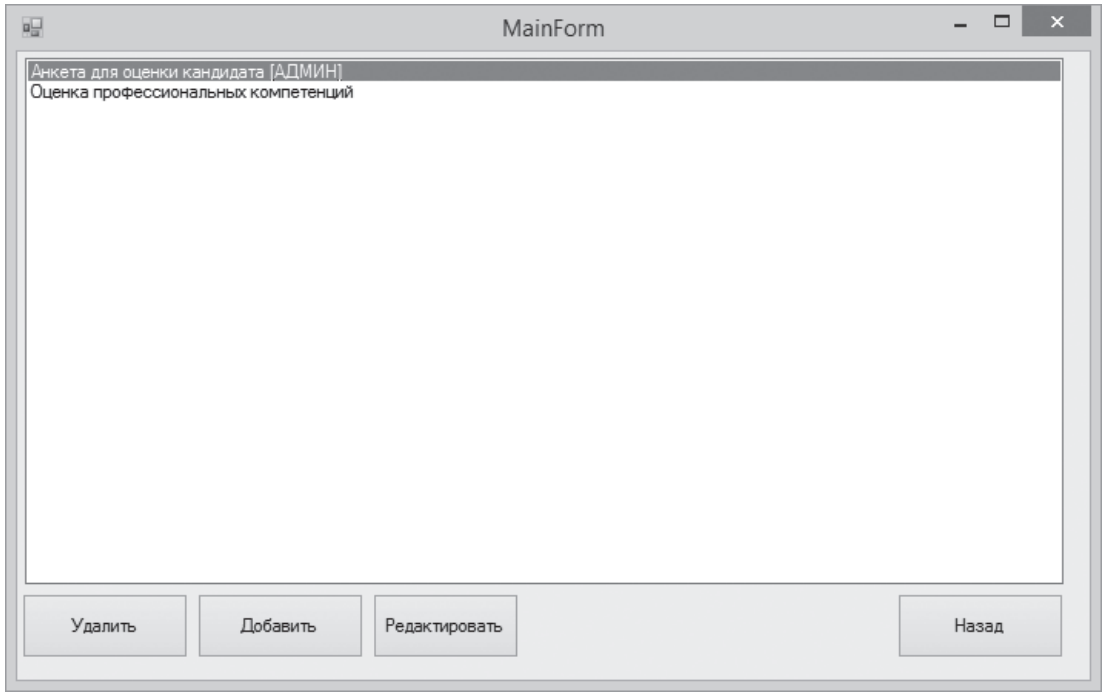


Рис. 3. Окно редактирования тестов

Программа включает в себя большой функционал по созданию различных форм опроса, таких, как тест, вопросы с открытым ответом, вопросы, требующие развёрнутого ответа, и т. д. (рис. 4).

В окне редактирования пользователей выводится полный список пользователей, в нём можно добавлять, удалять пользователей, просматривать информацию о пользователе, сводку результатов тестов, ответы пользователя на определенный тест, а также менять статус работника в зависимости от прохождения им всего жизненного цикла на предприятии – от соискателя вакансии до

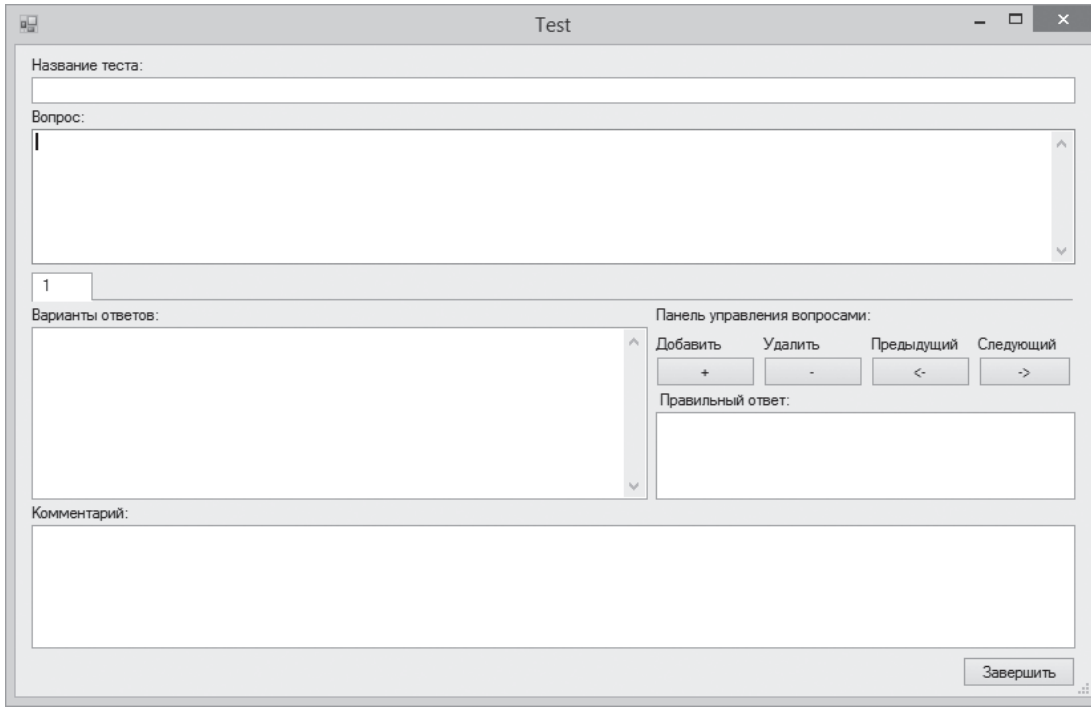


Рис. 4. Окно создания тестов

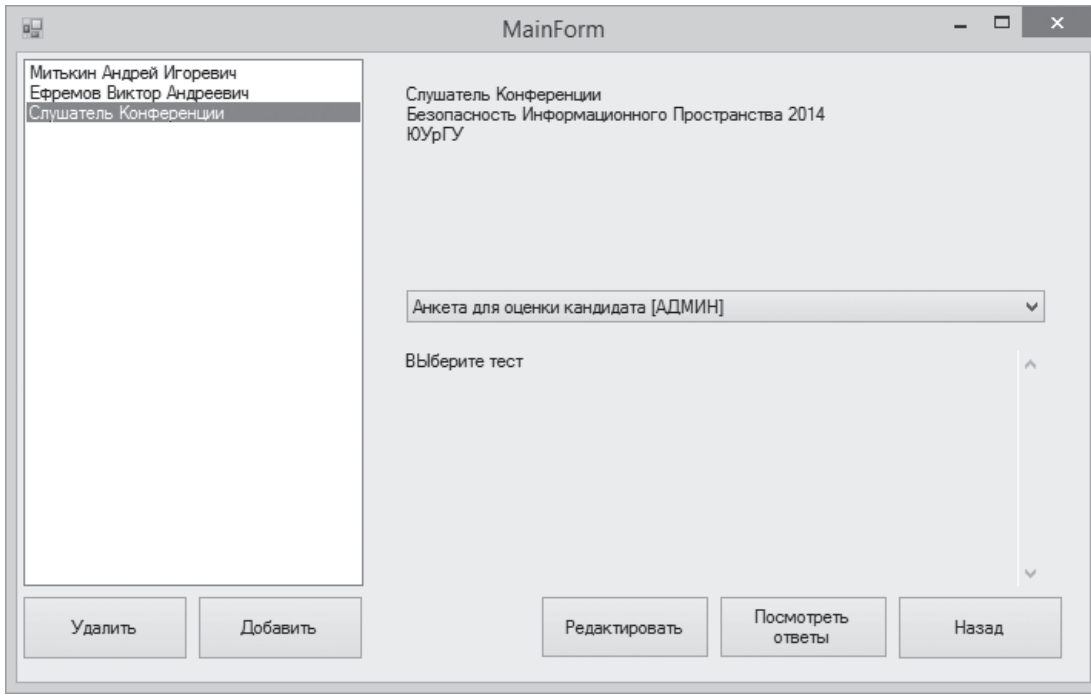


Рис. 5. Окно редактирования пользователей

кандидата на увольнение, при этом меняются доступные для работника тесты. Также можно добавлять другие свои комментарии и заметки для каждого работника (рис. 5).

В программе реализована высокая интеграция баз данных – все данные сотрудников, тесты, критерии оценивания, результаты прохождения могут храниться на выделенном сервере с настроенной базой данных.

Заключение

Таким образом, научная новизна разработанного программного продукта заключается в использовании методики многофак-

торной оценки кадровых уязвимостей информационной безопасности на разных этапах профессиональной деятельности сотрудников организации. Реализация автоматизации многофакторной оценки кадровых уязвимостей информационной безопасности может сыграть большую роль в упрощении, совершенствовании, структурировании этой деятельности, что позволит повысить качество подбора и мониторинга персонала. Кроме того, использование созданного программного продукта даст возможность прогнозировать и устранять утрату и утечку конфиденциальной информации при увольнении сотрудника с высоким уровнем кадровой уязвимости.

Примечания

1. Астахова Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия Компьютерные технологии, управление и радиоэлектроника. – 2013. – Т. 13, №.1. – С. 79–83.

2. Астахова Л. В., Землянская О. О., Ефремов В. А. Автоматизация оценки кандидата на вакантную должность для обеспечения информационной безопасности организации // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 1. – С. 34–38.

Астахова Людмила Викторовна, д. п. н., профессор, Южно-Уральский государственный университет, (г. Челябинск). E-mail: lvastachova@mail.ru

Ефремов Виктор Андреевич, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: EfremovVA@bk.ru

Митькин Андрей Игоревич, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: mr.erikost@gmail.com

Liudmila Viktorovna Astakhova, PhD Pedagogics, professor of South Ural State University. E-mail: lvastachova@mail.ru

Viktor Andreevich Efremov, student of South Ural State University. E-mail: EfremovVA@bk.ru

Andrey Igorevich Mitkin, student of South Ural State University. E-mail: mr.erikost@gmail.com

УДК 349.22 : 004.056.5 + 002 : 004.056 + 004.382.7.056

Лаптева Т. В., Мищенко Е. Ю., Макарова П. В.

ОСОБЕННОСТИ СОСТАВЛЕНИЯ ТРУДОВЫХ ДОГОВОРОВ И СОГЛАШЕНИЙ О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, НА ПРЕДПРИЯТИЯХ, ИСПОЛЬЗУЮЩИХ DLP-СИСТЕМЫ

Тема данной работы: организационные меры при использовании продуктов DLP. Широкий функционал DLP-систем позволяет собирать информацию о деятельности сотрудников на рабочем месте без их ведома, что ставит следующие цели и задачи: учесть интересы работников и работодателей и сформулировать ряд условий. Результатом работы является форма соглашения о неразглашении информации, составляющей коммерческую тайну, и трудового договора, с учетом выявленных особенностей DLP-систем, что отличает данную работу от родственных по тематике.

Ключевые слова: *информация, безопасность, защита информации, DLP-системы, трудовой договор, соглашение о неразглашении.*

Lapteva T. V., Mischenko E. Y., Makarova P. V.

FEATURES OF EMPLOYMENT CONTRACTS AND NON-DISCLOSURE AGREEMENTS WHICH COMPRISE TRADE SECRETS AT ENTERPRISES WHICH USE DLP SYSTEMS

The topic of the work is the organizational measures in the process of using DLP products. Broad functionality of DLP systems can collect information on the activities of employees on the workplace without their knowledge which establishes the following goals and objectives: to take into account the interests of employees and employers and to develop certain conditions. The result of the aforementioned work is a form of non-disclosure agreements which comprises a trade secret, as well as the employment contract based on identified features of DLP systems which distinguishes the article from related works.

Keywords: *information, security, information security, DLP systems, employment agreement, non-disclosure agreement.*

Широкое распространение DLP-систем и стремительный рост рынка данной продукции в последнее время определяет актуальность и значимость вопроса разработки на предприятии документации, регламентирующей порядок использования таких систем. Кроме того, производители таких систем заявляют, что помогают своим клиентам соблюдать законодательство, в том числе: ФЗ-98 «О коммерческой тайне», Приказ ФСТЭК России от 18.02.2013 № 21 и др.

Предотвращение утечек (англ. Data Leak Prevention, DLP) — технологии предотвращения утечек конфиденциальной информации за пределы информационной системы, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек [1]. Примеры различных торговых марок, выпускающих продукты DLP: InfoWatch , Websense, McAfee, Symantec, Инфосистемы Джет, Zecurion, МФИ Софт, GTB. По некоторым данным объем рынка DLP-систем в 2013 году составил 2265 млн. рублей, а рост – порядка 28%.

Возможности DLP, обозначенные вендорами:

1) контроль информационных потоков, передаваемых по каналам связи: корпоративной и личной электронной почты, вебсайтов, сервисов мгновенных сообщений (в текстовом представлении, средствами АС);

2) контроль файлов на рабочих станциях и серверах: данных, хранимых на серверах, мобильных и внешних носителях, рабочих станциях, системах хранения данных (средствами АС);

3) создание снимков экрана рабочих станций: непосредственно используемой информации (графическое представление, анализ человеком и ПО);

4) запись веб-камерами в составе рабочей станции и штатными камерами видеонаблюдения (видеоинформация, анализ человеком и ПО);

5) запись аудиомикрофонами в составе рабочей станции, дополнительное оборудование (аудио, человек + ПО).

Если возникает подозрение о том, что информация покидает разрешенный периметр, срабатывает одно из трех заранее определенных правил: доставка адресату разрешается, система приостанавливает доставку до решения специалиста безопасности или доставка блокируется. Но вместе с информацией правообладателя, составляющей коммерческую тайну, в системе обрабатываются также персональные данные и общедоступная информация. Однако сведения о просмотре общедоступной информации конкретным лицом не являются общедоступными, такую информацию можно отнести к тайне личной жизни.

Для того чтобы более детально рассмотреть правовую сторону вопроса, обратимся к законодательству РФ. Во-первых, на защиту прав граждан становится Конституция РФ. Например, в ст. 23 говорится, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [2]. Во-вторых, защита прав и свобод граждан гарантируется посредством Гражданского кодекса (например, ст. 152.2) Российской Федерации, Уголовного кодекса Российской Федерации и Семейного кодекса Российской Федерации.

Статья 137 УК РФ предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 138 УК РФ определяет ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан [3].

В Кодексе об административных правонарушениях тоже есть положение, а именно статья 13.11, предусматривающая ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Защита информации, составляющей тайну личной или семейной жизни, обычно неразрывно связана с охраной персональных данных. В ст. 2 ФЗ-152 обозначается цель документа, а именно – обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [4].

Теперь рассмотрим вопрос с другой стороны. Если на предприятии введен режим коммерческой тайны, обладатель информации заинтересован в её сохранности и должен принять меры для защиты, такую задачу

ставит ФЗ-149 «Об информации, информационных технологиях и о защите информации» и ФЗ-98 «О коммерческой тайне» (ст. 10).

ФЗ-149, статья 6, пункты 3–4:

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; <…>

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами[5].

Производители DLP-систем указывают на то, что в законодательстве нет определения понятий «личная и семейная тайна» и «частная жизнь лица», используемых в статье 137 УК РФ, а значит, они могут использовать удобную для себя трактовку этого понятия.

Также производители DLP настаивают на том, что их продукт не входит в категорию средств, предназначенных для негласного получения информации [6], и на них не распространяется действие ст. 138.1 УК РФ, а значит для производства, реализации и приобретения таких систем лицензии ФСБ не нужны.

В настоящее время не опубликовано прецедентов судебной практики, связанных с использованием DLP-систем. Однако можно привести яркий пример привлечения к дисциплинарному взысканию по инциденту, в расследовании которого бы такие системы были полезны. Сотрудница турфирмы «Интерсити сервис» (холдинг KPM Group) Кира Белокрылова в течение года отправляла конфиденциальную информацию в другую туристическую компанию как со своего компьютера, так и с компьютеров других сотрудниц. Уволена по статье 81 ч. 6 Трудового кодекса – разглашение коммерческой тайны (2008 год).

Кроме того, следует обратить внимание на определение Конституционного Суда по делу Захаркиных (2005 год), где сказано, что в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер [7].

Руководство предприятия может преследовать различные цели, разворачивая DLP-систему в стенах организации:

1) предотвращение утечек коммерческой тайны путем блокирования известных каналов широко распространенными методами, снизить риск утечек;

2) облегчение расследования инцидентов разглашения информации, составляющей коммерческую тайну, за счет архивирования событий, совершаемых пользователями;

3) оценка лояльности сотрудника (выявление систематических нарушений, проступков, фактов передачи конфиденциальной информации);

4) обеспечение требований законодательства.

Обычно целью руководства организации не является тотальное увольнение сотрудников. В том случае, если руководство организации действительно хочет предотвратить утечку КТ, имеет смысл предупредить сотрудников о применяемых мерах контроля (помимо ознакомления с Положением о коммерческой тайне и Перечнем информации, составляющей коммерческую тайну).

Предлагаемое решение:

1) обозначить правила, запрещающие обработку (хранение и передачу) личной информации на корпоративных устройствах, а также использование в этих целях корпоративных сервисов;

2) предупредить о том, что в компании используются средства мониторинга и контроля выполнения правил;

3) заявить об отсутствии умысла читать личную переписку.

В таком случае работник самостоятельно делает выбор – не использовать корпоративные средства в личных целях или использовать, зная, что эта информация может оказаться доступной офицерам информационной безопасности.

Таким образом, предлагается включить в соглашение о неразглашении или трудовой договор с работником (к примеру, в раздел второй «Права и обязанности сторон») следующие пункты:

2.1. В целях охраны конфиденциальности информации Работник обязан:

2.1.1. Выполнять установленный работодателем режим коммерческой тайны.

2.1.2. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях.

2.1.3. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось.

2.2. Работник обязуется не использовать корпоративное оборудование в личных целях, в том числе для обработки, хранения и передачи личной информации.

2.3. Работодатель оставляет за собой право контролировать выполнение пунктов 2.1 и 2.2, в том числе с использованием программно-аппаратных средств мониторинга.

2.4. Использование программно-аппаратных средств мониторинга Работодателем не будет применяться для умышленного чтения личной переписки.

Примечания

1. Википедия: свободная энциклопедия [электронный ресурс], 2014. URL: https://ru.wikipedia.org/wiki/Предотвращение_утечек_информации

2. Конституция Российской Федерации, 2014. URL: http://www.consultant.ru/document/cons_doc_LAW_2875/?frame=1

3. Уголовный кодекс РФ (УК РФ) от 13.06.1996 N 63-ФЗ, 2014. URL: http://www.consultant.ru/popular/ukrf/

4. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 04.06.2014) «О персональных данных», 2014. URL: http://www.consultant.ru/document/ cons_doc_LAW_163964/

5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации», 2014. URL: http://www.consultant.ru/document/cons_doc_LAW_165971/

6. Прозоров А. Информационная безопасность в России и мире // 4 горячих юридических вопроса про DLP [электронный ресурс], 2014. URL: http://www.securitylab.ru/blog/personal/80na20/79635.php

7. Определение Конституционного Суда РФ от 09.06.2005 г. № 248-О, 2005. URL: http://sutyajnik.ru/documents/278.html

Лаптева Тамара Владимировна, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: tamara.lapteva@gmail.com

Мищенко Евгений Юрьевич, ст. преподаватель, Южно-Уральский государственный университет, (г. Челябинск).

Макарова Полина Викторовна, к. п. н., доцент, Южно-Уральский государственный университет, (г. Челябинск).

Tamara Vladimirovna Lapteva, student of South Ural State University. E-mail: tamara.lapteva@gmail.com

Evgeny Yurievich Mischenko, senior lecturer of South Ural State University.

Polina Viktorovna Makarova, Cand. Sc. Pedagogics, associate professor of South Ural State University.

УДК 006.88 + 331.108.2 : 006.8 + 336.71 (470):331.108.2 : 004.056

Ульянов Н. Л., Астахова Л. В.

ПРОБЛЕМА КАДРОВОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА РОССИИ

Рассматриваются требования по вопросу кадровой безопасности в системе стандартов Банка России, проводится соотношение этих требований с требованиями международных стандартов, оценивается важность требований по вопросу кадровой безопасности в системе стандартов Банка России.

Ключевые слова: *информационная безопасность, кадровая безопасность, кадровые уязвимости, стандартизация.*

Ulianov N. L., Astakhova L. V.

THE PROBLEM OF PERSONNEL SECURITY IN THE SYSTEM OF STANDARDS OF INFORMATION SECURITY OF THE BANK OF RUSSIA

The authors dwell on the standards and requirements of the personnel security in the system of standards of the bank of Russia. The article considers the correlation of the aforementioned requirements with the requirements of the international standards and estimates the significance of requirements on the issue of personnel security in the system of the bank of Russia.

Keywords: *information security, personnel security, personnel vulnerabilities, standardization.*

На сегодняшний день вопрос о кадровых уязвимостях информационной безопасности становится все более актуальным. По данным «Исследования утечек конфиденциальной информации в I полугодии 2014 года» аналитического центра «InfoWatch», в 71% случаев виновными в утечке информации оказались сотрудники компаний [1], по результатам аналогичного исследования за 2013 год – это число было равно лишь 54,1% [2].

К сожалению, в настоящее время существует нормативная недооценка угроз и уязвимостей, связанных с персоналом. В нормативных документах государственных регуляторов вопросу кадровых уязвимостей информационной безопасности практически не уделяется внимание. Однако существуют стандарты по информационной безопасности, в которых затрагиваются вопросы кадровой безопасности. Центральный банк Российской Федерации разработал систему стандартов в области информационной безопасности, в которой затронута проблема персонала.

Основным стандартом в данной системе является СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». В стандарте особое внимание выделяется угрозам, связанным с персоналом. К основным источникам угроз причисляются работники организации БС РФ (банковской системы Российской Федерации), реализующие угрозы информационной безопасности с использованием легально или вне легально полученных прав и полномочий [3, п 6.6]. Приоритетность кадровых уязвимостей подчеркивается в пункте 5.4 стандарта:

«Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал.

В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ.

Незлоумышленные действия собственных работников создают либо уязвимости информационной безопасности, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает».

В стандарте также представлены принципы, которыми следует руководствоваться при распределении прав доступа работников к информационным активам организации БС РФ [3, п 7.1.4]. К этим принципам относятся: «знать своего служащего» (Know your Employee) – принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью; «необходимо знать» (Need to Know) – принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне минимально необходимых для выполнения определенных обязанностей.

Так как большинство требований СТО БР ИББС-1.0-2014 по обеспечению кадровой безопасности было разработано на основе международного стандарта ISO/IEC 27001:2013 «Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования», можно соотнести требования по кадровой безопасности этих стандартов. Далее перечислены требования пункта 7.2 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу» стандарта СТО БР ИББС-1.0-2014 и в скобках указан пункт и его название в стандарте ISO/IEC 27001:2013, содержащий аналогичное требование:

• В организации должны быть документально выделены роли ее работников, которые следует персонифицировать с установлением ответственности за их выполнение (приложение А, пункт А.6.1.1 «Роли и ответственность в системе информационной безопасности»);

• Не допускается совмещение в рамках одной роли следующих функций: разработки и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения (приложение А, пункт А.6.1.2 «Разделение обязанностей»);

• В организации должны быть определена, выполняться и регистрироваться процедура приема на работу, влияющую на обеспечение информационной безопасности, включающую: проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверку в части профессиональных навыков и оценку профессиональной пригодности с документальным фиксированием результатов (приложение А, пункт А.7.1.1 «Проверка благонадежности»);

• Письменное обязательство о соблюдении конфиденциальности, приверженности корпоративной этике, включая требования по недопущению конфликта интересов (приложение А, пункт А.7.1.2 «Обязательства в трудовом соглашении»);

• Обязанности персонала по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты, должностные инструкции (приложение А, пункт А.7.2.1 «Ответственность руководства»).

• Невыполнение работниками организации требований по обеспечению ИБ должно приравниваться к невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности (приложение А, пункт А.7.2.3 «Дисциплинарные взыскания»);

• Контроль деятельности работников, обладающих совокупностью полномочий, позволяющей получить контроль над информационными активами организации (приложение А, пункт А.12.4.3 «Регистрация действий администраторов и операторов»);

• Определить, выполнять и регистрировать с фиксацией результатов процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки — при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии (основной текст, пункт 7.2 «Компетентность»).

Также в стандарте затронут вопрос обучения и повышения осведомленности в области информационной безопасности персонала организации. Приведены следующие требования [3, п. 8.9]:

• Должна быть организована санкционированная руководством организации работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ;

• Должны быть разработаны планы, программы обучения и повышения осведомленности в области ИБ. По результатам выполнения указанных планов должна осуществляться проверка полученных знаний;

• В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности;

• Программы обучения и повышения осведомленности должны разрабатываться для различных групп сотрудников с учетом их должностных обязанностей и выполняемых ролей и включать информацию: по существующим политикам информационной безопасности; по применяемым в организации защитным мерам; по правильному использованию защитных мер в соответствии с внутренними документами организации; о значимости и важности деятельности работников для обеспечения информационной безопасности организации;

• В организации БС РФ должен быть определен перечень свидетельств выполнения программ обучения и повышения осведомленности в области ИБ. В частности, такими свидетельствами могут являться: документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области информационной безопасности с указанием уровня образования, навыков, опыта и квалификации обучаемых; документы, содержащие результаты проверок обучения работников организации; документы, содержащие результаты проверок осведомленности в области информационной безопасности в организации;

• Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области информационной безопасности, соответствующее полученной роли;

• В организации должны быть определены роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю результатов, а также назначены ответственные за выполнение указанных ролей.

В международном стандарте ISO/IEC 27001:2013 также уделяется внимание вопросу обучения и повышения осведомленности в области информационной безопасности персонала организации. В пункте А.7.2.2 (приложение А) приведены следующие требования: для всех сотрудников организации и, где это применимо, работающих по контракту должны быть проведены обучение и подготовка, обеспечивающие соответствующие знания, а также регулярное обновление организационных политик и процедур в той мере, в какой это касается их служебных обязанностей.

Можно заметить, что в стандарте СТО БР ИББС-1.0-2014 приведены более полные и конкретизированные требования, касающиеся вопроса обучения и повышения осведомленности в области информационной безопасности персонала организации.

Для оценки соблюдения требований стандарта СТО БР ИББС-1.0-2014 был разработан стандарт СТО БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014». В результате проведения оценки соответствия информационной системе присваевается один из 5 уровней со-

ответствия в зависимости от итогового показателя оценки [4, п. 11]. В методике представлены следующие показатели оценки: итоговый показатель, показатели по направлению оценки, групповые показатели, частные показатели. Значения всех показателей расположены в диапазоне от 0 до 1. Значение итогового показателя определяется по наименьшему значению из трех показателей по направлениям оценки. Всего в методике три направления оценки: 1) оценка текущего уровня информационной безопасности организации; 2) оценка менеджмента информационной безопасности организации; 3) оценка уровня осознания информационной безопасности организации. В соответствии с этими направлениями оценки распределены по 31 групповому показателю следующим образом: первое направление оценки – показатели М1М10; второе направление оценки – показатели М11М27; третье направление оценки – показатели М28М34. Каждый групповой показатель соответствует пунктам стандарта СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Пунктам стандарта СТО БР ИББС-1.0-2014, посвященным вопросу кадровой безопасности, соответствуют следующие групповые показатели: пункту 7.2 [4] соответствует групповой показатель М1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу»; пункту 8.9 [4] – М18 «Разработка и организация реализации программ по обучению и повышению осведомленности в области информационной безопасности» и М31 «Оценка деятельности руководства организации по поддержке реализации системы обеспечения информационной безопасности». Можно заметить, что вопросу кадровой безопасности уделено внимание в каждом направлении оценки. Каждый групповой показатель состоит из частных показателей. Частный показатель содержит требование, соблюдение которого непосредственно оценивается. Частные показатели делятся на обязательные и рекомендуемые. Оценку за обязательный частный показатель в зависимости от степени соблюдения требования ставят в диапазоне от 0 до 1 (в соответствии со шкалой оценки степени соблюдения требования). Оценке за рекомендуемый частный показатель присваивается значение, равное 1, в том случае, если требование полностью выполняется, в противном случае этот показатель отмечается как неоцениваемый и не учитывается в дальнейших расчетах. В старой редакции методики 2010 года [6] необходимо было умножить полученную оценку частного показателя на коэффициент значимости частного показателя для получения итогового значения показателя, которое использовалось для дальнейших расчетов. Таким образом, коэффициент значимости частного показателя устанавливал приоритетность одних требований над другими. В действующей редакции методики 2014 года [5] коэффициентов значимости частного показателя нет. Но в ней введены корректирующие коэффициенты, которые учитываются в расчете показателя по направлению оценки [5, п. 10].

Представим такую ситуацию, что при оценке соответствия требованиям СТО БР ИББС-1.0 все частные показатели получили значение, равное единице, кроме какого-либо одного обязательного частного показателя в групповом показателе, касающегося вопроса кадровой безопасности (М1, М18 или М31), он оказался равным нулю. Тогда значение этого группового показателя будет меньше единицы, но не более чем на 20% (в соответствии с обеими редакциями методики). Тогда, в соответствии со старой редакцией методики, значение показателя по направлению оценки, содержащего этот групповой показатель, а, следовательно, и итогового показателя будет меньше единицы, но это отклонение будет меньше 15%, то есть оценка соответствия требованиям будет являться рекомендуемой банком [6, п. 11]. В соответствии же с новой редакцией при расчете значения показателя по направлению оценки необходимо учесть корректирующие коэффициенты. С их учетом значение показателя оценки по направлению будет снижено дополнительно на 15%, так как в этом направлении содержится один частный показатель со значением, равным нулю [5, п. 10]. В итоге это приведет к тому, что итоговый показатель будет меньше единицы более чем на 15%, что является нерекомендуемым Банком России [5, п. 11].

На этом примере видно, как возросла значимость требований по вопросу кадровой безопасности в новой редакции методики 2014 года по сравнению с редакцией 2010 года. Если раньше полное несоблюдение требования, описанного в каком-либо частном показателе, касающегося кадровой

безопасности, незначительно снижало итоговую оценку соблюдения требований стандарта СТО БР ИББС-1.0, то теперь это вызовет снижение итоговой оценки до значения, нерекомендуемого Банком России. Также можно отметить, что в новой редакции уделено больше вниманию принципу комплексности защиты информации.

В международной системе стандартизации информационной безопасности на основе стандарта ISO/IEC 27001 конкретная методика оценки соответствия требованиям не представлена, однако существует стандарт ISO/IEC 27004 «Информационная технология. Методы и средства защиты информации. Менеджмент информационной безопасности. Измерения». В данном стандарте содержатся рекомендации по разработке и использованию измерений и мер измерения для оценки эффективности системы менеджмента информационной безопасности. Если взглянуть на «Типовую форму конструктивных измерений, связанных с информационной безопасностью» [7, Приложение А], то можно заметить, что почти каждый пункт этой формы находит отражение в стандарте СТО БР ИББС-1.2-2014.

К сожалению, остальные стандарты и рекомендации в области стандартизации Банка России ничем не могут дополнить вышеописанные в вопросах кадровой безопасности. По нашему мнению, было бы уместно дополнить систему стандартов более полными конкретизированными требованиями, например, к процедуре приема сотрудников на работу, к планам и программам обучения и повышения осведомленности в области информационной безопасности, к их периодичности; а также методическими рекомендациями по вопросу кадровой безопасности.

Примечания

1. Исследование утечек конфиденциальной информации в первом полугодии 2014 года аналитического центра «InfoWatch» (Электронный ресурс) // InfoWatch. 2014. URL: http://www.infowatch.ru/report2014_half (дата обращения: 10.11.2014)

2. Исследование утечек конфиденциальной информации в 2013 году аналитического центра «InfoWatch» (Электронный ресурс) // InfoWatch. 2014. URL: http://www.infowatch.ru/report2013 (дата обращения: 10.11.2014)

3. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

4. ISO 27001:2013 «Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования».

5. СТО БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014».

6. СТО БР ИББС-1.2-2010 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014».

7. ISO 27004 «Информационная технология. Методы и средства защиты информации. Менеджмент информационной безопасности. Измерения».

8. Астахова Л. В. Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. 2011. № 1. С. 26–33.

9. Астахова Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2013. Т. 13. № 3. С. 79–83.

Ульянов Никита Львович, студент, Южно-Уральский государственный университет, (г. Челябинск). E-mail: rettou74@gmail.com

Астахова Людмила Викторовна, д. п. н., профессор, Южно-Уральский государственный университет,(г. Челябинск). E-mail: lvastachova@mail.ru

Nikita Lvovich Ulianov, student of South Ural State University. E-mail: rettou74@gmail.com

Liudmila Viktorovna Astakhova, PhD Pedagogics, professor of South Ural State University. E-mail: lvastachova@mail.ru

ВИКТИМОЛОГИЯ

Новый научно-практический журнал **ВИКТИМОЛОГИЯ** посвящен актуальным проблемам отечественной виктимологии – вполне сложившейся подотрасли криминологии, имеющей признаки самостоятельной правовой дисциплины – криминальная виктимология, а также как самостоятельное научное направление, изучающее лиц, ставших жертвами несчастных случаев, стихийных бедствий, катастроф и т. д., изучение которых охватывает широкий спектр познаний в области социологии, психологии, педагогики и других научных направлений.

Виктимология сегодня – это развивающееся комплексное учение о лицах, находящихся в кризисном состоянии и обладающих определенной степенью виктимности, о причинах и условиях виктимизации, о жертвах преступности, стихийных бедствий, катастроф и пр., а также о мерах и способах обеспечения защищенности и оказания помощи таким жертвам.

Особое внимание предполагается уделить исследованию предмета и источников виктимологии, международных правовых норм и норм отечественного законодательства в области защиты жертв; рассмотрению проблем, связанных не только с обеспечением правовой и иной безопасности жертв преступности, но и вопросов, связанных с их реабилитацией; анализу причин виктимного поведения и виктимизации современного общества; характеристике субъектов государственной и негосударственной деятельности в области виктимологической профилактики и защиты; возможностям самих граждан как субъектов виктимологического противодействия преступности. Данный журнал может стать полезным не только ученым в различных отраслях знаний, изучающих жертв, но и практикующим психологам, юристам, педагогам и широкому кругу читателей.

РУБРИКИ ЖУРНАЛА:

- Теория учения о жертве
- Современная виктимология
- Виктимология и безопасность
- Виктимологическая профилактика
- Криминальная виктимология
- Психология поведения жертв
- Ювенальная виктимология
- Зарубежная виктимология
- Обзор виктимологического законодательства

Подготовленные статьи необходимо отправить на E-mail: victimologiy@mail.ru

ВЕСТНИК УрФО
Безопасность в информационной сфере № 4(14) / 2014

Дата выхода в свет 29.12.2014. Формат 70×108 1/16. Печать трафаретная.
Усл.-печ. л. 5,60. Тираж 300 экз. Заказ 33/106.
Цена свободная.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.

Bulletin of the Ural Federal District
Security in the Sphere of Information No. 4(14)/2014

Date of publication of the 29.12.2014. Format 70X108 1/16. Screen printing.
Conventional printed sheet 5,60. Circulation – 300 issues. Order 33/106. Open price.

Printed in the printing house of the Publishing Center of SUSU.
76, Lenina Str., Chelyabinsk, 454080