МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский технический университет связи и информатики»
(МТУСИ)

Федеральное учебно-методическое объединение в сфере высшего
образования по УГСНП 10.00.00 «Информационная безопасность»
(ФУМО ВО ИБ)

II ВСЕРОССИЙСКАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ **ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

2 ноября 2022 г.

II Всероссийская научно-практическая конференция
«Теория и практика обеспечения информационной безопасности»

* * *

ДАТА И МЕСТО ПРОВЕДЕНИЯ

2 ноября 2022 г.
МТУСИ, Конгресс-центр
г. Москва, ул. Авиамоторная, д. 8, стр. 39
09:00 – 18:00

* * *

ПРОГРАММА МЕРОПРИЯТИЙ

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 39 (конгресс-центр)

РЕГИСТРАЦИЯ УЧАСТНИКОВ
ПРИВЕТСВЕННЫЙ КОФЕ-БРЕЙК
09:00 – 10:00

ТОРЖЕСТВЕННОЕ ОТКРЫТИЕ
10:00 – 10:10

ПРИВЕТСТВЕННЫЕ ОБРАЩЕНИЯ:

Леохин Юрий Львович, доктор технических наук, профессор, проректор по научной работе Московского технического университета связи и информатики;

Белов Евгений Борисович, Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность», заместитель председателя

ПЛЕНАРНАЯ НАУЧНАЯ СЕССИЯ
10:10 – 11:40

ВЫСТУПЛЕНИЯ:

10:10 – 10:40
Крылов Григорий Олегович, профессор кафедры «Безопасность телекоммуникаций» МТУСИ, профессор Финансового университета при Правительстве РФ, доктор физико-математических наук, профессор
ТРЕБОВАНИЯ К НАУЧНОМУ ТЕКСТУ КВАЛИФИКАЦИОННЫХ РАБОТ

10:40 – 11:10
Кравец Василий Васильевич, начальник ОИИТ АО «ПМ»
Иванов Олег Александрович, руководитель направления АО «ПМ»
Морин Алексей Александрович, специалист АО «ПМ»
ТЕХНИКИ ЗАКРЕПЛЕНИЯ В ОС WINDOWS

11:10 – 11:40
Буряков Виктор Михайлович, старший технолог ПАО «Мегафон»
ID-FRAUD УЯЗВИМОСТИ СОТОВЫХ СЕТЕЙ ЧЕРЕЗ VoIP

ДИСКУССИЯ ПО ПЛЕНАРНЫМ НАУЧНЫМ ДОКЛАДАМ
11:40 - 12:00

ПЕРЕРЫВ
12:00 - 13:00

НАУЧНАЯ СЕКЦИЯ

«КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И АНАЛИЗ СЕТЕВОГО ТРАФИКА»

Руководители: **Панков Константин Николаевич**,
Московский технический университет связи и информатики, врио заведующего кафедрой «Теория вероятностей и прикладная математика», кандидат физико-математических наук

НАУЧНЫЕ ДОКЛАДЫ:

1. **Кокшев Павел Андреевич,** ЧГУ им. Ульянова, аспирант
   Галанина Наталия Андреевна, ЧГУ им. Ульянова, профессор, доктор технических наук, доцент

СЕТЕВОЙ АНАЛИЗАТОР ДАННЫХ И ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ЭНЕРГЕТИКЕ

Данный доклад освещает необходимость применения сетевых анализаторов данных в энергетике, в частности в высокоавтоматизированных (цифровых) подстанциях. Рассмотрены основные протоколы передачи данных, а также преимущества применения сетевого анализатора данных и защиты информации в автоматизированной системе управления технологическими процессами.

2. **Караулова Ольга Александровна,** Поволжский государственный университет телекоммуникаций и информатики
   Шакурский Максим Викторович, Самарский государственный технический университет, Поволжский государственный университет телекоммуникаций и информатики, к.т.н., доцент

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИИ В ЗВУКЕ

Сокрытие данных в аудиосигналах на сегодняшний день является актуальным в связи с широким распространением программ видеосвязи. В статье рассматривается формат без сжатия (WAVE). Для эффективного встраивания скрытой информации применяется метод замены младших значащих бит (LSB-метод). Реализация LSB – метода для формата WAVE в среде Python.

3. **Павленко Евгений Юрьевич,** Санкт-Петербургский политехнический университет Петра Великого, к.т.н.

МЕХАНИЗМЫ ИСКУССТВЕННОЙ ИММУНИЗАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ

Предложен подход, реализующий иммунизацию критических узлов современных многосвязных цифровых систем для защиты таких систем от различных кибератак. Представлена серия экспериментов, демонстрирующая важность защиты в первую очередь критических узлов системы, а также экспериментально подтверждена состоятельность подхода при реализации атак типа отказ в обслуживании, разрыв связи между компонентами и атаки типа "человек посередине".

4. **Зефиров Сергей Львович,** Пензенский государственный университет», заведующий кафедрой, к.т.н., доцент
Аккуратнов Александр Николаевич, Пензенский государственный университет, аспирант

МЕТОД АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В докладе предлагается метод анализа событий информационной безопасности, основанный на применении возможностей сигнатурного анализа и цифрового профиля событий. Анализ событий информационной безопасности осуществляется с помощью автоматизированного построения модели правил, выявленных в журналах событий информационной безопасности. Предлагаемый метод анализа событий информационной безопасности используется для получения знаний об изучаемой системе и выявления инцидентов информационной безопасности.

5. **Самарин Николай Николаевич,** ФГУП "НИИ "Квант", начальник НИО-6, к.т.н.
Сирота А.А., СПбПУ, студент

ПРИМЕНЕНИЕ ОБРАТНОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК В ИСПОЛНЯЕМОМ БИНАРНОМ КОДЕ

В настоящее время программное обеспечение (ПО) разрабатывается путем сложной комбинации множества различных технологий, а его функционирование выполняется в разнородной среде, включающей большое число устройств разного типа. Объем отдельных программных модулей в составе информационной системы крайне велик даже с учетом высокоуровневых языков программирования – свыше миллионов строк кода, следовательно, бинарные коды таких файлов занимают еще больше пространства.
В рамках практической апробации предложенной модели был реализован вариант зеркального объединения, состоящий в сокращении промежуточного множества ограничений путем его объединения с результатами работы метода ОСВ на отдельно взятых участках кода. Оценка эффективности предложенной модели проводилась на реализованном экспериментальном макете с использованием набора исходных данных Software Assurance Reference Dataset [10] от NIST (National Institute of Standards and Technology). В качестве результатов тестирования оценивалось время работы классического алгоритма символьного выполнения и алгоритма оптимизированного с помощью метода обратного символьного выполнения по логике зеркального объединения на определенных ветвях.
По результатам тестирования, время работы алгоритма с предложенным методом оптимизации при обнаружении программных ошибок и уязвимостей, порожденных вычислительными ошибками или отсутствием инициализации переменных, в среднем сократилось на 2.1%, что говорит о практической применимости разработанной модели.

НАУЧНАЯ СЕКЦИЯ

«ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

Руководитель: **Кубанков Александр Николаевич**,
Московского технического университета связи и информатики, доктор военных наук, профессор, заведующий кафедрой «Безопасность телекоммуникаций»

Секретарь: **Булгакова Елена Валерьевна**,
Московский технический университет связи и информатики, кандидат юридических наук, доцент

НАУЧНЫЕ ДОКЛАДЫ:

1. **Селиверстов Виталий Валерьевич,** Саратовский государственный технический университет имени Гагарина Ю.А., аспирант
   Корчагин Сергей Алексеевич, Саратовский государственный технический университет имени Гагарина Ю.А., к.ф.-м.н., доцент. Финансовый университет при Правительстве Российской Федерации, доцент

ТРЕБОВАНИЯ К ЗАЩИТЕ ПРИЛОЖЕНИЙ, ОСНОВАННЫХ НА ТЕХНОЛОГИИ КОНТЕЙНЕРИЗАЦИИ

В статье рассмотрены практические подходы и механизмы, необходимые при построении защиты систем на основе контейнеризации. Актуальность обусловлена выявлением различных способов вредоносного использования уязвимых мест в облачных и виртуальных инфраструктурах. Проведен сравнительный анализ некоторых существующих технологий для обеспечения информационной безопасности запускаемых контейнеров. Вопросы безопасности рассмотрены на уровнях операционной системы, образов контейнеров, оркестраторов и программных продуктов для контейнеризации. Даны практические примеры и эксплуатируемые решения, которые необходимы для построения информационной системы с повышенными требованиями к безопасности и надежности.

2. **Ефимова Ксения Алексеевна,** Удмуртский государственный университет, студент
   Колчерина Жанна Николаевна, Удмуртский государственный университет, Институт права, социального управления и безопасности, старший преподаватель

ПРИМЕНЕНИЕ МОДЕЛЕЙ ЗРЕЛОСТИ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предлагается метод оценивания эффективности процессов информационной безопасности, основанный на оценке зрелости критичных процессов через измерения определенных атрибутов оценки в форме анкет с привлечением экспертов и метрик информационной безопасности. Данная методика оценки позволяет понять состояние процессов информационной безопасности и может характеризовать уровень зрелости процесса. На основании полученных результатов оценки зрелости, далее можно выработать необходимые мероприятия для повышения зрелости и эффективности процессов.

3. **Гель Ангелина Владимировна,** МосУ МВД России имени В.Я. Кикотя

ИССЛЕДОВАНИЕ СЛЕДОВ, ОБРАЗУЮЩИХСЯ В БРАУЗЕРАХ ПРИ ИСПОЛЬЗОВАНИИ СОЦИАЛЬНЫХ СЕТЕЙ В РАМКАХ КОМПЬЮТЕРНЫХ ЭКСПЕРТИЗ

Главной особенностью современного состояния исследований, проводимых экспертами по компьютерным инструментам, является не только отсутствие мониторинга и методической поддержки самого теста, но и отсутствие детальной проработки задействованных процедур. Доступные в настоящее время материалы носят общий характер и в основном используются для изучения работы поисковых и следственных органов по получению информации в виде электронных документов, графики, видео и аудио информации. Однако текущая практика показывает, что существует острая необходимость в разработке систематических руководств по уголовным расследованиям с использованием компьютеризированных инструментов для улучшения сбора, поиска и использования доказательств. В этом отношении использование технических знаний значительно повысило роль расследования таких преступлений. Одним из основных аргументов в пользу этой деятельности является изучение программных продуктов, цель которого - выявление фактов и обстоятельств, связанных с незаконным использованием и разработкой компьютеров.

4. **Рудаков Иван Алексеевич,** Московский технический университет связи и информатики, студент
   Булгакова Елена Валерьевна, Московский технический университет связи и информатики доцент

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ: ЗАЩИТА ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ И ЦИФРОВОЙ РЕПУТАЦИИ

Данный доклад посвящен тенденции развития цифрового общества. Рассматриваются риски информационной безопасности личности, введение цифровой репутации в общество и её влияние на человека. Прогнозирование будущих вызовов нашей цифровой репутации, а также рассматриваются некоторые способы защиты своей цифровой репутации.

5. **Подъемов Александр Максимович,** ЮРГПУ(НПИ) им. М.И. Платова, студент

СОВЕРШЕНСТВОВАНИЕ СПОСОБОВ ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОНЛАЙН АТАК НА КОМПЬЮТЕРНУЮ СЕТЬ

В докладе , я рассказываю о выгодной (в экономическом плане) для компании, схеме построения защищенной сети, которая основана на Sandbox(песочница).Параллельно расскажу как еще можно выгодно укомплектовать сеть компании, для меньших затрат. На мой взгляд эта идея даже очень актуальна, в наше непростое время, ведь каждый день злоумышленников становиться больше.

6. **Зорин Александр Евгеньевич,** ЮРГПУ(НПИ) им. М.И. Платова, студент

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Целью работы является понятие определения телекоммуникационной сети. Рассмотрение видов и классификаций телекоммуникационных систем связи, типы сетей, линий и каналов связи.

В ходе работы рассматривается защита информации в телекоммуникационных сетях и задачи направленные на защиту информации в телекоммуникационных сетях.

В соответствии с определёнными требованиями предложены необходимые организационные, инженерно-технические и программно-аппаратные методы и средства защиты информации.

Итогом работы являются средства и методы защиты информации в телекоммуникационных сетях.

7. **Санников Кирилл Викторович,** ЮРГПУ(НПИ) им. М.И. Платова, студент

РАЗРАБОТКА КСЗИ НА ПРЕДПРИЯТИИ

Цель работы заключается в изучении разработки комплексной системы защиты информации учреждения, направленной на предотвращение угроз утраты, хищения, уничтожения, искажения и подмены защищаемой информации за счет несанкционированного доступа и других воздействий.

В ходе работы показано, как проводить анализ объекта защиты, определять и категорировать информацию, циркулирующая на объекте; выявлять источники и носители информации, актуальные угрозы информации. В соответствии нормативными и руководящими документами, а также исходя из анализа актуальных угроз, сформулировать требования к комплексной системе защиты.

В соответствии с определёнными требованиями предложены необходимые организационные, инженерно-технические и программно-аппаратные методы и средства защиты информации.

Итогом работы является комплексная система защиты информации на предприятии, включающая как установку различных средств защиты, так и проведение организационных мероприятий.

8. **Максимович Катарина Еленковна,** Московский технический университет связи и информатики, студент
Булгакова Елена Валерьевна, Московский технический университет связи и информатики, доцент

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ПРИМЕРЕ БАНКА

Учитывая происходящие изменения в экономике РФ, многие вендоры решений ИБ ушли с рынка РФ, крайне остро стоит замена импортных решений попавших под санкции и минимизация рисков информационной безопасности для критический информационной инфраструктуры (Далее по тексту КИИ) в организациях банковской сферы возникших по причине отзыва лицензий (Cisco, Fortinet и др.). Так как в банковской сфере преобладают решения Cisco и Fortinet, быстрая замена повлечет высокую нагрузку как на производителей импортозамещающей техники так и на сам рынок в целом. Бюджеты ИБ с учетом текущих курсов доллара и евро на защиту данных будут расти, вероятно они будут выше чем текущие расходы на ИТ составляющую, по причине того, что безопасность данных является критическим фактором успеха любого бизнеса, в частности организаций банковского сектора.

В банковской сфере вопрос информационной безопасности набирает все больший приоритет, информационная инфраструктура из-за отзыва лицензий решений ИЮ фактически остается без активной защиты, устройства откатывают сигнатурные базы до заводских настроек или вовсе блокируется функционал. Банки должны с учетом роста ddos атак (атаки направленные на отказ оборудования) на ресурсы РФ, обязаны максимально обеспечить безопасность платежных процессов, сохранить доступность и работоспособность сервисов.

9. **Минакова Наталья Николаевна,** Алтайский государственный университет, профессор д.ф.м.н., профессор
Мансуров Александр Валерьевич, Алтайский государственный университет, доцент к.т.н, доцент

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА С ИСПОЛЬЗОВАНИЕМ МЕТОДА ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ

Оценивается возможность идентификации личности с помощью метода локальных бинарных шаблонов, применение которого реализуется на базе свободно распространяемых библиотек. Среди методов локальных бинарных шаблонов выбран метод перечений. Применен базовый оператор для восьми пикселей окрестности. Выполненные расчёты

позволили сделать вывод о том, что корректное сравнение изображений радужной оболочки глаза можно выполнить путем применения метода пересечений к текстуре изображения.

10. **Тивелев Никита Александрович,** Московский технический университет связи и информатики, студент
Булгакова Елена Валерьевна, Московский технический университет связи и информатики, доцент

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕШЕНИЯХ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ И ОБЕСПЕЧЕНИЮ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В докладе будет рассмотрено применение искусственного интеллекта (ИИ) для обеспечения информационной безопасности предприятия. Будут раскрыты основные понятия ИИ, описаны методы ИИ, применяемые для защиты информации. А также будет изучена необходимость его использования в современных средствах защиты.

11. **Зверьков Никита Владимирович,** Московский технический университет связи и информатики, студент
Булгакова Елена Валерьевна, Московский технический университет связи и информатики, доцент

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ-ОБЩЕСТВА

Актуальность обусловлена процессами изменения современного общества, которое развивается в соответствии с современными технологиями. Целями является: рассмотреть само определение "смарт-общество"; попытаться выяснить какие угрозы информационной безопасности имеет "смарт общество"; проанализировать какую опасность несут те или иные угрозы информационной безопасности для смарт общества.

12. **Гришина Наталия Васильевна,** Российский государственный гуманитарный университет, доцент, Московский государственный лингвистический университет, доцент, к.т.н., доцент

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЗАЩИЩЕНЫ ИЛИ НЕТ?

В статье показана важность обеспечения целостности, доступности и конфиденциальности информационных ресурсов для реализации национальных проектов России в области цифровой экономики.

Рассматривается проблема утечки персональных данных. Показана динамика по ряду аспектов, касающаяся утечки данных вообще и персональных данных в частности.

13. **Сиротский Алексей Александрович,** ФГБОУ ВО НИУ МГСУ, доцент, к.т.н., доцент

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ИЗМЕНЕНИЯ В ПРОЦЕССАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СВЯЗИ С ИЗМЕНЕНИЯМИ ЗАКОНОДАТЕЛЬСТВА, ВСТУПАЮЩИМИ В СИЛУ С 1 СЕНТЯБРЯ 2022 ГОДА

В докладе рассматриваются и анализируются некоторые наиболее принципиальные изменения законодательных требований к обработке персональных данных, вступающих в силу с 1 сентября 2022 года, и которые влекут за собой существенные изменения процессов обработки персональных данных в организациях, потребуют произвести корректировку и расширение применяемых операторами мер и средств обеспечения защищённости персональных данных.

НАУЧНАЯ СЕКЦИЯ

«ПРОБЛЕМЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

Руководители: **Крылов Григорий Олегович**,
доктор физико-математических наук, профессор кафедры «Безопасность телекоммуникаций» Московского технического университета связи и информатики, профессор Финуниверситета, профессор Национального исследовательского ядерного университета «МИФИ́»

Секретарь: **Закомолдин Семён Дмитриевич,**
Московский технический университет связи и информатики, студент кафедры «Безопасность телекоммуникаций»

НАУЧНЫЕ ДОКЛАДЫ:

1. **Лисютин Павел Александрович,** АО «НИИ «Кулон», инженер-конструктор; МТУСИ, аспирант

ПОМЕХОЗАЩИЩЕННОСТЬ И УЯЗВИМОСТЬ ПРОВОДА ВИТОЙ ПАРЫ КАК СРЕДЫ РАСПРОСТРАНЕНИЯ СИГНАЛА НА ФИЗИЧЕСКОМ УРОВНЕ МОДЕЛИ OSI

В статье структурирована теоретическая информация из различных источников по физическому уровню сетевой модели OSI.

На опытном рабочем экспериментальном кабеле предпринята попытка измерения осциллографом электрических параметров сигнала пакета данных протокола TCP/IP.

Выдвинута гипотеза о применении магнитных свойств среды для передачи информации в линиях связи.

2. **Глозштейн Даниил Александрович**, Поволжский государственный технологический университет, старший преподаватель
Сидоркина Ирина Геннадьевна, Поволжский государственный технологический университет, заведующая кафедрой информационной безопасности факультета информатики и вычислительной техники, доктор технических наук, профессор

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО КАНАЛА СВЯЗИ

В статье предложена экспериментальная схема применения квантового ключа в традиционной системе видеоконференцсвязи. В соответствии с этой схемой, в традиционную систему видеоконференцсвязи был встроен квантовый шлюз. Благодаря этому данные, передаваемые через систему видеоконференцсвязи, могут быть зашифрованы квантовым ключом, генерируемым таким шлюзом. Небольшая скорость генерации квантового ключа компенсируется применением алгоритма его расширения, что позволяет сохранять нормальное качество видеоизображений.

3. **Шукенбаев А.Б.,** РТУ МИРЭА, к.т.н., доцент
Мирзоева Л.В., банк ВТБ, специалист

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ТЕСТИРОВАНИЯ БЕЗ-ОПАСНОСТИ ПРОЕКТОВ

В настоящее время в деятельности человека используется огромное количество информационных технологий, что приводит к росту случаев несанкционированного доступа

к конфиденциальной информации. Снизить число таких случаев можно как с помощью совершенствования систем ин-формационной безопасности, так и с помощью проведения процесса про-верки текущего состояния защищенности информационных систем, то есть их тестирования.

Тестирование безопасности проектов является необходимым первым шагом для организаций любых размеров, целью которых является определение уровня информационной безопасности и ее повышения для укрепления защиты с течением времени.

В связи с этим становится актуальным проведение анализа известных методик и стандартов тестирования безопасности проектов.

4. Кадацкова Влада Валерьевна, ЮРГПУ (НПИ) им. М.И.Платова, студент

ПОДГОТОВКА СОТРУДНИКОВ ДЛЯ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

В статье рассказано о подготовке сотрудников для мониторинга событий информационной безопасности. Бывают различные вирусы, которые находят уязвимости в операционной системе. Для обучения сотрудников необходимо создать реальные условия. В статье указана статистика наиболее распространенных угроз, выявлено программное обеспечение, в котором могут быть уязвимости для наиболее актуальных угроз. Для подготовки сотрудников необходимо составить наиболее реальные условия (которые можно выполнить на киберполигоне) для защиты сети предприятия.

5. Дебеева Екатерина Евгеньевна, ЮРГПУ (НПИ) им. М. И. Платова, студент
Алексеев Виктор Павлович, ЮРГПУ (НПИ) им. М. И. Платова, старший преподаватель

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЙ НА УЯЗВИМОСТИ

Современный этап развития информационного общества характеризуется массовым использованием интернет ресурсов, и предоставлением широкого спектра онлайн-услуг. Всё больше пользователей обращаются к сайтам, web-приложениям для обмена и хранения информации, которая требует защиты от всевозможных злоумышленников. Поэтому на сегодняшний день анализ защищенности web-приложений от уязвимостей является одной из актуальных задач в области информационной безопасности.Разработанный нами программный комплекс может быть использован в качестве как самостоятельного программного обеспечения на этапе сбора информации, так и в качестве средства решения специфичных задач при использовании дополнительных скриптов, созданных пользователями.

6. Дорохов Станислав Васильевич, РТУ-МИРЭА, доцент, к.т.н., с.н.с.
Михайлов Вячеслав Эдуардович, РТУ-МИРЭА, ассистент

ПРОБЛЕМА НЕКОРРЕКТНОЙ ВАЛИДАЦИИ СЕРТИФИКАТОВ (IMPROPER CERTIFICATE VALIDATION) ПРИ УСТАНОВЛЕНИИ ДОВЕРЕННЫХ СОЕДИНЕНИЙ

В статье представлено описание природы возникновения уязвимости, связанной с некорректной валидацией сертификатов (Improper Certificate Validation) при установлении доверенных соединений, рассмотрены примеры исходных кодов программ с некорректной валидацией сертификатов, а также приведены рекомендации по устранению данного типа уязвимости для разработчиков программного обеспечения.

7. **Хромова Анна Владимировна,** Акционерное общество "Перспективный мониторинг", системный аналитик; Российская академия народного хозяйства государственной службы при Президенте РФ, аспирант

ТЕНДЕНЦИИ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ РОССИИ: СОЗДАНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА

Цифровизация активно входит в повседневную жизнь, определяя тренды современного научно-технологического развития. Скорость развития и распространения ИКТ ежегодно увеличивается. Сегодня «технологическая сфера стала ареной противоборства ведущих держав и оказывает существенное влияние на расстановку сил в мире. Способность государства обеспечивать цифровой суверенитет будет символизировать независимость в 21 веке. Анализ тенденций в высокотехнологичном секторе экономики России показывает, что, несмотря на некоторый рост по многим показателям научно-технологического развития, Российская Федерация продолжает оставаться в тени ведущих мировых стран.

8. **Зорин Александр Евгеньевич,** ЮРГПУ(НПИ) им. М.И. Платова, студент

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Целью работы является понятие определения телекоммуникационной сети. Рассмотрение видов и классификаций телекоммуникационных систем связи, типы сетей, линий и каналов связи.

В ходе работы рассматривается защита информации в телекоммуникационных сетях и задачи направленные на защиту информации в телекоммуникационных сетях.

В соответствии с определёнными требованиями предложены необходимые организационные, инженерно-технические и программно-аппаратные методы и средства защиты информации.

Итогом работы являются средства и методы защиты информации в телекоммуникационных сетях.

9. **Межутков Дмитрий Викторович,** ЮРГПУ(НПИ) имени М.И. Платова, студент

ЗАЩИЩЁННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Статья посвящена разработке систем электронного документооборота на предприятии, а также внедрению более совершенных систем коммуникации с применением интернет ресурсов. Внедрение системы электронного документооборота позволяет организации работать быстрее и с наименьшей вероятностью потери документов. Ранее при почтовой пересылке письма могли пропадать или задерживаться, в результате чего компании испытывали массу неудобств. Электронный документооборот решает эти проблемы. Немаловажными факторами в этом должны служить правильно разработанные системы защиты. Следовательно, надежная защита документооборота является актуальной задачей на данный момент.

10. **Потапова Ксения Андреевна,** Морской государственный университет им. адм. Г.И. Невельского, аспирант

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ С МОРСКОГО СУДНА НА БЕРЕГ В УСЛОВИЯХ ОГРАНИЧЕННОГО КАНАЛА СВЯЗИ

В данной статье рассмотрены вопросы, связанные с проблемами передачи информации с морского судна на берег в условиях ограниченного канала связи. Определено понятие сигнала связи и их виды. Изучены такие проблемы как затухание сигнала, шум, теневые зоны, многолучевое распространение сигналов, замирание сигнала, его ограниченность. Разработан алгоритм повышения эффективности передачи информации с морского судна на берег в условиях ограниченного сигнала связи.

11. Денис Владимирович Лузганов, Московский университет МВД Российской Федерации имени В.Я. Кикотя, слушатель

АНАЛИЗ ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ В ЦЕЛЯХ ИДЕНТИФИКАЦИИ ЛИЦ

Создание и внедрение цифровых досье граждан имеет криминалистическое значение для идентификации и обмена данными между государственными органами, организациями, гражданами, а также доступа к актуальной и своевременной информации, однако необходимо убедиться, что персональные данные, содержащиеся в цифровых досье, имеют адекватный уровень защиты и механизмы, обеспечивающие безопасность государства и частных лиц от возможной утечки данных.

12. Мурашко Ю. В.

МЕТОДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ОТПЕЧАТКОВ

Развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше, что обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации. Под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

НАУЧНАЯ СЕКЦИЯ

«КИБЕРБЕЗОПАСНОСТЬ»

Руководитель: **Симонян Айрапет Генрикович**,
Московский технический университет связи и информатики,
доцент кафедры «Информационная безопасность»,
кандидат технических наук, доцент

НАУЧНЫЕ ДОКЛАДЫ:

1. **Козьминых Сергей Игоревич,** Финансовый университет при Правительстве РФ, профессор Департамента Информационной безопасности, доктор технических наук, доцент

ПРОБЛЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Фомы и методы телефонного мошенничества в России. Социальная инженерия, как метод, который используют мошенники, чтобы заставить сообщить данные, необходимые для хищения. Примеры телефонного мошенничества. Методы и рекомендации по противодействию телефонному мошенничеству. Чего ожидать в будущем.

2. **Соколов Александр Сергеевич,** РТУ МИРЭА, студент
Шутов Василий Александрович, РТУ МИРЭА, преподаватель, ассистент

ШИФРАТОРЫ, ДЕШИФРАТОРЫ И ИХ ЗНАЧЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью данной статьи является анализ одной из важнейших областей в информационной безопасности – шифрование данных. Так на примере простейшей программы на языке программирования python был изучен процесс шифрования данных, и, соответственно, его дешифрования. Таким образом, при детальном рассмотрении понятия шифр был сделан вывод о том, насколько безопасным и открытым он является, а также составить модель закрытой системы для передачи информации на основе шифрования данных.

3. **Красов Андрей Владимирович,** Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, заведующий кафедрой ЗСС кандидат технических наук, доцент

СРАВНЕНИЕ ВОЗМОЖНОСТЕЙ НЕЙРОННОЙ СЕТИ И СИСТЕМЫ ПРЕДТВРАЩЕНИЯ ВТОРЖЕНИЙ ПРИ ОБНАРУЖЕНИИ СЕТЕВОЙ СТЕГАНОГРАФИИ В ПРОТОКОЛЕ TCP

Развитие вычислительной техники и методов алгоритмизации привело к появлению модели, имитирующей структуру человеческого мозга – нейронную сеть. Дальнейшее развитие данной модели привело к её применению во многих сферах человеческой деятельности. Одна из таких сфер – информационная безопасность. В данной статье сравниваются возможности нейронной сети и системы предотвращения вторжений в обнаружении вложений в пакеты протокола TCP.

4. **Красов Андрей Владимирович,** Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, заведующий кафедрой ЗСС, кандидат технических наук, доцент
Паскидов Никита Владимирович, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент

Салита Андрей Сергеевич, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент

ИСПОЛЬЗОВАНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ В СЕТЯХ NGN

С развитием информационных технологий возрастает потребность в новых услугах связи и улучшении качества существующих сервисов, в связи с чем требуется развитие и модернизация транспортной системы. Одна из ветвей такого развития – сети NGN. Данные сети позволяют объединить существующие сети старого поколения с сетями, построенными на базе стека протоколов TCP/IP. Однако как и все существующие технологии в сетях NGN остро стоит вопрос безопасности. Данная работа посвящена теме возможности использования сетевой стеганографии в сетях NGN.

5. Горнич Владимир Валерьевич, ЮРГПУ (НПИ) имени М.И. Платова, студент

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ WEB-САЙТОВ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Влияние самых распространенных видов атак и уязвимостей на web-сайты и их защита от злоумышленников. Угрозы от их внедрения и рекомендации по защите информации с вышеперечисленными проблемами.

6. Лысенко Наталья Викторовна, ЮРГПУ (НПИ) им. М.И.Платова, доцент, к.п.н.

ОСОБЕННОСТИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭНЕРГОПРЕДПРИЯТИЙ

Настоящая статья посвящена исследованию вопросов информационной безопасности энергопредприятий страны. Рассмотрены особенности управления рисками информационной безопасности на предприятиях энергетического комплекса. Приведены методы обнаружения вторжений и аномалий киберсистем.

7. Кадацкова Влада Валерьевна, ЮРГПУ (НПИ) им. М.И.Платова, студент

ПОДГОТОВКА СОТРУДНИКОВ ДЛЯ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

Киберполигон — многофункциональный программно-аппаратный комплекс, повторяющий типовые инфраструктуры предприятий различных отраслей. Позволяет отработать практические навыки специалистов без рисков, что что-то пойдет не по плану, и киберучения нанесут ущерб деятельности реального предприятия.

Подготовка сотрудников для мониторинга событий информационной безопасности должна происходить на реальных угрозах, которые существуют в базе данных ФСТЭК (БДУ - Угрозы (fstec.ru)).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

По результатам определения угроз безопасности информации необходимо найти наиболее популярные уязвимости для подготовки специалистов на платформе киберполигона.

8. Гнидин Дмитрий Александрович, ЮРГПУ (НПИ) им. М.И.Платова, студент

РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОПЫТОК КИБЕРАТАК НА СЕРВЕРЫ БАЗ ДАННЫХ

В статье рассмотрена разработка методов защиты информации от попыток кибератак на серверы баз данных.

Целью исследования является вопрос повышения уровня защиты баз данных.

Задачами исследования является: анализ существующих способов кибератак и защиту от них, методов защиты баз данных, анализ эффективности методов защиты баз данных.

Актуальность данной научной работы заключается в изучении и анализе кибератак, разработке методов защиты, повышение безопасности баз данных, защиты информации хранящейся в базах данных.

9. **Лошкарев Алексей Валерьевич,** Морской государственный университет имени адмирала Г.И.Невельского, аспирант
Балацкий Илья Александрович, МОБУ СОШ № 3 Арсеньевского ГО, школьник

ВИДЫ КИБЕРУГРОЗ В СУДОВОЖДЕНИИ

В настоящий момент пользование электронных систем набирает все больше популярности во всех сферах жизни человека. Каждая электронная система может быть подвержена угрозе взлома с помощью внедрения различных вирусов и вредоносных программ. Знание всех видов информационного вмешательства ведет к предотвращению взломов систем или скорейшему восстановлению элетронно-информационных баз.

Наряду с прогрессом электронных систем каждая судоходная компания должна разработать план по кибербезопасности и меры по предотвращению кибервзломов и проводить с членами экипажа всех судов ежеконтрактный или полугодовой тренинг согласна разработанному плану и методам по киберзащите всех информационных баз данных.

В связи с вышеизложенным, в статье приведены виды киберугроз в сфере кибербезопасности и меры по предотвращению их действия и распространения в судовождении.

10. **Раковский Дмитрий Игоревич**, Московский технический университет связи и информатики, аспирант, ассистент

ПРОГНОЗИРОВАНИЕ ПРОФИЛЯ ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ АППАРАТА ТОЧЕЧНО-МНОЖЕСТВЕННЫХ ОТОБРАЖЕНИЙ

В работе приводится обоснование модели обнаружения и предупреждения нарушений в компьютерной системе посредством прогнозирования профиля поведения КС при помощи математического аппарата точечно-множественных отображений и многозначных зависимостей. Приводится обобщенная структура алгоритма, синтезированного на основе приведенной модели (Алгоритм Прогноза Многозначных Зависимостей, АМПЗ). Итогом работы является новый алгоритм прогнозирования профиля нормального функционирования КС, выраженных категориальными понятиями, на основе «исторических данных».

11. **Штеренберг Станислав Игоревич,** Московский технический университет связи и информатики, доцент, к.т.н.

ИССЛЕДОВАНИЯ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В РАМКАХ КОНЦЕПЦИИ РАЗВИТИЯ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ «ИНДУСТРИЯ 4.0»

В данном тезисе делается направление на исследования для мультиагентных систем искусственного интеллекта. Будет объяснено почему данный путь развития отечественных ИТ-систем, может быть, в определённой части прорывным и правильным с точки зрения построения как раз систем защиты информации.