

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)

Институт компьютерных технологий и информационной безопасности
Инженерно-технологической академии Южного федерального университета (г. Таганрог)
Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ» (г. Ростов-на-Дону)

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

**СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ**

(Ставрополь, 14-18 декабря 2015)

Часть 2

Ставрополь
2015

УДК 004.2/9
ББК 32.97
С 88

Организаторы конференции:

Министерство образования и науки Российской Федерации
Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)
Институт компьютерных технологий и информационной безопасности Инженерно-технологической
академии Южного федерального университета (г. Таганрог)
Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ»
(г. Ростов-на-Дону)

Оргкомитет конференции:

Председатель:

Лиховид А.А. – проректор по научной работе и стратегическому развитию СКФУ, доктор географических наук, кандидат биологических наук, профессор.

Члены оргкомитета:

Чипига А.Ф. – директор Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой информационной безопасности автоматизированных систем, кандидат технических наук, профессор.

Мезенцева О.С. – заместитель директора по учебной работе Института информационных технологий и телекоммуникаций СКФУ, кандидат физико-математических наук, доцент.

Петренко В.И. – заместитель директора по научной работе Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой организации и технологии защиты информации, кандидат технических наук, доцент.

Веселов Г.Е. – директор Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета, полномочный представитель ректора по развитию инженерного направления, доктор технических наук, доцент.

Самойлов А.Н. – заместитель директора Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета по научной и международной деятельности, кандидат технических наук, доцент.

Маслов О.Н. – заведующий кафедрой экономических и информационных систем Поволжского государственного университета телекоммуникаций и информатики, доктор технических наук, профессор.

Тищенко Е.Н. – заведующий кафедрой информационных технологий и защиты информации Ростовского государственного экономического университета (РИНХ), доктор экономических наук, доцент.

Ответственный секретарь:

Толстова Н.А. – доцент кафедры межинститутской базовой кафедры СКФУ, кандидат педагогических наук.

С 88 Студенческая наука для развития информационного общества: сборник материалов III Всероссийской научно-технической конференции. Часть 2. – Ставрополь: Изд-во СКФУ, 2015. – 374 с.

ISBN 978-5-9296-0813-1

Материалы конференции посвящены вопросам развития инновационных образовательных и инфокоммуникационных технологий, проблемам информационной безопасности объектов информатизации, изучению информационных систем и технологии. Изложены результаты научных исследований в области разработки информационных технологий решения экономических задач, затрагиваются вопросы создания и использования робототехнических систем.

УДК 004.2/9
ББК 32.97

ISBN 978-5-9296-0813-1

© ФГАОУ ВПО «Северо-Кавказский
федеральный университет», 2015

Классификационные схемы являются устаревшими и нереалистичными. Для большей части, классификации данных является субъективным процессом. Два человека могут смотреть на ту же часть данных и давать очень различные уровни систематизации, особенно когда применяется сложная схема. У организаций с давно установившейся схемой классификации также могут возникнуть проблемы внесения изменений или колебаний. Во многих из подобных ситуаций, систематизация просто не пригодна или не реалистична для исполнения. Еще одна проблема, которая делает классификацию невозможной - не совпадение или противоречие с безопасностью и использование данных политики вместе внутри организации.

Глобальная рабочая сила добавляет дополнительную сложность классификации. Ворочать главную схему классификации данных для большой, многонациональной организации без ясного понимания местных или региональных соображений является первым шагом к неудачной реализации. Есть множество конфиденциально связанных правовых обязательств, которые рассматриваются и понимаются со стороны различных внутренних заинтересованных сторон, где визуальная маркировка или метки помогают создать единое понимание терминов этикеток.

Роли и обязанности ясны. Каждая организация имеет свою собственную историю ответственности и право собственности данных. Различные группы также имеют разнообразные представления о значении информации, обработке и потребности в их безопасности. Это необходимо для оппортунистической классификации, или систематизации данных, которая позволяет использовать его для нужд этой группы. Отсутствие сдержек и противовесов в роли данных и обязанности усугубляет проблему оппортунистической классификации.

Классификация данных имеет различные значения в пределах организации. Различные группы могут выделять виды классификации по-разному с точки зрения безопасности. Например, индивидуальный контроль управления информационными знаниями может иметь инициативу классификации данных, которая включает в себя систематизацию данных (определение, если файл данных представляет собой договор) вместо чувствительности. Необходимо понимать плюсы и обоснование различных типов классификаций, которые могут существовать в рамках организации, и работать вместе с другими, объединяя усилия и представляя единую стратегию и бизнес-дела для классификации на предприятии.

Литература

1. Петренко С. А., Курбатов В. А. Политика информационной безопасности. [Электронный ресурс] Режим доступа: <http://www.universalinternetlibrary.ru>
2. Без автора. Компьютер + Локальная сеть + Интернет. [Электронный ресурс] Режим доступа: <http://pgtk.edu.ru>

МЕТОДЫ БОРЬБЫ С ВРЕДНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ НА СЪЕМНЫХ НОСИТЕЛЯХ

А. А. Честнов, З. А. Носиров

*руководитель – ассистент кафедры информационной безопасности О. М. Князева
Астраханский государственный университет, г. Астрахань*

Введение. Вредоносное компьютерное программное обеспечение (ПО) — одна из наиболее широко известных угроз для сетей любой структуры [3]. Подобно живым микроорганизмам, они распространяются от компьютера к компьютеру, от носителя к носителю, «заражая» программы и файлы приложений и операционной системы [4]. Если пользователь часто использует USB накопители: подключает к различным компьютерам, переносит на них/ с них файлы, то вероятность того, что на них окажется вредоносное ПО достаточно велика. Примерно каждый десятый компьютер может стать причиной «заражения», приводящей к потере/искажению данных [4].

Ежедневно, студенты высших учебных заведений, абсолютно не задумываясь, пользуются различными флеш-накопителями в стенах университета. При этом в каждом учебном классе учреждения находится около 20 компьютеров. Таким образом, вредоносные программы переходят от одного устройства к другому, пополняя список «зараженных». Таким образом, одной из актуальных проблем высшего учебного заведения является распространение вредоносного программного обеспечения в пределах его локально-вычислительной сети.

Основная часть. Задачей исследования является выявление списка часто встречающегося вредоносного ПО, циркулирующего в локально-вычислительной сети университета на примере ФГБОУ ВПО АГУ и определение методов предупреждения и ликвидации последствий от их действий.

Для выявления списка часто встречающихся вредоносных программ при содействии отдела Эксплуатации Программного Обеспечения был проведен опрос студентов 1–4 курсов АГУ (364 человека). Опрос проводился методом анкетирования (рис. 1).

Анкета опроса студента		
Форма обучения _____ Специальность _____ Курс _____ Группа _____ Год _____		
Анкета «Вредоносное ПО в университете»		
Уважаемые студенты! В университете проводится опрос с целью выявления угроз информационной безопасности посредством заражения устройств вредоносным ПО на основе изучения ваших мнений и пожеланий. Если затрудняетесь ответить, оставьте поле пустым.		
Заполните таблицу.		
Аудитория, № компьютера	Название вредоносного ПО	Признаки заражения

Рисунок 1. Пример анкеты для опроса студентов на предмет выявления вредоносного ПО на флеш-накопителях

По результатам анкетирования было выявлено, что наиболее часто встречающимися вредоносными программами в университете являются: 1) Флеш-вирус f4448e25.exe и 2) Вирус autorun.inf

Флеш вирус f4448e25.exe

Вирус f4448e25.exe довольно распространен в глобальной сети Интернет. Он скрывает файлы на внешнем запоминающем устройстве (ВЗУ), вследствие чего они становятся недоступными для пользователя.


К основным «симптомам заражения» относятся:

- визуальное исчезновение файлов на накопителе, при неизменном объеме памяти;
- визуальное исчезновение файлов на накопителе, при значительном уменьшении объема памяти;
- замена всех файлов и папок на носителе на соответствующие ярлыки.

Процесс ликвидации данного вредоносного ПО проводится в несколько этапов. Первоначально необходимо проверить Флеш-накопитель антивирусным ПО. После проверки следует перейти к восстановлению утраченных файлов. В рамках исследования для решения данной задачи (восстановления файлов) был написан bat файл, представленный на рис.2 [1].

После запуска Recovery.bat компьютер запросит букву, соответствующую «зараженному» ВЗУ. После того, как будут удалены ярлыки вместо папок и само вредоносное ПО, пользователю будет показано содержимое устройства.

```

 Recovery.bat
:lable
cls
set /p disk_flash="Буква флешки: "
cd /D %disk_flash%
if %errorlevel%==1 goto lable
cls
cd /D %disk_flash%
del *.lnk /q /f
attrib -s -h -r autorun.*
del autorun.* /F
attrib -h -r -s -a /D /S
rd RECYCLER /q /s
explorer.exe %disk_flash%

```

Рисунок 2. Recovery.bat

Вирус autorun.

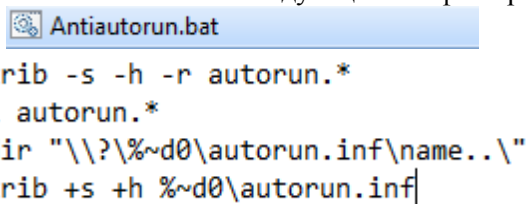
Изначально безобидное предназначение файла автозапуска autorun.inf стало использоваться, как эффективный способ распространения компьютерного «червя» win32 autorun. Сам по себе файл autorun.inf не содержит исполняемый код вредоносного ПО, он является лишь средством запуска autorun «червя». Такие вредоносные программы распространяются посредством копирования исполняемого файла на съемные носители и прописываясь в файл автозапуска autorun.inf, таким образом заражая их. [1] Губительному воздействию подвержены абсолютно все внешние накопители.

«Симптомы заражения»:

- наличие файла autorun.inf и скрытой папки RECYCLER на внешнем накопителе. Данные файлы скорее всего будут скрытыми, поэтому необходимо предварительно убедиться, что поставлена соответствующая галочка в настройках вида папок;

- отсутствие возможности запуска (чтения, выполнения) или удаления файла autorun.inf;
- отсутствие в меню Проводника «Сервис» пункта «Свойства папки».

Для лечения «вируса» autorun.inf был написан следующий bat файл рис.3.



```
attrib -s -h -r autorun.*
del autorun.*
mkdir "\\?\%~d0\autorun.inf\name..\"
attrib +s +h %~d0\autorun.inf
```

Рисунок 3. Antiautorun.bat

На первом этапе файл Antiautorun.bat удаляет существующий вредоносный файл, а затем создает неудаляющуюся папку autorun.inf. Созданную папку таким методом уже ничем невозможно удалить. Единственный способ удалить папку – это отформатировать флеш-накопитель.

Приведенные выше bat файлы позволяют ликвидировать последствия от заражения ВЗУ вредоносным ПО. Однако более действенным методом борьбы с данными программами является предупреждение заражения носителей и распространения вредоносного ПО в сети.

В целях предупреждения угрозы распространения вредоносного ПО в локально-вычислительной сети АГУ и дальнейшего заражения съемных носителей была предложены мероприятия по защите ВЗУ студентов, включающие в себя организационные и программные средства и меры защиты информации:

1. Организационные меры по защите информации:

- Проведение лекционного курса на тему «Предупреждение заражения ВЗУ», дающего студенту базовые представления об основных источниках и признаках заражения ВЗУ вредоносным ПО, а также об эффективных средствах предотвращения заражения и ликвидации последствий от его действия.

- Создание ознакомительной инструкции пользователя студента по безопасной работе на компьютере в компьютерном классе. Инструкция содержит свод правил, выполнение которых сводит к минимуму угрозу заражения ВЗУ вредоносным ПО.

2. Программные средства защиты информации:

Рекомендация к профилактике и устранению последствий заражения ВЗУ вредоносным ПО на домашнем компьютере:

- Установка антивирусной утилиты «Зоркий глаз», способной обнаружить подавляющее большинство вредоносных программ, обитающих на флеш накопителях (даже новых и ранее неизвестных) [2].

- Установка скрипта Autostop, способного противостоять autorun-вирусам;

- Установка Panda Internet Security;

- Предоставление открытого доступа студентов к разработанным bat файлам.

Внедрение данных мероприятий должно позволить значительно снизить угрозу заражения ВЗУ студентов ФГБОУ ВПО АГУ посредством распространения вредоносного ПО на различные носители данных.

Заключение. В ходе исследования был проведен опрос студентов АГУ, в результате которого был выявлен список наиболее часто встречающихся вредоносных программ в локальной сети

университета и предложены методы борьбы с ними путем предупреждения и ликвидации последствий заражения. В результате был предложен комплекс мероприятий, позволяющий обезопасить взаимодействие различных накопителей информации и рабочего компьютера, избежав потери/искажения данных.

Литература

1. Некром О. Вирус скрыл файлы на флешке: [Электронный ресурс] /Некром О.// Компьютерная грамотность: интернет центр компьютерной грамотности,2014. – Режим доступа: [www.url: http://osnov-computer.ru/](http://osnov-computer.ru/). – 14.31.2014.
2. Зоркий глаз [Электронный ресурс]. – Режим доступа: <http://www.exnax.narod.ru/antivir.htm>. – 12.03.2012.
3. Михайлов, А.В. Компьютерные вирусы и борьба с ними/ Михайлов, А.В. – Москва: Диалог-МИФИ,2011. – 104 с.
4. Крис Касперски. Компьютерные вирусы изнутри и снаружи/ Крис Касперски. – СПб: Питер,2006. – 526 с.

ЧИСЛЕННОЕ РЕШЕНИЕ УРАВНЕНИЯ ВЫБОРА ОПТИМАЛЬНОЙ СТРАТЕГИИ СНИЖЕНИЯ РИСКА

М. М. Чудинов

*руководитель – ассистент кафедры информационной безопасности Р. Ю. Дёмина
Астраханский государственный университет, г. Астрахань*

Введение. Оценка рисков и управление их уровнем занимает одну из ключевых позиций в сфере информационной безопасности.

Хранение конфиденциальной информации о своих клиентах (номера кредитных карт, адреса и т. д.) свойственно многим компаниям. При этом должен быть обеспечен достаточный уровень контроля хранения информации и процессов её обработки, потому что с каждым днём риск несанкционированного доступа к ней, либо утраты (повреждения) этой информации становится всё больше.

Решение о применении какой-либо политики обеспечения безопасности принимаются только после тщательной оценки рисков.

Существует множество подходов по исследованию проблемы управления рисками. Один из них рассмотрен в [1].

В статье рассмотрена математическая модель, позволяющая формализовать процедуру принятия управленческих решений в области риск-менеджмента. На её основе было выведено уравнение для выбора оптимальной стратегии снижения риска:

$$S_U^2 \cdot (U_0 - U) - S_P^2 \cdot a \cdot b \cdot e^{-bU} \cdot (P_0 - a \cdot e^{-bU}) = 0 \quad (1),$$

где S_U – уровень затрат на снижение вероятности возникновения неблагоприятного события (НС); S_P – уровень затрат на снижение ущерба от возникновения (НС); a – соответствует вероятности, с которой допускается возникновение незначимого ущерба; b – определяет скорость падения допустимой вероятности нанесения ущерба; U_0 – минимальное значение ущерба; P_0 – текущее значение вероятности возникновения ущерба U_0 .

Данное уравнение трансцендентно и не имеет аналитического решения. Поэтому необходимо задействовать численные методы.

На сегодняшний день существует множество разнообразных методов решения трансцендентных уравнений. Они различаются между собой по используемым подходам и, как следствие, эффективности, которая может оцениваться количеством итераций или временем вычисления.

Целью работы является анализ наиболее распространенных численных методов и выбор наиболее подходящего для рассматриваемой задачи.

Численные методы решения уравнений

Рассмотрим некоторые широко используемые численные методы. Для уравнений, не имеющих аналитического решения, используются итерационные методы с заданной степенью точности.

Решить уравнение *итерационным методом* значит установить, имеет ли оно корни, сколько корней и найти значения корней с нужной точностью.

СОДЕРЖАНИЕ

ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

<i>Алексеева Е. Н., Рясная В.С.</i> Личность в виртуальной и дополненной реальности	3
<i>Аникин В.А.</i> Разработка рекомендаций по защите локальных сетей от внешних угроз	4
<i>Аникин В.А.</i> Анализ уязвимостей протокола ARP	6
<i>Белова А.А.</i> Обзор однофотонных регистраторов	7
<i>Болтенко Е.П., Сорокина О.Г., Харитонов Е.Г.</i> Математическая модель инфокоммуникационной системы предприятия на основе матрицы ресурсов	10
<i>Бороденко В.В., Корольков А.Э.</i> Структура модулярных цифровых фильтров с устройством масштабирования	12
<i>Братченко Н.Ю., Серветник О.Л.</i> Анализ процессов оценки качества инфокоммуникационных услуг	15
<i>Брынза С.Ю.</i> Функции сетевых сообществ	18
<i>Бурмистров В. А., Гавришев А. А.</i> О защите радиоканала за счет использования стохастических ортогональных кодов	19
<i>Васюта С.Д., Ганжа А.Е.</i> Преимущества технологии NFC и области её применения	22
<i>Гиргель Г. В., Шмырин А. Ю.</i> Применение методов сетевого кодирования для повышения эффективности работы сенсорной сети	25
<i>Гладких А.А.</i> Технология Li-Fi и возможности её совместного использования с технологией Wi-Fi. 28	
<i>Гончарова Т.О., Доновская Т.В., Ковалёва А.В.</i> Расчет и экспериментальное исследование фильтра на встречных стержнях	30
<i>Гостюнина В.А.</i> Разработка программно-аппаратного комплекса системы родительского контроля в сети Интернет	32
<i>Гриневиц Т. В., Орлянская Я. С., Лукьянов М. В.</i> Мобильные приложения в образовании	35
<i>Гурова Д. Г.</i> Помехоустойчивость полиномиальной системы класса вычетов	37
<i>Гусева Д. В., Шевченко Н. И.</i> Алгоритм кодирования сообщений с помощью тригонометрической функции двух аргументов	39
<i>Евсеев Я. С.</i> Методы оптимизации заголовка документа в HTML5	42
<i>Зеленский С.С.</i> Анализ технологических и теоретических решений в области маршрутизации на основе качества обслуживания	45
<i>Зимовец К. С., Корольков А.Э.</i> Применение метода расчета коэффициентов цифрового фильтра с помощью согласованного z-преобразования	47
<i>Ивакина Д.А.</i> Обзор протоколов тунелирования	49
<i>Ивакина Д.А.</i> Исследование уязвимостей информационной безопасности банковских структур РФ	52
<i>Кирьянцев А. С.</i> Динамическая генерация ключей и подписей в приложении Cryp2Chat.....	55
<i>Кодинцев В.Г., Корольков А.Э.</i> Анализ методов разработки рекурсивных цифровых фильтров	57
<i>Коняев А.В., Сиволапенко Е.В., Величко А.А., Персиянова А.В.</i> К вопросу о роли информационно-коммуникационных технологий в образовании в области устойчивого развития	59
<i>Корольков А.Э., Бороденко В.В. Рыжов С.В.</i> Анализ точности и количества коэффициентов на АЧХ не рекурсивного	61
<i>Косяк Н. В.</i> GSM или CDMA: какая разница и что лучше	64
<i>Кузьменко В.В.</i> Аналитический обзор биометрических методов распознавания лиц	66
<i>Лаган Е.А.</i> Радиоканалы в системах охранно-пожарной сигнализации	68
<i>Лещанов Д.В., Запорожец Ю.Ю.</i> Перспективные направления развития информационно- телекоммуникационных технологий в области образования	70
<i>Мамонтова Н. А.</i> Расчет цифровых радиорелейных линий связи	72
<i>Новикова А.А.</i> Разработка комплексной системы автоматизированного радиомониторинга и принятия решений на основе анализа видеопотока	75
<i>Павлов К.В.</i> Модель абсолютного порога слышимости в системе MATLAB+Simulink	77
<i>Папе А.В.</i> Модель арифметико-логического устройства в пакете Simulink	80
<i>Пелипенко А. В., Свердлова А. А.</i> Обзор технологий оптоволоконной связи	82
<i>Пелипенко А. В., Шмырин А. Ю.</i> Анализ методов измерения параметров передачи цифровых сигналов	84
<i>Пилипенко И.А., Задорожная Т.В.</i> Повышение вероятности правильной передачи цифровых потоков в каналах распределенной системы радиосвязи	87

Проценко С.В., Сухинов А.А. Пространственно-двумерная модель транспорта наносов в прибрежной зоне и параллельный алгоритм ее численной реализации	89
Свердлова А. А., Шмырин А. Ю. Обзор современных технологий беспроводной связи	92
Свиридов В.В. Особенности увольнения персонала, владеющего конфиденциальной информацией	94
Братченко Н.Ю., Серветник О.Л. Процессно-ориентированный подход к управлению качеством инфокоммуникационных услуг	96
Попков Д.В. Применение PTZ-камер в современных системах видеонаблюдения	99
Тяпкина К.Д. Информационные и коммуникационные технологии в науке и образовании	101
Футерман М.Ю. Оптическое волокно, витая пара, коаксиальный кабель. Чему быть?	102
Болтенко Е.П., Харитонов Е.Г. Гибридная модель пересылки пакетов в системе передачи данных в среде имитационного моделирования AnyLogic	104
Чернявская А.В. Применение профиля технологических решений в задачах разработки виртуальных образовательных сред	107
Чеховский А. С. Анализ технологий для VoIP звонков в WEB-приложениях	109
Пиманьков Е.В., Демин М.А., Некрасов Г.А., Изотов М.Х. Развитие сектора телекоммуникаций как основы информационного общества	111
Демин М.А., Некрасов Г.А., Пиманьков Е. В., Изотов М. Х. Особенности волоконно-оптических линий связи	112
Бондарева Е.Н. Обзор технологий беспроводной высокоскоростной передачи данных для мобильных устройств	114
Моисеенко В.А., Зикеев В.В., Сапелкин И.В. Виртуальная реальность сети Интернет	116

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Аветисян Р.Ю. Многопользовательские ролевые онлайн-игры как угроза психологической безопасности личности	119
Аликберова Д.О. Собеседование кандидата как метод отбора кандидатов	120
Аликберова Д.О. Современные подходы к системе подбора персонала, работающего с информационной безопасностью в организации	122
Алтунина Н. А., Ложкин С.А., Хачатрян А.Х. Обеспечение информационной безопасности систем контроля и управления доступом	124
Алтунина Н. А., Ложкин С.А., Хачатрян А.Х. Контроль защищенности выделенного помещения	127
Амплиев Е.А., Шилов А.К. Влияние увеличения популярности биометрических технологий на её развитие	129
Ананченко А.Ю., Лигостаева Д.О. Повышение защищенности сетей IP-телефонии	130
Анзин И.В., Карпов И.Н. Разработка протокола взаимодействия между модулями для контроля целостности файловой системы	133
Ахмедова А.Г., Садыкова У. В. Создание автоматизированной системы поддержки организационных мероприятий по защите информации	135
Антипов А.С., Кузьменко Л.А. Анализ угроз информационной безопасности в системах облачных технологий	138
Белозёрова К.С. Информационная безопасность в современном обществе	140
Белоусов Р.Г., Колесников О.В. Обзор параметров и характеристик защищаемой информационной системы	142
Березкин Д.В. К вопросу оценки рисков утечки конфиденциальной информации	144
Березнев А.А. Человек как главный источник угрозы защищаемой информации	145
Бордак И.В. К вопросу применения марковских случайных процессов в теории защиты информации	148
Бульков Т.А., Сычев А.Д. Виды угроз информационной безопасности на объекте	149
Вепринцева О.В., Чумичев В.С., Джамбинов С.В., Гайдуков А.Б. Виды и сравнительная характеристика криптографических протоколов	151
Ворошилов Р.А., Минкина Т.В. Перспективные системы защиты информации при формировании начальной популяции в процессе генетического поиска	153
Высотенко А. А., Топорков К. И., Пелешенко В. С., Фролов Е. А. Разработка подсистемы защиты на основе модели защищенной базы данных на примере «Базы знаний мониторинга состояния ионосферы»	156

Галкина Т.Ю. Рекомендации по проведению анализа системы информационной безопасности в производственной среде	158
Гнедышев А.Г., Гусева Л.Л., Куннуев З.А., Лукьянов А.К. Разработка ультрабюджетного вибрационного охранного извещателя на базе пьезоэлемента	160
Голошубов К.С., Ложечкин А.А. Исследование проведения проверки по выполнению норм эффективности защиты речевой информации от утечки по акустическому каналу	163
Голошубов К.С., Ложечкин А.А. Исследование модели угроз безопасности информации от утечки по акустическому каналу и анализ методов защиты информации от несанкционированного доступа	165
Горбачев С.В. К вопросу защиты информации, циркулирующей в локальной вычислительной сети от внешних угроз	167
Денисенко И.В. Обзор клавиатурных шпионов	168
Денисенко И.В., Пилипенко А.В. Международные стандарты информационной безопасности в Интернете	170
Джадтоева А.Р. Анализ уровня информационной безопасности в облачных хранилищах ...	173
Домащенко А.А., Беспутнев В.В., Минкина Т.В. Актуальность защиты информации в сети интернет	174
Ермолов В.В. Защита информации при автоматизированной обработке жалоб граждан в государственной инспекции труда в астраханской области	176
Ерохин А.В. SSH – безопасный протокол сетевого уровня	179
Забокрицкий Е.И., Заводнов В.С. Предпосылки угроз информационной безопасности объекта	181
Иванов И.И. Исследование предпосылок развития систем биометрической аутентификации по голосу	183
Карасева Е.С., Вельц А.Г. Информационная безопасность в бизнесе	187
Кипарисова А.И., Краснонёрова А.А. Обеспечение доступа к информационным системам высшего учебного заведения в случае утраты ключевой информации	189
Кравченко К.Л., Петров М.Ф. Оценка приемлемого уровня риска информационной безопасности в филиале пао «МРСК Юга» - «Астраханьэнерго»	192
Краснонёрова А.А., Кипарисова А.И. Воздействие на персонал организации с целью повышения уровня информационной безопасности	194
Кузьменко Л.А., Колесников О.В., Антипов А.С. Построение модели развития популяции нейронных сетей на базе моментных уравнений	197
Кузьменко Л.А., Колесников О.В., Масленников И.А. Необходимые и достаточные условия устойчивости модели развития популяции нейронных сетей	199
Кукушкин Г.В. Исследование проблемы оценки эффективности защиты систем электронного документооборота	203
Кулебякин Р.Б., Частухина Л.В. Реализация класса Hashtable для управления и работы с группой связанных объектов на языке программирования C#	205
Кулебякин Р.Б., Частухина Л.В. Реализация динамической библиотеки для расшифровки паролей на языке C++	208
Курилов О.С. Некоторые особенности защиты информации в сетях Wi-Fi	212
Лалин Д.И., Соколова Я.В. К вопросу кадрового обеспечения комплексной системы защиты информации	214
Лецев А.Е. Сравнение алгоритмов «ГОСТ Р 34.12-2015» и «AES»	216
Ложечкин А.А., Голошубов К.С. Биометрическая идентификация личности по радужной оболочке глаза	218
Ложечкин А.А., Голошубов К.С. Комплексный подход к организации системы защиты информации на предприятии	221
Локовей А.В. Математическое моделирование оценки влияния дополнительных средств защиты на загрузку вычислительной системы	223
Макарова Е. А. Информационная безопасность в коммерческих организациях и способы ее защиты	224
Макарова А.В. Исследование метода пересчета ортогональных базисов при деградации структуры непозиционного спецпроцессора функционирующего в ПСКВ	226
Марков Д.С. Защита информации организации, как проблема современности	229
Марченко Е.И., Рогова А.А., Давыдов В.С. Организация расследовании неправомерного доступа к компьютерной информации	231

Мелкозёрв Д. М. Анализ моделей управления доступом к информации	232
Михно П.С. Атаки на мобильные устройства	235
Михно П.С., Сидоренко Э.О. Информационная безопасность как инструмент профилактики и противодействия терроризму	236
Новиков О.Г. Перспективы операционной системы «Хамелеон»	238
Носиров З.А., Честнов А.А. Разработка алгоритма защиты сети от DOS-атак на основе качественного анализа трафика	239
Орлов И.А., Пурчина О.А., Фугаров Д.Д., Ефремов С.В. Численное исследование кривой намагничивания магнитодиэлектрического датчика переменного тока	242
Остапенко Д.А., Фугаров Д.Д., Пурчина О.А., Петренко А.И. Имитационное моделирование системы стабилизации амплитуды испытательного тока в процессе диагностики коммутационных элементов электроустановок	244
Парахин Д.В. Защитные механизмы персональных данных в мобильных устройствах на базах IOS, Android, Windows phone	247
Пахотин М.С., Калмыков Е.Г. О модели разграничения доступа к приложениям в автоматизированной информационной системе	248
Перепелица А.В. Информационные технологии в авиатехнике	250
Петров М.Ф., Кравченко К.Л. Организация защищенного обмена информацией между мобильными группами и головным офисом в ПАО «МРСК Юга» – «Астраханьэнерго»	253
Петросян С. М. Оценка состояния безопасности информационной системы предприятия на основе нечетной модели с лингвистической шкалой	256
Пилипенко А.В. Скрытый ICMP-канал	258
Подушкина М.А. Особенности организации систем условного доступа CAS при предоставлении услуг телевидения	260
Ростовцева И.А., Амплиев А.Е. Лазерная система охраны объекта телекоммуникаций	262
Саргасян А.А. Оценка эффективности систем физической защиты объектов информатизации	264
Сафонова Н.В. Имитационное моделирование процесса ограничения доступа к информационным ресурсам в условиях dos атаки	265
Свирь А. Акустические каналы утечки информации в компьютерных системах	267
Селезнев А.Г., Пурчина О.А., Фугаров Д.Д., Титаренко В.И. Математическая модель магнитодиэлектрического датчика тока для устройств диагностики коммутационных аппаратов электроустановок	269
Сенченко Ж.П. Защита ВОСП от несанкционированного съема информации	271
Скребцов Е.В., Кузема В.Я. Особенности моделирования безопасности обработки информации в компьютерных системах	274
Соколова Я.В. К вопросу защиты информации в работе кадровой службы	277
Сушкова М.В. Программный продукт для изучения принципов создания и использования электронной подписи на основе асимметричных криптоалгоритмов	280
Текеев З.Х.-М. Оптимизация аппаратной реализации операции умножения по модулю	282
Тимофеев Е.А., Ливенская Е.В. Анализ пожарной безопасности помещения архива на примере филиала компании ООО «РосИнтеграция» в городе Ставрополе	285
Тимофеев Е.А. Анализ методов и средств защиты информации в виртуальных социальных сетях на примере сети «ВКонтакте»	287
Тимощенко А.В. Обеспечение конфиденциальности хранящейся информации при помощи технологии «прозрачного» шифрования	290
Ткачук И.Д., Фугаров Д.Д., Пурчина О.А., Арефьев Б.А. Лабораторные стенды на базе аппаратно-программных комплексов	292
Тохчуков А. Х., Тер-Саркисов Б. О., Крамин А. П. Принципы построения системы авторизации и аутентификации с использованием баз данных	293
Троянов А.А., Новиков О.Г. Характеристика организационных мер защиты информации	295
Троянов А.А. Методы аудита изменений в Active directory Microsoft Windows Server 2008r2	299
Фугаров Д.Д., Пурчина О.А., Черненко И.В., Чернов Р.Ю. Измерение токов больших амплитуд в процессе диагностики автоматических выключателей переменного тока	301
Ходакова В.А., Евдокимов И.Р., Лобжанидзе Н.Д. Анализ критериев выбора DLP-системы для обеспечения информационной безопасности предприятия	303
Ходакова В.А., Маршанский Н.А., Барышев Д.М. Анализ подходов к классификации DLP-систем	305

Холин А. В. Советы по защите домашней сети	308
Холин А. В. Как защитить личные данные от утечек	310
Чапайкина Н.Е. Анализ стандартов в области биометрии	311
Черненко Е.И., Шилов А.К., Демидов Н.Н. Обнаружение данных и способы их классификации для упрощения безопасности органов политики и управления	312
Честнов А.А., Носиров З.А. Методы борьбы с вредоносным программным обеспечением на съемных носителях	314
Чудинов М.М. Численное решение уравнения выбора оптимальной стратегии снижения риска	317
Шендриков Н.В. Обзор основных технологий активной защиты речевой информации на предприятии	319
Шерстобитов А.В. Анализ методов оценки защищенности информационной системы от ошибок персонала	322
Щербинина Ю.В., Колесников О.В. Регистрация событий информационной безопасности базы данных распределенной системы аутентификации и авторизации пользователей	324
Язмухамедов И.М. Обеспечение информационной безопасности в региональной информационно-аналитической медицинской системе	325
Яковлева А.П., Яковлева Е.П. Способы защиты распределенных сетей WAN	328
Яковлева Е.П., Яковлева А.П. Факторы, влияющие на безопасность банковских информационных систем	329

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕШЕНИЯ ЭКОНОМИЧЕСКИХ ЗАДАЧ

Бондаренко Ю.В., Ширяев Н.В. Информационные технологии в реинжиниринге бизнес-процессов	331
Губская Т.Е. Моделирование бизнес-процессов на примере сервиса и продажи картриджей для лазерных принтеров	333
Денисенко Ю.Н., Муратова Е.Р. Public relations - как инструмент создания и поддержания репутации бренда	336
Жулин М. Д., Корж Е. А., Сушко Д. С. Виртуальные организации как новая форма управления в среде электронно-сетевых коммуникаций	338
Завелеев Д. В. Разработка программы на C++ решения нелинейных уравнений методом последовательных приближений (методом итераций)	341
Кольган М. В., Сарафанова А. Е. Влияние информационных технологий на систему управления предприятием	343
Кольган М. В., Умеренкова Н.В. Использование CRM-систем для анализа потребительской лояльности	345
Кошкош О.С. Вопросы оптимизации системы коммуникаций сотрудников образовательного учреждения	348
Куцевалов К.В. Декомпозиция риска на предприятии малого бизнеса	349
Ловяников П.С. Корпоративный сайт в виде менеджера задач	351
Моисеенко В.А., Зикеев В.В., Сапелкин И.В. Виртуальная реальность сети Интернет	353
Олейникова Ю.А., Денисенко Ю.Н. Вопросы повышения эффективности реализации кластерной политики регионального экономического развития (на примере Ростовской области)	355
Самарин А. А., Скрыпник Д. О. Снижение затрат и повышение отдачи от внедрения информационных систем	357
Сейтнязова Н. Р. Экономические аспекты информационных технологий	359
Смаргунова А. С., Олейников К. А. Автоматизированный выбор плана сертификационного контроля качества товаров и услуг в среде MathCad	360
Шабанова Д.В. Роль информационных технологий в современной экономике	363
Шутова Ю.А. Постановка задачи установления разрешимости уравнения модели Леонтьева и пути ее решения использованием IT-технологий	366

Научное издание

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
(Ставрополь, 14-18 декабря 2015)
Часть 2

Издается в авторской редакции

Компьютерная верстка М. И. Толмачёв

Подписано в печать 16.12.2015

Формат 60x84 1/8

Усл. п. л. 43,48

Уч.-изд. л. 42,72

Бумага офсетная

Заказ 295

Тираж 500 экз.

Отпечатано в Издательско-полиграфическом комплексе
ФГАОУ ВПО «Северо-Кавказский федеральный университет»
355028, г. Ставрополь, пр-т Кулакова, 2.