

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

ФГБОУ ВО «МИРЭА — РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»



«ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ»

**МАТЕРИАЛЫ
Всероссийской научно-технической конференции**

16 декабря 2022 г.



МАХАЧКАЛА - 2022

УДК 004
ББК 16.8
В74

Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской научно-технической конференции – Махачкала: ДГТУ, 2022 г. - 387 с.

В сборнике представлены материалы Всероссийской научно-технической конференции «Вопросы обеспечения безопасности в киберпространстве», которая состоялась в Махачкале 16 декабря 2022 года. Доклады и статьи отражают такие направления работы конференции как информационная безопасность, IT-технологии, информационные технологии, математика, нанотехнологии, технические науки, цифровая трансформация и кибербезопасность, безопасность телекоммуникаций.

Сборник предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций, специализирующихся в области информационной безопасности.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ:

Баламирзоев Н.Л.
Белов Е.Б.

к.э.н., доцент, врио ректора ФГБОУ ВО «ДГТУ», Председатель заместитель председателя ФУМО ВО ИБ, заместитель начальника Института криптографии, связи и информатики
Советник Делового совета Россия-АСЕАН при МИД России и Торгово-промышленной Палате РФ по информационной безопасности, генеральный директор ООО «Центр исследования безопасности информационных технологий»

Иванов О.В.

Мастер по этичному хакингу и тестированию на проникновение (Licensed Penetration Tester Master)

Красов А.В.

к.т.н., доцент, заведующий кафедрой «Защищенные системы связи» СПбГУТ

Крылов Г.О.

д.ф.-м.н., профессор кафедры «Безопасность телекоммуникаций» МТУСИ, профессор Финуниверситета, профессор НИЯУ МИФИ

Кубанков А.Н.

д.в.н., профессор, заведующий кафедрой «Безопасность телекоммуникаций» МТУСИ

Лось В.П.

д.в.н., профессор, президент МОО «Ассоциация защиты информации»

Малахов И.В.

к.в.н., доцент. Эксперт по информационной безопасности, сертифицированный инструктор «Крипто-Про», «Код-Безопасности»

Новиков С.Н.

д.т.н., доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» СибГУТИ

Петренко С.А.

д.т.н., профессор, руководитель направления Информационная безопасность, конструктор и практик в области защиты объектов КИИ РФ,

Пичкур А.Б.

к.ф.-м.н., доцент, председателя ФУМО ВО ИБ, начальник Института криптографии, связи и информатики ФГКОУ «Академия Федеральной службы безопасности Российской Федерации»

Рашидов А.Г.

начальник центра информационных технологий, связи и защиты информации Министерства внутренних дел Республики Дагестан

Хайретдинов Р.Н.

Президент Ассоциации по вопросам защиты корпоративной информации (BISA)

Шелухин О.И.

д.т.н., профессор, заведующий кафедрой «Информационная безопасность» МТУСИ

Магомедов Ш.Г.

д.т.н., доцент., заведующий кафедрой «Интеллектуальные системы информационной безопасности» Института кибербезопасности и цифровых технологий МИРЭА — Российский технологический университет

ОТВЕТСТВЕННЫЙ СЕКРЕТАРЬ:

Магомедов Р.М. - ст. преподаватель кафедры ИБ. Дагестанский государственный технический университет, г. Махачкала.

ISBN 978-5-907698-01-7

© Дагестанский государственный технический университет, 2022.

© Оформление. ИП Тагиев Р.Х., 2022.

Полученные результаты способствуют повышению защищенности проведения ВКС. Данный подход можно использовать в любом из режимов работы ВКС.

Список литературы:

1. Меджидов З.У. Исследование киберугроз посредством Threat Intelligence: вопросы теории и практики // Промышленные АСУ и контроллеры. 2022. № 3. С. 36-44.
2. Банк данных угроз ФСТЭК России [электронный ресурс] – Режим доступа. – URL: <https://bdu.fstec.ru/> (дата обращения: 20.10.2022).
3. Меджидов З.У. Особенности реализации распределенных сетевых атак // В сборнике: Актуальные проблемы информационно-телекоммуникационных технологий и математического моделирования в современной науке и промышленности. Материалы I Международной научно-практической конференции молодых учёных. Комсомольск-на-Амуре, 2021. С. 293-298.
4. Карижов А.А., Меджидов З.У. Анализ современных моделей оценки ценности информации // В сборнике: Наука и творчество: вклад молодежи. Материалы всероссийской молодежной научно-практической конференции студентов, аспирантов и молодых ученых. Махачкала, 2021. С. 54-57.
5. Меджидов З.У. Особенности социальной инженерии в свете информационной безопасности // В сборнике: Использование цифровых образовательных платформ в образовательном процессе. Сборник научных трудов Международной научно-практической конференции, VI Всероссийской научно-практической конференции. Махачкала, 2021. С. 55-62.
6. Меджидов З.У. Уязвимости к атакам по сторонним каналам в защищенных мессенджерах (на примере Whatsapp, Telegram И Signal) // В сборнике: Теоретические и прикладные вопросы комплексной безопасности. Материалы IV Международной научно-практической конференции. Москва, 2021. С. 170-172.

УДК 621.37(045)

НЕЙТРАЛИЗАЦИЯ ОПАСНЫХ ИСТОЧНИКОВ СИГНАЛОВ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

Подгорный Э.Р., студент;

Стерхова Т.Н., к.т.н, доцент

Удмуртский государственный университет, г.Ижевск
emil.podgorny1999@gmail.com

Аннотация: В статье рассмотрены методы и способы нейтрализации опасных источников из-за возникновения побочных электромагнитных излучений, при передачи по радио каналам связи, по каналам акустической информации.

Ключевые слова: нейтрализация, белый шум, помехоподавляющий фильтр, зашумление, опасные сигналы, акустоэлектрический преобразователь, разделительный трансформатор, генераторов шума, синфазные помехи.

В современном мире одной из основных угроз безопасности информации является утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала от его источника через среду до технического средства, осуществляющего прием информации.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения.

Носители информации в виде полей тока называются сигналами. Если информация,

содержащаяся в сигналах, секретная или конфиденциальная, такие сигналы представляют опасность для информации и называются опасными.

Опасные сигналы бывают двух типов функциональные и случайные. Функциональные – это сигналы. Обеспечивающие функционирование коммутационных станций и узлов для выполнения поставленных задач по обработке и передаче информации. Случайный сигнал - это сигнал со случайным характером изменения во времени. Для случайного сигнала невозможно определить значения в заданные моменты Источники сигналов — это источники, от которых могут распространяться несанкционированные сигналы защищаемой информации.

- акустоэлектрические преобразователи;
- излучатели низкочастотных сигналов;
- излучатели высокочастотных сигналов;
- наводки.

Акустоэлектрический преобразователь (АЭП) — это устройство, преобразующее акустическую энергию (так называемую энергию упругих волн в среде) в электромагнитную. Средства АЭП используются по функциональному назначению для создания микрофонов различных типов. Все АЭП можно подразделить на три вида: индуктивные, ёмкостные, пьезоэлектрические[2].

Низкое частотное опасное поле образуется при прохождении по проводам электрических проводов в диапазоне звука с конфиденциальными данными. Источником такого сигнала могут служить громкоговорящие устройства. *Источники высокочастотных сигналов* — высокочастотные генераторы, усилительные каскады, в которых возникают паразитные колебания, нелинейные элементы — диоды, транзисторы и другие активные радиоэлементы[2].

Фильтрация информационных сигналов. Основной способ устранения опасного сигнала, который циркулирует в технических средствах и системах обработки информации это фильтрация. Фильтрация электромагнитных источников осуществляется с целью устранения распространения нежелательных электромагнитных колебаний в пределах потенциального источника утечки информации.

Фильтрация электромагнитных приборов и наводок должна исключать их воздействие на приборы. Чтобы фильтровать сигналы в цепи питания, используются разделители *трансформаторов* и *фильтры помехоподавления*. Трансформаторы разделительного назначения должны обеспечить развязывание первичных и вторичных цепей по сигналам нагрузки. Это значит, что во вторичной цепи трансформатора не должны проникать наводки, которые появляются в первичной цепи трансформатора.

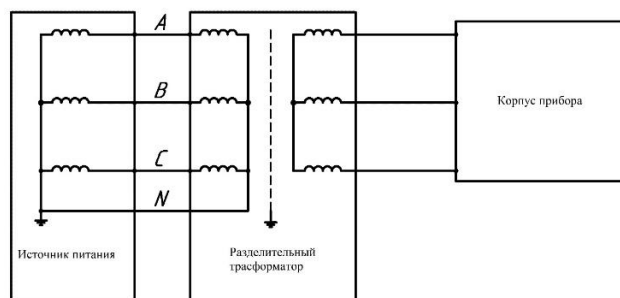


Рисунок 1. Схема разделительного трансформатора

Для решения ряда задач связанных с ослаблением симметричных наводок в цепи вторичной обмотки используются разделительные трансформаторы (рисунок 1). Их использование обусловлена наличием асимметричных наводок в цепи первичной обмотки.

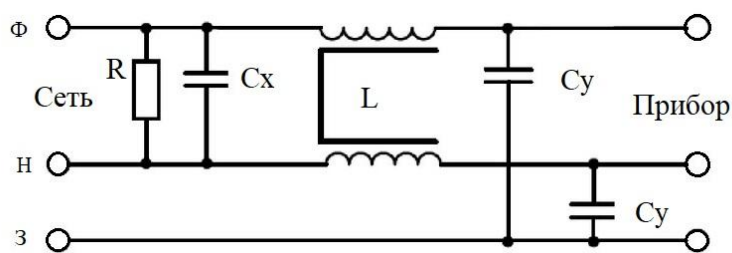


Рисунок 2. Схема помехоподавляющего фильтра

Помехоподавляющие фильтры – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки (рисунок 2). В качестве помехоподавляющих в них используют фильтры, которые ослабляют нелинейные сигналы в заданных участках частотного диапазона. Основной задачей данных фильтров является то, чтобы они должны пропускать сигнал без значительного ослабления, лежащего в рабочей полосе частот, и ограничивать сигналы за пределами этой полосы. Для ограничения пропускания информационных сигналов в цепи чаще всего используются фильтры низких частот.

К помехоподавляющим фильтрам предъявляется ряд требований, для их эффективной работе. Данные требования заключаются в следующем:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
- габариты и масса фильтров должны быть минимальными;
- фильтры должны обеспечивать функционирование про определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т. д.);
- конструкции фильтров должны соответствовать требованиям техники безопасности[1].

Для того чтобы ток через фильтр не был насыщен сердечниками катушки фильтра, необходимо проводить такой ток, чтобы сердечники катушки фильтра не были насыщены. При этом следует отметить, что при увеличении тока по катушке увеличивается и реактивное снижение напряжения на катушке. Она может привести к ухудшению эквивалентного коэффициента стабилизации напряжений в цепи с фильтром, а также к возникновению взаимозависимости процессов перехода на различные нагрузки цепи.

Для исключения перехвата побочного электромагнитного излучения по каналу электромагнитного излучения используется *пространственный шум*, а для исключения наводок информационного сигнала с посторонними проводниками и соединительными линиями ВТСС используется *линейный шум*.

Для системы пространственного зашумления предъявляются следующие требования: они должны создавать электрические помехи по диапазону частот возможного побочного электромагнитного излучения ТСПИ; помехи должны иметь горизонтальную и вертикальную поляризацию, поэтому выбор антенны генератора должен быть особенно внимательным и не превышать необходимых норм совместимости электромагнитного излучения на границе контрольной зоны.

Целью пространственного шума считается достижение, если связь опасного сигнала с шумом на границе контрольной зоны не превысит некоторое допустимое значение, рассчитанное по специальным методам для каждого частотного показателя - информационной опасной электромагнитной волны.

В системах пространственного зашумления в основном используются помехи типа

«белого шума» или «синфазные помехи».

Для защиты ПЭВМ в большинстве случаев используют методику «синфазной помехи».

В роли помехового сигнала выступают импульсы амплитуды, которые в свою очередь синхронизируются по форме и времени с импульсами сигнала. Из-за этого по своему составу помеховый сигнал схож со спектром побочных электромагнитных излучений ПЭМВ. Данная система создаёт (генерирует) «имитационную помеху», которая аналогична по своему спектральному скрываемому сигналу.

На сегодняшний день чаще всего применяются пространственные зашумления. Пространственное зашумление использует помехи типа «белый шум». Они значительно превышают уровни побочных электромагнитных излучений. Данные системы используются для защиты обширного класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т. д.

Диапазон рабочих частот генераторов шума — от 0,01—0,1 до 1000 МГц. При мощности излучения около 20 Вт обеспечивается спектральная плотность помехи 40—80 дБ[2].

В системах пространственного зашумления в основном используются слабонаправленные антенны. При использовании данных систем зашумления необходимо понимать, что вместе с помехами нежелательным сигналом создаются помехи и радиоэлектронным сигналам, которые могут представлять важность. Поэтому при работе с системой пространственного зашумления необходимо проводить тесты и исследования по требованиям ЭМС. «Белый шум» также эффективен для электрических каналов утечки информации, так как помеховый сигнал при излучении наводится в соединительных линиях ВТСС и посторонних проводниках, выходящих за пределы контролируемой зоны.

Линейное зашумление включает в себя зашумление заземления, электропитания, соединение линий ВТСС и зашумление проводников не входящих в систему.

Зачастую системы линейного шума используются для маскирования наведенных опасности сигналов постороннего проводника и ВТСС соединительных линий, выходящих из контролируемой зоны. По сути, СЛЗ является генератором шумовых сигналов, создающим шумовые напряжения с заданными характеристиками времени, энергии, спектра.

Проблемы защиты информации сейчас очень важны в современном информационном обществе. Информационная безопасность является одной из главных характеристик информационных систем. Очень важным является комплексное проведение профилактических защитных мероприятий, т.е. гарантирование нейтрализации всех опаснейших каналов передачи информации. Не забывайте, что одним открытым каналом утечки информации могут свести к потере эффективности всей защитной системы.

Список литературы:

1. Векслер Г.С., Недочетов В.С., Пилинский В.В. и др. Подавление электромагнитных помех в цепях электропитания. - К.: Техника. 1990. - 167 с, 31.03.2022
2. Основные положения информационной безопасности (https://studref.com/306260/informatika/osnovnye_polozeniya_informatsionnoy_bezopasnosti), дата обращения: 31.03.2022.
3. Федеральный закон от 27.07.2006 г. № 149-З «Об информации, информационных технологиях и о защите информации» (<https://duma.consultant.ru/page.aspx?878565>), 31.03.2022.

СОДЕРЖАНИЕ

СЕКЦИЯ 1: «КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

УЯЗВИМОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ VPN

Абдулхаликов М.А., Качаева Г.И. 3

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ И БЕЗОПАСНОСТЬ

Амиров К.А., Магомедов Р.М., Саркаров Т.Э. 6

ОПАСНОСТЬ DDOS-АТАК И МЕРЫ ЗАЩИТЫ ПО ИХ ПРОТИВОДЕЙСТВИЮ

Гусева Т.М., Бондаренко Н.А. 10

УЛУЧШЕНИЕ КРИПТОСИСТЕМЫ МАКЭЛИСА НА КОДАХ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК

Иванов Ф.И., Рудзянский А.Д. 13

ПРИМЕНЕНИЕ ПРОТОКОЛА АУТЕНТИФИКАЦИИ ФЕЙГЕ-ФИАТА-ШАМИРА НА УСТРОЙСТВАХ ИНТЕРНЕТА ВЕЩЕЙ

Кацапов М.Е., Назаренко Е.Е. 23

ИССЛЕДОВАНИЕ САМОСИХРОНИЗИРУЮЩИХСЯ ПОТОЧНЫХ ШИФРОВ НА ОСНОВЕ ГЕНЕРАТОРА ФИББОНАЧИ

Медведева А.С., Гиш Т.А. 27

ПРИКЛАДНОЕ ИССЛЕДОВАНИЕ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ В УПРАВЛЕНИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТЬЮ

Пашаева Ф.Р. 31

ИССЛЕДОВАНИЕ АЛГОРИТМА ШИФРОВАНИЯ S-A5

Ржевская Н.В., Гиш Т.А. 34

БЕЗОПАСНОСТЬ В BLUETOOTH, RFID И БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Смотряев М.М., Поплавский Д.А., Большунов Д.В. 38

СЛЕПАЯ SQL ИНЪЕКЦИЯ КАК СРЕДСТВО ТЕСТИРОВАНИЯ БАЗЫ ДАННЫХ НА УЯЗВИМОСТЬ

Фейламазова С.А., Качаева Г.И. 42

ИСТОРИЯ И АНАЛИЗ АТАКИ НА ХЭШ-ФУНКЦИЮ MD-5

Чернов С.Е. 48

СЕКЦИЯ 2: «БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИЙ»

ОБЕСПЕЧЕНИЕ ТЕМПЕРАТУРНЫХ РЕЖИМОВ РАБОТЫ ДИСКРЕТНЫХ ЭЛЕКТРОРАДИОЭЛЕМЕНТОВ, ВХОДЯЩИХ В СОСТАВ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Евдулов О.В., Ибрагимова А.М., Качаева Г.И. 52

СИСТЕМЫ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Калмыкова В.Е., Гусева Л.Л., Самарина К.А., Чугунова О.В. 58

БЕЗОПАСНОСТЬ СЕРВИСА ВИДЕОКОНФЕРЕНЦИЙ ZOOM

Киракосян Г.О. 61

ПОЛНОСТЬЮ ОПТИЧЕСКАЯ КОММУТАЦИЯ ПАКЕТОВ ДЛЯ ГОРОДСКИХ СЕТЕЙ: ВОЗМОЖНОСТИ И ПРОБЛЕМЫ

Кормилец В.П., Давлетова Д.Р. 63

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Меджидов З.У. 67

НЕЙТРАЛИЗАЦИЯ ОПАСНЫХ ИСТОЧНИКОВ СИГНАЛОВ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

Подгорный Э.Р., Стерхова Т.Н. 71

КЛАССИФИКАЦИЯ АНТИВИРУСНЫХ ПРОГРАММ	
Раджабова З.Р., Урдиханов А.Э.....	75
МЕТОДЫ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ТЕЛЕКОММУНИКАЦИЙ	
Сарваров Р.А., Шафиков М.Р.	77
ВОПРОСЫ УПРАВЛЕНИЯ РИСКАМИ УПРАВЛЕНИЯ РЕШЕНИЯМИ ЗАЩИТЫ ИНФОРМАЦИИ	
Селифанов В.В., Солдатов А.Ю., Солдатов Е.Ю., Подлегаев А.И., Скориков В.С.	80
ВЛИЯНИЕ ЦИФРОВИЗАЦИИ ОТРАСЛИ ЭЛЕКТРОЭНЕРГЕТИКИ НА РАЗВИТИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	
Середа Н.В.	87
 СЕКЦИЯ 3: «ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ»	
АНАЛИЗ ДАННЫХ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Азнабаев Ю.С., Яппаров Р.М.	89
РАЗВИТИЕ ТЕХНОЛОГИИ «ДЕЕРФАКЕ» КАК УГРОЗА ИДЕНТИФИКАЦИИ СУБЪЕКТОВ БИОМЕТРИЧЕСКИХ ПДН	
Алискеров М.Р.	91
НОВОВВЕДЕНИЯ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Арбузова М.М.	94
АНАЛИЗ АКТУАЛЬНЫХ УГРОЗ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Васильева Л.С.	97
ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА С ИСПОЛЬЗОВАНИЕМ СЕРВИСА «АЛЬФАДОК»	
Карапац А.Н.	100
МЕТОДЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ	
Гусева Т.М., Николаенко Е.Э., Шаталов А.В.	104
КОМПРОМЕТАЦИЯ ЛИЧНОСТИ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ. СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Житяйкина В.Д., Конева Ю.Л.	108
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РАЗРАБОТКЕ ВИДЕОИГР	
Загиров А.А.	112
ФУНКЦИОНИРОВАНИЕ ОБЛАЧНЫХ ХРАНИЛИЩ ДАННЫХ	
Корниенко Д.В., Мишина С.В.	116
ПЕРСПЕКТИВЫ РАЗРАБОТКИ НЕЙРОЧИПА NEURALINK	
Никифоров Д.В., Альбекова З.М.	121
ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НЕОБХОДИМЫЙ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОГЛАСНО НОРМАТИВНО-ПРАВОВЫМ АКТАМ РОССИЙСКОЙ ФЕДЕРАЦИИ	
Таранец К.А., Прохоров А.И.	125
ЗАЩИТА ДАННЫХ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ: ВЫЗОВЫ И ПОИСК ПУТЕЙ РЕШЕНИЯ	
Темирова А.Б., Бакаев М.М.	129
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ	
Халимбеков М.Х., Магомедов Р.М.	131
CRM-СИСТЕМЫ В РОССИЙСКОМ БИЗНЕСЕ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ	
Элбакян А.А., Альбекова З.М.	136

СЕКЦИЯ 4: «ТЕХНОЛОГИИ ФИЛЬТРАЦИИ ИНТЕРНЕТ-КОНТЕНТА»

ПРОБЛЕМА ИГРОВОЙ ЗАВИСИМОСТИ МОЛОДЕЖИ

Галеев А.Ф., Фарвазов Б.И. 139

ФИЛЬТРАЦИЯ КОНТЕНТА В ОБРАЗОВАТЕЛЬНЫХ УЧЕРЕЖДЕНИЯХ

Галеев А.Ф., Фарвазов Б.И. 140

ФИШИНГОВЫЕ АТАКИ ОДИН КАК ОДИН ИЗ ВИДОВ ХАКЕРСКИХ АТАК

Качаева Г.И., Сапиюлаев Ш.М. 142

СРЕДСТВА КОНТЕНТНОЙ ФИЛЬТРАЦИИ ДЛЯ НЕБОЛЬШОГО ОФИСА

Киздермишов А.А. 145

ТЕОРИЯ ЦВЕТА КАК ОСНОВА РАБОТЫ В ВЕБ-ДИЗАЙНЕ.

РОЛЬ ЦВЕТА В ВЕБ-ДИЗАЙНЕ

Луданова У.Г., Альбекова З.М. 148

ФИЛЬТРАЦИЯ СЕТЕВОГО КОНТЕНТА В СИСТЕМЕ ОБЕСПЕЧЕНИЯ

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Полянина А. 154

ОЦЕНКА УРОВНЯ ЗАВИСИМОСТИ ОТ КОМПЬЮТЕРНЫХ ИГР В МОЛОДЕЖНОЙ

СРЕДЕ НА ТЕРРИТОРИИ РЕСПУБЛИКИ ДАГЕСТАН

Попов П.М. 157

СРЕДСТВА И МЕТОДЫ БЛОКИРОВКИ НЕЖЕЛАТЕЛЬНОЙ

ИНФОРМАЦИИ В СЕТИ

Саадиев О.С. 162

СЕКЦИЯ 5: «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»

СОВРЕМЕННАЯ ХАРАКТЕРИСТИКА ИНФОРМАЦИОННЫХ ВОЙН

Ахмадиева В.Ф., Ахмадиева В.Ф., Яппаров Р.М. 166

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ

ИНФРАСТРУКТУРЫ

Велибеков А.Н., Магомедов Р.М. 168

МЕТОДИКА АВТОМАТИЗИРОВАННОЙ ДИАГНОСТИКИ И МОНИТОРИНГА

МЕДИАТИЗИРОВАННЫХ ЛОКАЛЬНЫХ ИНЦИДЕНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

Виткова Л.А. 172

ЗАДАЧА ОБНАРУЖЕНИЯ АНОМАЛИЙ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ

ИНФРАСТРУКТУРЫ

Виткова Л.А., Таланов Ю.А. 175

СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В

ИНФОРМАЦИОННЫХ СИСТЕМАХ

Гусева Т.М., Зеленский Е.О. 179

АУДИТ ИТ-БЕЗОПАСНОСТИ: ВАЖНОСТЬ, ВИДЫ И МЕТОДОЛОГИЯ

Гусева Т.М., Микитова И.М. 182

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Гусева Т.М., Мова А.А., Васильева Л.С. 186

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В ОРГАНИЗАЦИИ

Раджабова З.Р., Магомедова Л.М. 189

О ВОПРОСАХ ОБНОВЛЕНИЯ БАЗОВОГО КОМПЛЕКТА ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ В ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОВД

Ефимов А.О., Романова В.Р., Вольф В.А. 192

РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ

ИНФОРМАЦИИ

Крыжановский А.В., Писарев М.Н. 196

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕР ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ	
Милько Д.С.	201
О ПРИМЕНЕНИИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В РАССЛЕДОВАНИИ ПРАВОНАРУШЕНИЙ	
Миронова Н.Г., Аюпов А.Я.	205
АНАЛИЗ ВЕКТОРОВ АТАК В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ	
Пучков В.В., Пикос А.В.	208
УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В ОРГАНИЗАЦИИ	
Раджабова З.Р., Магомедова Л.М.	213
ОБ ЭКОСИСТЕМНОМ ПОДХОДЕ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Миронова Н.Г., Чупеева Л.А.	216
АНАЛИЗ И ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	
Романова В.Р., Рогозин Е.А., Ефимов А.О.	219
ОСОБЕННОСТИ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ	
Сахибгареев И.Р., Шагапов И.А.	225
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	
Хаджаев К.Ш., Магомедов Р.М., Саркаров Т.Э.	228
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РАМКАХ ЦИФРОВОЙ ДОВЕРЕННОЙ СРЕДЫ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ	
Яковлева Е.А.	230
ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК, В ПЕРИОД ИМПОРТОЗАМЕЩЕНИЯ	
Хайретдинов А.И., Шагапов И.А.	234
РАСЧЕТ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОТКРЫТЫХ ОПЕРАЦИОННЫХ СИСТЕМ НА ОСНОВЕ АНАЛИЗА ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ПО ГОСТ Р ИСО/МЭК 15408	
Янгиров А.И., Рогозин Е.А.	238
 СЕКЦИЯ 6: «ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И КИБЕРБЕЗОПАСНОСТЬ»	
ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ЭЛЕКТРОЭНЕРГЕТИКЕ	
Аветисян А.С.	244
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РАМКАХ СОВРЕМЕННОГО ОБРАЗОВАНИЯ	
Акинъшин И.Н., Гусева Т.М.	247
МОДЕЛЬ И ПРОГРАММНЫЙ КОМПЛЕКС ЦИФРОВОГО ДВОЙНИКА ТИПОВОЙ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ	
Алексеев А.В.	251
РАЗРАБОТКА АРХИТЕКТУРЫ МОДЕЛИ НЕЙРОННОЙ СЕТИ ПО РАСПОЗНАВАНИЮ РУКОПИСНЫХ СИМВОЛОВ	
Бойко А.С., Соломонов Д.В.	255
ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ЗДРАВООХРАНЕНИЯ	
Валямятова Н.Б.	258
СФЕРЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	
Васильева Л.С., Котлярова Д.В.	260
ИСПОЛЬЗОВАНИЕ ПРАКТИКО-ОРИЕНТИРОВАННОГО ПОДХОДА В ОБУЧЕНИИ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Волков Е.А., Яппаров Р.М.	263
КИБЕРПРЕСТУПНОСТЬ В НАПРАВЛЕНИИ УЧЕБНЫХ ЗАВЕДЕНИЙ	
Воронов Е.Ю.	265

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СИСТЕМ	
Галеев Р.Т., Шагапов И.А.	267
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ТЕОРИЯ ПЕРКОЛЯЦИИ.	
СОВМЕЩЕНИЕ АППАРАТА ДВУХ НАПРАВЛЕНИЙ В НАУКЕ ДЛЯ РЕШЕНИЯ	
ПРОБЛЕМ КАЖДОЙ	
Гамзатов И.М.	272
ТЕНДЕНЦИИ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННОМ	
ОБЩЕСТВЕ	
Гусева Т.М., Белюченко Н.Е.	275
АНАЛИЗ АНТИШПИОНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	
Гусева Т.М., Гулиев Д.З., Васильева Л.С.	279
РЕВОЛЮЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	
Гусева Т.М., Гурьянов А.С.	283
РАЗВИТИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	
Гусева Т.М., Желтов А.В.	286
СОВРЕМЕННЫЕ СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	
Гусева Т.М., Коваленко К.М.	290
ПЕРСПЕКТИВЫ И ТЕНДЕНЦИИ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	
Гусева Т.М., Ломакин Н.А.	293
УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ	
СИСТЕМАХ	
Гусева Т.М., Михайлюк Д.В.	296
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И СОВРЕМЕННОЕ ОБРАЗОВАНИЕ	
Гусева Т.М., Орловская Е.Д.	300
МЕТОДЫ ЗАЩИТЫ JAVA ПРИЛОЖЕНИЙ	
Гусева Т.М., Пуйко Д.Д.	302
ТЕХНОЛОГИЯ РУЧНОГО ТЕСТИРОВАНИЯ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ	
КАЧЕСТВА ПРОГРАММНОГО ПРОДУКТА	
Дмитриева Д.Д., Яппаров Р.М.	307
АНАЛИЗ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ	
В СЕТЯХ 5G С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ	
Карпенко Н.Э., Гомбоев С.М., Плешакова Е.С.	310
СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
В МАЛОМ БИЗНЕСЕ	
Куршиев И.Д., Магомедов Р.М., Саркаров Т.Э.	315
ИСПОЛЬЗОВАНИЯ VI-СИСТЕМ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ	
ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ	
Лукьянов Д.В.	318
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В БАНКОВСКОЙ СФЕРЕ:	
ЧТО ЭТО ОЗНАЧАЕТ НА ПРАКТИКЕ	
Мартыновский К.И., Рерих А.В.	321
BIG DATA В ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ПРОМЫШЛЕННОГО	
ПРЕДПРИЯТИЯ	
Мекибаева Д.К.	324
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Раджабова З.Р., Касумова А.А.	327
КИБЕРБЕЗОПАСНОСТЬ: ПОНЯТИЕ, ВИДЫ КИБЕРАТАК И СПОСОБЫ	
БОРЬБЫ С НИМИ	
Раджабова З.Р., Яхьяев Р.Р.	330
ОБНАРУЖЕНИЕ ЛАВИННЫХ DOS АТАК В СЕТЯХ 5G С ПРИМЕНЕНИЕМ	
МАШИННОГО ОБУЧЕНИЯ	
Плешакова Е.С., Малахов Д.П.	334

ПРОГРАММНО-АППАРАТНЫЙ МЕТОД ОПТИМИЗАЦИИ ДИЗАССЕМБЛИРОВАНИЯ ИСПОЛНЯЕМОГО КОДА	
Поплавский Д.А., Калинкина А.А., Туринцев К.А.	339
ОРГАНИЗАЦИЯ КИБЕР-ПОЛИГОНА В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ УЧЕБНОГО ЗАВЕДЕНИЯ	
Рыженко А.А.	344
СОВРЕМЕННЫЕ ПРОЕКТОРЫ, ИХ ПРЕИМУЩЕСТВА И НЕДОСТАТКИ	
Рядская М.А., Альбекова З.М.	347
ИСПОЛЬЗОВАНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX КАК ПЕРСПЕКТИВНОЕ РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Сальникова А.А., Яппаров Р.М.	352
ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ	
Серета Н.В.	355
МОДЕЛЬ СБОРА И КАТЕГОРИЗАЦИИ УЛИКОВОЙ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ КИБЕРБЕЗОПАСНОСТИ	
Симонов О.И., Мальцев А.В., Огур М.Г.	358
МЕТОДЫ КИБЕРГИГИЕНЫ ДЛЯ ОРГАНИЗАЦИИ БЕЗОПАСНОГО ДИСТАНЦИОННОГО ОБУЧЕНИЯ	
Темирова А.Б., Рожапов С.М.	362
КОНСТИТУЦИОННО-ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Угольников И.А.	365
ТЕХНОЛОГИИ OCR В DLP-СИСТЕМАХ РАСПОЗНАВАНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ	
Хабрахманова Л.А., Яппаров Р.М.	368
СФЕРЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ BIG DATA	
Шалаева А.И.	370
БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ НА МЕЖДУНАРОДНОМ УРОВНЕ СРЕДСТВАМИ ПРАВОВОГО РЕГУЛИРОВАНИЯ	
Шихметова З.М., Качаева Г.И.	373
ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ДВУНАПРАВЛЕННОГО ОБМЕНА ИНФОРМАЦИЕЙ ПО ОТКРЫТЫМ КАНАЛАМ	
Якунин А.Г., Кайст Д.В.	377