

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

Современные отечественные операционные системы могут пойти по двум реальным направлениям развития. В первую очередь хочется отметить вполне оправданную заинтересованность военных. Именно для них важно защищенное отечественное программное обеспечение. Второй путь можно отметить в качестве «патриотической разработки»[4].

Иногда в интернете встречаются проекты, которые разработаны авторами, анонсирующими российскую операционную систему. Стоит упомянуть о таких операционных системах, как «Роса», «Патриот ОС», «Фантом», PhantomOS, KolibriOS. Операционная система PhantomOS (<http://www.dz.ru/solutions/phantom>) от Дмитрия Завалишина система наиболее подходит под громкое звание российской операционной системы. Но она настолько оригинальна, а заложенные в её основу идеи настолько необычны, что она лет на 10 опередила своё время[4].

### Литература

1. Википедия. Хамелион. [Электронный ресурс] URL: <https://ru.wikipedia.org/wiki/Хамелеоны> (дата посещения 29.11.2015)
2. Интернет ресурс: [Электронный ресурс] URL <http://l4os.ru/> (дата посещения 29.11.2015)
3. Hameleon [Электронный ресурс] URL <http://habrahabr.ru/company/hameleon/profile/> дата посещения 29.11.2015
4. Phantom. [Электронный ресурс] URL: <http://www.dz.ru/solutions/phantom>) дата посещения 30.11.2015)

## РАЗРАБОТКА АЛГОРИТМА ЗАЩИТЫ СЕТИ ОТ DOS-АТАК НА ОСНОВЕ КАЧЕСТВЕННОГО АНАЛИЗА ТРАФИКА

**З. А. Носиров, А. А. Честнов**

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

Быстрое и повсеместное распространение Интернета привело к бурному развитию компьютерных сетей, что позволило существенно расширить возможности для компаний, предоставляющих свои услуги через глобальную сеть. К глобальной сети подключены миллионы устройств и пользователей, благодаря чему множество фирм и потребителей взаимодействуют между собой. Для реализации своих услуг компании используют информационные ресурсы, которые позволяют выполнять обработку информации, относящуюся к их клиентам. Некорректная работа или недоступность сервисов может повлечь значительные потери, как финансовые, так и клиентские. Именно по этим причинам в последние годы информационные ресурсы и сервисы все чаще сталкиваются с вредоносным воздействием, осуществляемым с использованием протоколов межсетевого взаимодействия – удаленной сетевой атакой. Частой причиной нарушения доступности ресурсов являются DDos-атаки на сервер, где физически расположен сайт. Уязвимости, через которые реализуются DDos-атаки сводятся к:

- Ошибкам в программном обеспечении, которая работает на атакуемом сервисе
- Недостаткам протоколов сети [1]
- Ограничениям в пропускной способности канала связи.

Источником DDos-атаки является определенное количество зараженных компьютеров, объединенных в сеть, именуемую «ботнет». Зараженные компьютеры, управляются определенным портом или же откликами на команды в IRC-чате (англ. InternetRelayChat — протокол прикладного уровня для обмена сообщениями в режиме реального времени). Впрочем, в настоящее время получили распространение ботнеты, управляемые через сайт или же по принципу p2p-сетей.

Согласно отчёту [2], размещенному фирмой Arbor Networks, предоставляющей одни из наилучших решений для обеспечения стабильной работы информационной системы и имеющей большой опыт в вопросах борьбы с DDos-атаками, число DDos-атак со скоростью 20 Гбит/с в 2014 году, по сопоставлению с аналогичным периодом 2013 года увеличилось вдвое. Больше 100 DDos-атак со скоростью 100 Гбит/с были зафиксированы за 2014 год. 46% атак относились к всеохватывающим DDos-атакам, использующим отправку мусорного трафика, SYN-флуд и UDP Flood, а также атаки с использованием протоколов уровня приложений. Впрочем, в сопоставлении с прошлыми годами соотношения заявленных атак этого типа практически не изменились по отноше-

нию к большинству служб, таких как HTTP, DNS и SMTP. Есть определённая обеспокоенность по поводу компрометации (факта доступа постороннего лица к защищаемой информации) рабочих станций. Есть вероятность того, что компьютеры, принадлежащие к корпоративной сети, имеют все шансы быть частью ботнета. Эта обстановка приводит к усилению эффекта от атаки, так как защита может быть направлена только на внешнюю сеть, игнорируя внутрисетевой корпоративный трафик. Повышение числа хостов, входящих в ботсети, не вызывает удивления, беря во внимание численность и сложность существующих на сегодняшний день вирусов, темпы их развития и исходящую из этого невозможность построить надёжную систему защиты на основе антивирусных программ и систем обнаружения проникновений.

Рассмотрим принципы, по которым была произведена самая мощная DDos-атака. Согласно проведённому отчету [3] в основе данной атаки лежит UDP-флуд(сетевая атака типа «отказ в обслуживании», использующая без сеансового режима протокола UDP),который сопровождается SYN-флудом. Это указывает на наличие достаточно большого числа подконтрольных серверов.

В ходе данной атаки осуществлялось умножение первоначального вредоносного трафика за счёт отражения DNS-запросов через DNS-резолверы, которые установлены у каждого Интернет-провайдера. Обычно DNS-резолверы сконфигурированы так, чтобы обрабатывать только запросы своих пользователей, но существует большое количество компаний, которые неправильно их сконфигурировали, так что резолверы принимают запросы от любого пользователя интернета. Любопытно заметить, что в значительной мере усиление происходило благодаря большим ключам DNSSEC, которые включены в тело ответа, а ведь протокол DNSSEC внедрялся с целью повысить безопасность системы DNS.



Рис.1 Схематическое представление DDos-атаки

Существуют три основных решения по защите от атак:

- Программные решения;
- Аппаратные решения;
- Облачные решения.

Программные решения – самое распространённое на рынке информационных технологий, представляет собой набор правил фильтрации трафика, которые составлены разработчиком. Данное решение достаточно просто установить прямо на сервер, на котором работает ресурс, но поможет только от малозаметных атак.

Аппаратные решения – это распределенная сетевая структура с большим запасом пропускного трафика. Используются в масштабных сетевых структурах, таких как: точки обмена трафиком, дата-центры, крупные региональные провайдеры.

Облачные решения представляют сетевую структуру с большой пропускной способностью, в состав которой вводятся сервера для фильтрации вредоносного трафика. Таким образом, такая сеть постепенно будет отфильтровывать негативный трафик и снижать количество вредоносных пакетов.

Анализ трафика является достаточно сложной задачей, поэтому некоторые компании патентуют свои алгоритмы, например, компания “Black Lotus” запатентовала алгоритм «Human Behavior Analysis» [4], который определяет, кто генерирует трафик, человек или бот. Определив причины возникновения и проблемы, которые подлежат решению при борьбе с данным видом атак, появляется возможность найти методы решения данных проблем.

Рассмотрим атаку на предприятие со следующей топологией сети (рис.2).

Вредоносный и полезный трафик поступает во внутреннюю сеть. Сперва данные поступают на устройство анализа трафика. На данном этапе применяются простые алгоритмы фильтрации – статические таблицы, с помощью которых появляется возможность блокировать вредоносный трафик от определенных узлов. Управление данным узлом (заполнение таблиц) осуществляет сервер, который находится в сети за устройством анализа трафика. Этот сервер выполняет активную верификацию данных и собирает статистические данные о вредоносном трафике и его источниках возникновения. После установления источника вредителя он передает информацию о нем в устройство анализа трафика и блокирует его. Чтобы к заблокированным узлам не попали доверенные и другие рабочие устройства, сервер выполняет постоянный активный анализ всего трафика. Далее сервер выполняет лимитирование скорости и перенаправление проверенного трафика в сеть предприятия. Проверенный трафик доставляется до узлов назначения по корпоративной сети без проблем и перегрузок.

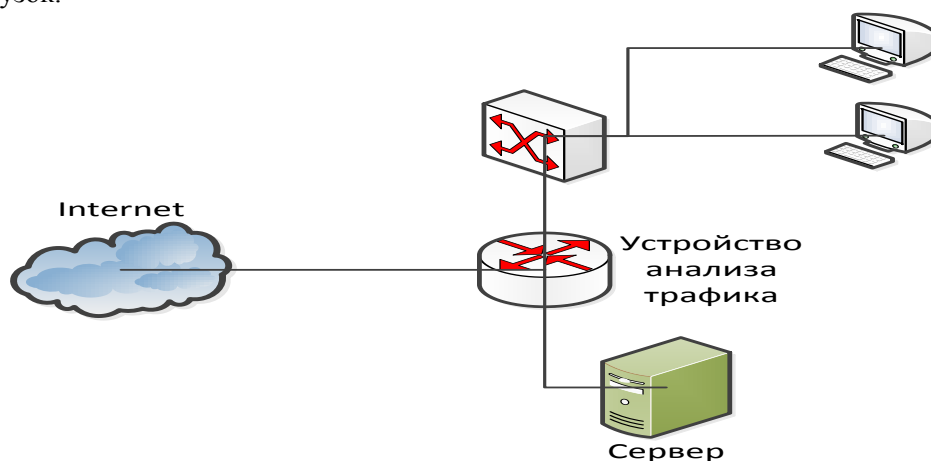


Рис.2 Схематическое представление моделируемой сети

Хотя существуют лидеры рынка в данной области, предлагаемый ими продукт является полностью закрытым. В отличие от решений с закрытым исходным кодом, открытые рекомендации позволяют привести методы и алгоритмы к единому стандарту, что сделает данные решения более гибкими и позволит пользоваться ими с большей эффективностью.

Несмотря на все передовые методы защиты от хакеров, методы проведения атак на шаг опережают тех, кто разрабатывает защиту от уязвимостей. Поэтому владельцам веб-приложений необходимо быть начеку вследствие постоянного появления новых угроз

### Литература

1. Лейкин А.В. Протоколы транспортного уровня UDP, TCPиSCTP достоинства и недостатки [Электронный ресурс] – Санкт-Петербург: СПбГУТ, 2013. – Режим доступа: <http://niits.ru/public/2013/2013-007-pp.pdf>
2. Максим зайцев. Статистика глобальной сетевой активности [Электронный ресурс] – Москва:KasperskyLab,2014 –Режим доступа: <http://qps.ru/z1PWV>
3. Abliz M. Internet Denial of Service Attacks and Defense [Электронный ресурс] – Pittsburgh : University of Pittsburgh,2011– Режим доступа: <http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf>

## ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ КРИВОЙ НАМАГНИЧИВАНИЯ МАГНИТОДИЭЛЕКТРИЧЕСКОГО ДАТЧИКА ПЕРЕМЕННОГО ТОКА

**И. А. Орлов, О. А. Пурчина, Д. Д. Фугаров, С. В. Ефремов**

руководитель – д-р техн. наук, профессор, заведующий кафедрой автоматизации и математического моделирования в нефтегазовом комплексе **Ю. Я. Герасименко**

Донской государственный технический университет, г. Ростов-на-Дону

Для обеспечения гальванической развязки силовых цепей переменного тока и измерительной схемы наиболее целесообразно применение измерительных преобразователей индукционного типа, однако применение трансформаторов тока не обеспечивает заданный диапазон линейности для всей шкалы задания величин переменных токов больших амплитуд при приемлемых массогабаритных характеристиках [1]. Решением является использование датчиков тока с магнитодиэлектрическим сердечником (МДТ) на основе порошковых материалов (*Iron Powder*) фирмы *Magnetics* (США). В литературных источниках описываются МДТ, созданные на основе порошков карбонильного железа марок P10, P20, P100 или ПС, которые применялись в корабельных энергетических системах [2]. Применение современных материалов даёт возможность обеспечить улучшенные характеристики МДТ при приемлемой погрешности преобразования первичных токов.

На рис. 1 представлена основная кривая намагничивания смеси *Magnetics 60*. В данном случае задача аппроксимации основной кривой намагничивания, с требуемой точностью простыми выражениями является крайне актуальной [2]. Предлагается основную кривую намагничивания магнитодиэлектриков на основе *Iron Powder* аппроксимировать формулой [3]:

$$B = A \ln(\alpha H + 1), \quad (1)$$

где  $B$  и  $H$  – координаты кривой намагничивания;  $A$  и  $\alpha$  – коэффициенты аппроксимации.

Для дальнейших расчетов выходных напряжений датчиков тока с магнитодиэлектрическим сердечником с наименьшей погрешностью необходимо достичь максимально возможного совпадения экспериментальной кривой и аппроксимирующей функции на начальном участке кривой намагничивания, в связи с чем на все аппроксимируемые выражения наложим дополнительные ограничения:

$$\lim_{H \rightarrow 0} B(H) = 0, \quad \lim_{H \rightarrow 0} \frac{dB}{dH} = \mu_H, \quad (2), \quad (3)$$

где  $\mu_H$  – начальная магнитная проницаемость основной кривой намагничивания.

Из основной формулы (1) в общем виде получим:

$$\frac{dB}{dH} = \frac{A\alpha}{\alpha H + 1}, \quad (4)$$

откуда при  $H \rightarrow 0$  имеем

$$\lim_{H \rightarrow 0} \frac{dB}{dH} = A\alpha. \quad (5)$$

С учетом выражений (3) и (5) можем записать:

$$A = \frac{\mu_H}{\alpha}. \quad (6)$$

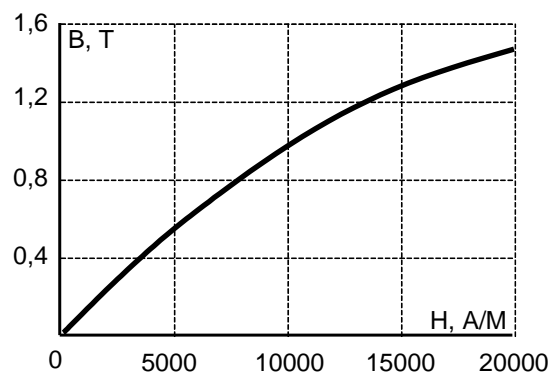


Рис. 1. Основная кривая намагничивания магнитодиэлектрика на основе смеси *Magnetics 60*

## 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

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

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

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



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

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

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

## **ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕШЕНИЯ ЭКОНОМИЧЕСКИХ ЗАДАЧ**

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