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)

III Всероссийская научно-практическая конференция

«ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

8 ноября 2023 г.

ПРОГРАММА

Москва
2023

III Всероссийская научно-практическая конференция
«ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

* * *

ДАТА И МЕСТО ПРОВЕДЕНИЯ

8 ноября 2023 года,
09:00 – 17:00

Московский технический университет связи и информатики (МТУСИ),
г. Москва, ул. Авиамоторная, д. 8, стр. 39, Конгресс-центр

* * *

РЕГИСТРАЦИЯ УЧАСТНИКОВ, ПРИВЕТСВЕННЫЙ КОФЕ-БРЕЙК

09:00 – 10:00

Конгресс-центр, 1 этаж

* * *

ТОРЖЕСТВЕННОЕ ОТКРЫТИЕ, ПЛЕНАРНАЯ НАУЧНАЯ СЕССИЯ

10:00 – 12:30

Конгресс-центр, 2 этаж

Онлайн-трансляция: https://youtube.com/live/VX9TQGCZvYk?feature=share

ВЕДУЩИЙ:

Безумнов Данил Николаевич, Московский технический университет связи и информатики, начальник отдела по реализации образовательных проектов

ПРИВЕТСТВЕННОЕ СЛОВО:

Леохин Юрий Львович, проректор по научной работе МТУСИ, доктор технических наук, профессор

Белов Евгений Борисович, заместитель председателя ФУМО ВО ИБ

НАУЧНЫЕ ДОКЛАДЫ:

10:10 – 10:35

Теренин Алексей Алексеевич, управляющий директор Центра внутрикорпоративного взаимодействия Департамента кибербезопасности ПАО «Сбербанк», кандидат технических наук

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10:35 – 11:00

Буряков Виктор Михайлович, ассистент кафедры «Безопасность телекоммуникаций» МТУСИ

РОССИЯ И СКРЫТЫЕ УГРОЗЫ ЦИФРОВОЙ ПАРАДИГМЫ

11:00 – 11:25

Марков Алексей Сергеевич, президент АО «НПО «Эшелон»,

доктор технических наук, профессор
ПРИМЕНЕНИЕ ОТЕЧЕСТВЕННЫХ ТЕХНОЛОГИЙ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11:25 – 11:50

Булгакова Елена Валерьевна, доцент кафедры «Безопасность телекоммуникаций» МТУСИ, кандидат юридических наук, доцент

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ СУДЕБНОЙ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ ПО ИЗВЛЕЧЕНИЮ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ИЗ ЗАЩИЩЕННЫХ УСТРОЙСТВ

11:50 – 12:15

Кравец Василий Васильевич, начальник ОИИТ АО «ПМ»

УСТРОЙСТВО СЕРВИСОВ ОС WINDOWS И ЭКСПЛОЙТЫ СЕМЕЙСТВА POTATO

12:15 – 12:30

Дискуссия по научным докладам

*** * ***

ПЕРЕРЫВ

12:30 – 13:00

НАУЧНАЯ СЕКЦИЯ № 1
«Криптографические алгоритмы и анализ сетевого трафика»

13:00 – 17:00

Место проведения: МТУСИ, главный корпус, ауд. А-257

Дистанционное участие: https://events.webinar.ru/49645555/2091715665

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

Секретарь: **Раковский Дмитрий Игоревич,**
Московский технический университет связи и информатики, ассистент кафедры «Информационная безопасность»

НАУЧНЫЕ ДОКЛАДЫ:

1. **Цыгулев Игорь Николаевич**, Южно-Российский государственный политехнический университет имени М.И. Платова, Старший преподаватель кафедры "Информационная безопасность"

   Светашев Владислав Александрович, Южно-Российский государственный политехнический университет имени М.И. Платова, студент

   Дебеева Екатерина Евгеньевна, Южно-Российский государственный политехнический университет имени М.И. Платова, студент

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ ДЛЯ ПРОВЕДЕНИЯ СТАТИСТИЧЕСКИХ ТЕСТОВ ГЕНЕРАЦИЙ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Настоящая работа описывает разработку веб-приложения, предназначенного для выполнения тестов NIST Statistical Test Suite на мощных серверах. Приложение позволяет пользователям поэтапно загружать данные и анализировать их независимо друг от друга, обеспечивая эффективное использование вычислительных ресурсов. Такой подход позволяет быстро проводить анализ больших последовательностей случайных чисел, снижая нагрузку на вычислительные ресурсы.

После выполнения появляется необходимость объединить результат. Для этого был выбран метод оценки равномерности распределения с использованием статистики хи-квадрат. Такой подход обеспечивает точные результаты и повышает надежность анализа случайных числовых последовательностей.

Разработанное веб-приложение и методика анализа могут быть полезны в различных областях, включая статистику, криптографию и информационную безопасность.

2. **Чепурко Иван Александрович**, студент кафедры «Информационная безопасность» Южно-Российский государственный политехнический университет (НПИ)

   Лущаков Максим Александрович, студент кафедры «Информационная безопасность» Южно-Российский государственный политехнический университет (НПИ)

   Вахненко Игорь Викторович, Старший научный сотрудник НИО-1 НИЦ ВАС

ВЗАИМОСВЯЗЬ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ И АНАЛИЗА СЕТЕВОГО ТРАФИКА

Данная научная работа представляет собой обширный обзор ключевых аспектов криптографии, начиная с классических принципов и применений, и заканчивая передовыми тенденциями, такими как квантовая криптография. В работе подробно исследуются основные принципы криптографии, включая шифрование, асимметричные и симметричные ключи, а также основные алгоритмы, такие как RSA, AES, и 3DES. Особое внимание уделяется анализу и сравнительной оценке их эффективности и надежности в различных контекстах сетевого трафика.

3. **Раковский Дмитрий Игоревич**, Московский технический университет связи и информатики, ассистент кафедры "Информационная безопасность"

Александров Илья Дмитриевич, Московский технический университет связи и информатики, студент кафедры "Информационная безопасность"

Боков Александр Дмитриевич, Московский технический университет связи и информатики, студент кафедры "Информационная безопасность"

СТЕНД ДЛЯ СБОРА ТЕЛЕМЕТРИИ МНОГОЗНАЧНЫХ КОМПЬЮТЕРНЫХ АТАК

Современные компьютерные сети (КС) могут подвергаться нескольким компьютерным атакам одновременно. Актуальной задачей является разработка стенда для сбора телеметрии КС в условиях проведения многозначных контролируемых компьютерных атак. Новизна разработанного стенда заключается автоматизированной одновременной маркировке всех ККА, направленных на целевую КС. Собраны демонстрационные экспериментальные данные.

Анализ полученных данных показывает, что доля многозначных данных, собранных за время эксперимента, составляет 5% от общего числа записей.

4. **Липатников Валерий Алексеевич**, Военная академия связи, старший научный сотрудник НИЦ, доктор технических наук, профессор

Мелехов Кирилл Витальевич, Военная академия связи, адъюнкт

Щукин Андрей Владимирович, Военная академия связи, адъюнкт

МОДЕЛЬ ЦИФРОВОГО ПОТОКА СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ МНОГОЭТАПНЫХ АТАК

Для более детального рассмотрения процессов по управлению защищенностью сети передачи данных (СПД), предлагается исследовать особенности цифрового потока (ЦП) СПД в условиях многоэтапных атак (МЭА). Модель должна учитывать структурно-функциональные параметры. Целью работы является повысить защищенность СПД путем создания модели ЦП СПД в условиях МЭА и её исследования. Для исследования использовался метод положения теории формальных грамматик. Результатом данного исследования будет считаться модель ЦП СПД в условиях МЭА с учетом взаимоувязанных параметров исследуемого объекта. Новизна модели ЦП СПД в условиях МЭА в отличие от известных учитывает выделение признаков ЦП СПД, селекцию управляющей информации, данных с целью их дальнейшей обработки и распознавание возможного воздействия МЭА, определение мер защиты. Практическая значимость проведенного моделирования позволит разработать меры (способы) обеспечения защищенности СПД.

НАУЧНАЯ СЕКЦИЯ № 2
«Организационно-правовые и инженерно-технические методы защиты инфокоммуникационных систем»

13:00 – 17:00

Место проведения: МТУСИ, главный корпус, ауд. А-403

Дистанционное участие: https://events.webinar.ru/49645555/1285053733

Руководители: **Кубанков Александр Николаевич**,
Московский технический университет связи и информатики, заведующий кафедрой «Безопасность телекоммуникаций», доктор военных наук, профессор,

Булгакова Елена Валерьевна,
Московский технический университет связи и информатики, доцент кафедры «Безопасность телекоммуникаций», кандидат юридических наук, доцент

НАУЧНЫЕ ДОКЛАДЫ:

1. **Седаков Кирилл Андреевич,** ФГБОУ ВО «Брянский государственный технический университет»; ассистент кафедры «Системы информационной безопасности»
   Рытов Михаил Юрьевич, ФГБОУ ВО «Брянский государственный технический университет»; заведующий кафедры «Системы информационной безопасности»; к.т.н., доцент

АНАЛИЗ МЕТОДИКИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Привлекательность медучреждений для киберпреступников объясняется содержанием в информационных системах различной конфиденциальной информации, включая личные данные пациентов, номера банковских карт, медицинские сведения. В 2022 году здравоохранение стало самой атакуемой сферой, доля медицинских учреждений в статистике жертв киберпреступников постоянно росла: с 8% в 1 квартале до 12% в конце года.

2. **Робак Валерий Антонович,** Санкт-Петербургский государственный университет аэрокосмического приборостроения
   Задбоев Вадим Александрович, Военная академия связи имени С.М. Буденного
   Мелехов Кирилл Витальевич, Военная академия связи имени С.М. Буденного

МОДЕЛЬ СРЕДСТВА КОНТРОЛЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ, РАННЕГО ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ АТАК

В наше время, когда важность информационной безопасности нельзя переоценить, вопрос обработки и анализа информации о многоэтапной атаке (МЭА) становится все более актуальным. Повышение эффективности системы выявления аномалий может быть полезным для улучшения процесса сохранения полученной из них информации и прогнозирования будущих аномалий.

3. **Шевченко Александр Александрович,** Военная академия связи имени Маршала Советского Союза С.М. Буденного, старший научный сотрудник, к.т.н., университет аэрокосмического приборостроения

   Роговой Николай Александрович, Военная академия связи имени Маршала Советского Союза С.М. Буденного, оператор роты (научной)

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЗАРУБЕЖНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

В настоящее время мониторинг информационной безопасности является приоритетным направлением при обеспечении защищенности как государственных, так частных сетей передачи данных. В виду того, что существует очень много решений, позволяющих контролировать защищенность, в статье представлен анализ возможностей зарубежных средств, применяемых для мониторинга информационной безопасности сетей передачи данных, для выбора наиболее подходящего продукта.

4. **Борисова Влада Владимировна,** студент 3-го курса, Дальневосточный федеральный университет

   Дегтярев Данил Викторович, студент 2-го курса, Дальневосточный федеральный университет

   Боршевников Алексей Евгеньевич, и.о. директора департамента информационной безопасности ИМКТ ДВФУ

РЕАЛИЗАЦИЯ АЛГОРИТМА КВАНТОВОЙ ФАКТОРИЗАЦИИ ШОРА

Квантовый алгоритм Шора представляет собой метод факторизации целых чисел, позволяющий эффективно разложить большие числа на их простые множители. Этот алгоритм использует квантовые вычисления для решения задач, характеризующихся высокой вычислительной сложностью в рамках классических алгоритмов. В данном исследовании описывается основной механизм работы квантового алгоритма Шора и его применение в различных задачах. Также рассматривается, как данный алгоритм может быть реализован в квантовых вычислительных системах, и какие вычислительные ресурсы требуются для успешной его реализации.

5. **Звежинский Станислав Сигизмундович,** МТУСИ, профессор кафедры ИБ, д.т.н., профессор

   Альбов Николай Александрович, МТУСИ, магистрант 2-го года обучения

ВИДЕО РАСПОЗНАВАНИЕ ЛИЦ В СЛОЖНЫХ УСЛОВИЯХ

Представлен анализ истории развития и современного состояния алгоритмов видео распознавания лиц. Актуальность данного сегмента IT систем безопасности высока и подтверждается ростом в 1,5 раза в 2022 г. В стандартных условиях точность алгоритмов распознавания, основанных на CNN, достигает 99% и выше, однако в неблагоприятных условиях она составляет не более 95%, что ограничивает ее использование.

НАУЧНАЯ СЕКЦИЯ № 3
«Проблемы цифрового суверенитета и программно-аппаратные средства защиты инфокоммуникационных систем»

13:00 – 17:00

Место проведения: МТУСИ, библиотечный корпус, ауд. Б-201 (отдел ОНИРС)

Дистанционное участие: https://events.webinar.ru/49645555/458530052

Руководители: **Крылов Григорий Олегович**,
Московский технический университет связи и информатики, профессор кафедры «Безопасность телекоммуникаций», Финансовый университет при Правительстве Российской Федерации, профессор, доктор физико-математических наук, профессор

Буряков Виктор Михайлович,
Московский технический университет связи и информатики, ассистент кафедры «Безопасность телекоммуникаций»

НАУЧНЫЕ ДОКЛАДЫ:

1. **Пахомов Максим Анатольевич,** ФГАОУ ВО «СПбПУ», Институт компьютерных наук и кибербезопасности, аспирант

   Павленко Евгений Юрьевич, ФГАОУ ВО «СПбПУ», Институт компьютерных наук и кибербезопасности, к.т.н., доцент

   Сорокин Александр Алексеевич, ФГАОУ ВО «СПбПУ», Институт компьютерных наук и кибербезопасности, студент

РАЗРАБОТКА ПРОТОКОЛА БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ MANET-СЕТЕЙ

Исследованы проблемы обеспечения безопасной маршрутизации MANET-сетей, а также подходы к противодействию известных классов атак. Сформулирован состав протокола, реализующего защиту от внешних и внутренних нарушителей сети. Предложена модификация протокола оценки вредоносности узла сети с применением алгоритма случайного леса. Предложенные подходы сравнены с аналогами.

Ключевые слова: мобильные сети, безопасность маршрутизации, безопасность самоорганизующихся сетей.

2. **Гололобов Н.В.,** ФГАОУ ВО «СПбПУ», Институт компьютерных наук и кибербезопасности, аспирант

   Павленко Е.Ю., ФГАОУ ВО «СПбПУ», Институт компьютерных наук и кибербезопасности, к.т.н., доцент

ВЫЯВЛЕНИЕ АТАК НА РАСПРЕДЕЛЁННУЮ АВТОМОБИЛЬНУЮ КИБЕРФИЗИЧЕСКУЮ СИСТЕМУ НА ОСНОВЕ НЕРОЙННОЙ СЕТИ С ДОЛГОЙ КРАТКОСРОЧНОЙ ПАМЯТЬЮ

Состояние киберустойчивости системы во много определяется спецификой ее функционирования, степенью изоляции, количеством входных узлов и многими другими факторами. Длительность интервала безотказной работы зависит от большого числа факторов, точно предсказать которые невозможно, поэтому, отказ или нарушение безопасности обычно считают случайным событием. Киберустойчивость принято характеризовать вероятностью отказа в работе или нарушения состояния защищенности киберфизических систем (КФС) в течение определенного отрезка времени.

3. **Самарин Николай Николаевич,** ФГУП "НИИ "Квант", начальник научно-исследовательского отделения, к.т.н.

АНАЛИЗ ВОЗМОЖНОСТЕЙ НАПРАВЛЕННОГО ФАЗЗИНГ-ТЕСТИРОВАНИЯ В ЗАДАЧАХ ПОИСКА ОШИБОК В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Поиск и исправление ошибок в программном обеспечении (ПО) имеет большое значение при обеспечении безопасности информационной системы, в которой оно применяется. Согласно отчету, опубликованному компанией по кибербезопасности Veracode в 2017 году, наблюдается тенденция к увеличению числа использований методик гибкой разработки и применения ПО с открытым исходным кодом. В среднем, 75% ПО исходит из компонентов с открытым исходным кодом, поэтому уязвимости в этих компонентах создают огромный риск для безопасности. Применяемые в такого рода системах безопасности методы сосредоточены только на известных уязвимостях и практически не могут выявлять потенциальные уязвимости, скрытые в бинарном коде.

4. **Щербинина Инна Александровна,** Морской государственный университет им. адм. Г.И. Невельского, г. Владивосток, декан физико-технического факультета, к. п. н., доцент

   Потапова Ксения Андреевна, Морской государственный университет им. адм. Г.И. Невельского, г. Владивосток, аспирант

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИМЕНЕНИЯ RFID-ТЕХНОЛОГИЙ ПРИ ИДЕНТИФИКАЦИИ КОНТЕЙНЕРОВ

Объём внешнеторгового оборота – ключевой показатель мировой экономики, в частности, отношений между странами. Существует несколько способов транспортировки грузов. Для перевозки больших объёмов товаров на дальние расстояния самый экономически выгодный – морской транспорт, что обуславливает его востребованность во все времена. Согласно данным Росморречфлота, грузооборот морских портов России по итогам 2022 года увеличился на 0,7 % по сравнению с предыдущим годом и составил 841,5 млн тонн. В том числе, объем перевалки сухих грузов составил 404,7 млн тонн (-2,0%), наливных грузов – 436,8 млн тонн (+3,4%).

Однако, как утверждают члены экипажей, работающих на судах торгового флота, вопрос безопасности данных о грузе остаётся открытым до сих пор.

В данной статье рассматриваются проблемы безопасности при перевозке грузов, возникающие при применении RFID-технологий.

5. **Марченко Екатерина Александровна,** Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева», студент

   Жуков Семен Викторович, Федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева», старший преподаватель кафедры ГИиИБ

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ В DLP-СИСТЕМЕ ДЛЯ АНАЛИЗА ДАННЫХ

За последний год утекло больше 40 миллионов записей с персональными данными. Большие компании не могут рисковать такой статистикой. С одной стороны, они должны соответствовать нормативным требованиям и защищать чувствительные данные. С другой стороны, компании должны адаптироваться к современным реалиям и технологическим изменениям, которые, в свою очередь, подразумевают большую мобильность сотрудников, использование облачных приложений. Появилось больше свободы, а это значит, увеличивается количество способов утечки данных из организации. Технология применения нейронных сетей помогла бы оптимизировать работу систем контроля утечки данных и улучшить анализ данных в рамках поведенческого анализа.

НАУЧНАЯ СЕКЦИЯ № 4
«Кибербезопасность»

13:00 – 17:00

Место проведения: МТУСИ, главный корпус, ауд. А-254

Дистанционное участие: https://events.webinar.ru/49645555/1734826564

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

Секретарь: **Рыбаков Сергей Юрьевич**,
Московский технический университет связи и информатики, ассистент кафедры «Информационная безопасность»

НАУЧНЫЕ ДОКЛАДЫ:

1. **Затеев Станислав Вадимович,** Научно-инжиниринговый центр «Доверенные системы на основе АПК» ТУСУР, техник

ПРОДЛЕННАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ АНАЛИЗА КЛАВИАТУРНОГО ПОЧЕРКА

В современном мире цифровые технологии применяются во всех сферах нашей жизни. Огромное количество информации личного характера и информации иных видов, требующих соблюдения ее конфиденциальности, хранится в цифровом виде. Статья посвящена исследованию одного из самых распространенных типов СЗИ - средств идентификации и аутентификации пользователя. В статье описываются методы изучения и сбора клавиатурного почерка пользователей, методы формирования признаков клавиатурного почерка, а также модель, предназначенная для классификации параметров клавиатурного почерка по пользователям. Собранный материал составляет основу для реализации системы продленной аутентификации.

2. **Романова Надежда Николаевна,** Петербургский государственный университет путей сообщения, аспирант
   Грызунов Виталий Владимирович, Петербургский государственный университет путей сообщения, Доцент кафедры Информатики и информационной безопасности, доктор технических наук, доцент

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ЗЛОУМЫШЛЕННИКАМИ OSINT: СИСТЕМАТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ

В данной статье рассматривается процесс поиска литературы для изучения проблемы обеспечения безопасности персональных данных при использовании злоумышленниками OSINT методом систематического обзора литературы. В процессе обзора определяются исследовательские вопросы, поисковые запросы, критерии включения и исключения, оценки качества найденных источников. Из отобранных источников литературы даются ответы на поставленные вопросы исследования.

3. **Иванов Денис Александрович,** Филиал высшего учебно-научного центра военно-воздушных сил «военно-воздушная академия» в городе Челябинске, преподаватель, кандидат технических наук
   Горбатко Николай Владимирович, Филиал высшего учебно-научного центра военно-воздушных сил «военно-воздушная академия» в городе Челябинске, преподаватель, кандидат технических наук
   Яковлев Семён Владимирович, Филиал высшего учебно-научного центра военно-воздушных сил «военно-воздушная академия» в городе Челябинске, студент

БЕЗОПАСНОСТЬ И ЕЕ ТЕОРЕТИЧЕСКИЕ ОСНОВЫ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Анализ современных подходов к защите информации важнейших ИТ-сегментов показывает, что используемые в настоящее время методы и модели противодействия кибератакам на основные ИТ-сегменты не разрешают ряд противоречий. Способом создания защищенных от кибератак основных ИТ-сегментов является основной ИТ сегмент интеграции информационных технологий с датчиками противодействия кибератакам, а безопасность важнейших ИТ-сегментов будет достигнута при комплексном применении организационных и технических мер, максимальном использовании средств административного и сетевого мониторинга, антивирусных средств, сертифицированного программного обеспечения, компьютерного и коммутационного оборудования, а также компонентов противодействия кибератакам.

4. **Пономарёв Константин Гавриилович,** Дальневосточный федеральный университет, аспирант 2 курса Института математики и компьютерных технологий
   Верещагина Елена Александровна, Департамент программной инженерии и искусственного интеллекта Дальневосточного федерального университета, доцент, кандидат технических наук

ПРИНЦИПЫ КОНТРОЛЯ РЕЧЕВОГО ПОТОКА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ С ПРИМЕНЕНИЕМ СИСТЕМЫ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Речевой поток информации нуждается в таком же контроле и сборе сведений как и сетевой трафик телекоммуникационного оборудования, рабочих мест сотрудников в организации. Современные системы защиты от утечек информации, а также более большие системы управления событиями информационной безопасности, включающие в себя множество средств защиты информации должны включать в себя средства сбора и контроля речевой информации. Новые киберугрозы активно используют область звука, и мы уже сейчас наблюдаем массовое применение голосовых роботов и различных способов атак с помощью подмены владельца голоса. Данная работа направлена на изучение фундаментальных математических подходов по сбору речевой информации и практическому их использованию в сфере информационной безопасности.

5. **Лобов Борис Николаевич,** Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ))
   Загорулько Анна Федоровна, Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ))
   Игнатьев Даниил Русланович, Южно-Российский государственный политехнический университет имени М.И. Платова (ЮРГПУ (НПИ))

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ И ЧАСТНЫХ УЧРЕЖДЕНИЯХ И ОРГАНИЗАЦИЯХ ПОСРЕДСТВОМ АНАЛИЗА ЗАРУБЕЖНОГО И ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО-ОБЕСПЕЧЕНИЯ И ПРОГРАММ

Суть проблемы данного доклада сводится к замене иностранного ПО и программ на отечественные аналоги для исключения нарушения законодательства Российской Федерации, заранее встроенных уязвимостей в них, а также незаконного сбора и использования данных пользователей иностранными организациями. В настоящий момент необходимо поддерживать отечественных производителей программ и программного обеспечения, поскольку спрос и необходимость в нем с каждым днем растут все больше и больше.

6. **Лавров Павел Владимирович,** Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Студент 4 курса
Ильменёв Павел Александрович, Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Студент 4 курса
Ларичева Мария Сергеевна, Институт кибербезопасности и цифровых технологий РТУ МИРЭА
Потапова Дарья Александровна, Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Аспирант 3 курса

АКТУАЛЬНЫЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ И ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННЫХ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ

Данная статья посвящена рассмотрению современных сетевых атак, способов защиты от них с помощью отечественных средств защиты. С течением времени злоумышленники стали развивать и ухищряться свои способы атак на инфраструктуры различных компаний.Были рассмотрены способы решения современных сетевых атак, с помощью средств защиты информации класса NTA.

7. **Потапова Дарья Александровна,** Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Аспирант 3 курса
Ушаков Данила Анатольевич, Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Студент 4 курса
Ватутин Иван Геннадьевич, Институт кибербезопасности и цифровых технологий РТУ МИРЭА, Студент 4 курса

АНАЛИЗ УГРОЗ KERBEROS. УЧИМСЯ ДУМАТЬ, КАК ЗЛОУМЫШЛЕННИКИ

В данной статье представлен обзор различных атак на протокол аутентификации Kerberos, используемый в сетях и системах для обеспечения безопасности. Рассматриваются такие атаки, как Skeleton Key, Pass-the-Ticket, Golden Ticket Attack, Silver Ticket Attack, Kerberoasting, Pass-the-Key, DCShadow Attack и Diamond Ticket. Для каждой атаки предоставлено описание, сложность проведения, тактика MITRE, меры противодействия.

8. **Чекунов Никита Дмитриевич,** Студет БКС2001
Большаков Александр Сергеевич, Московский технический университет связи и информатики, доцент кафедры информационная безопасность, кандидат технических наук

РАЗРАБОТКА ЛАБОРАТОРНОГО СТЕНДА ОЦЕНКИ ЗАЩИЩЕННОСТИ ИС НА ПЛАТФОРМЕ EVE-NG

Доклад рассматривает процесс разработки лабораторного стенда для оценки защищенности информационных систем (ИС) с использованием платформы eve-ng. Будут представлены основные компоненты стенда, такие как виртуальные машины и сетевые устройства, а также рассмотрены различные методы оценки защищенности, включая сканирование уязвимостей и анализ потенциальных угроз. В результате доклада участники смогут ознакомиться с практическим подходом к оценке защищенности ИС и использованием платформы eve-ng в исследовании уязвимостей.

9. **Завадский Евгений Владимирович,** Санкт-Петербургский политехнический университет Петра Великого, аспирант
   Калинин Максим Олегович, Санкт-Петербургский политехнический университет Петра Великого, д.т.н., профессор

АДАПТИВНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ КИБЕРЗАЩИЩЕНОСТЬ НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗ ГРАФОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ ЦИФРОВОГО ДВОЙНИКА

Предложенное в рамках данной работы решение обеспечивает выявление и противодействие атакам программ-вымогателей (WannaCry) и APT-группировок. Точное определения трассы вторжения в КФС реализуется за счет внедрения в функциональную инфраструктуру узлов-индикаторов и применения методов интеллектуального интеллектуальном анализе графа функциональных зависимостей и графа потенциальных атак. Противодействие распространению атаки основано на прогнозируемой реконфигурации функциональной инфраструктуры: обнаруженные скомпрометированные узлы перемещаются в изолированный цифровой двойник защищаемой сетевой инфраструктуры с целью сбора поведенческих сигнатур и восстановление цепочек реализации технологических процессов.

Экспериментальное моделирование продемонстрировало корректную работу предложенного решения на развивающуюся целевую атаку и распространение программы-шифровальщика.

Таким образом, данные методы позволяют выявлять некорректное поведение узлов сетевой инфраструктуры и минимизировать последствия деструктивных воздействий со стороны злоумышленников.

10. **Балеев Михаил Алексеевич,** ЮФУ, ИКТИБ, кафедра БИТ им О.Б. Макаревича, студент
    Пескова Ольга Юрьевна, ЮФУ, ИКТИБ, кафедра БИТ им О.Б. Макаревича, к.т.н., доцент

OSINT-ИНСТРУМЕНТАРИЙ - ОПРЕДЕЛЕНИЕ ГЕОГРАФИЧЕСКОГО ПОЛОЖЕНИЯ ОБЪЕКТА ПО IP-АДРЕСУ

Данная работа описывает методику определения местоположения объекта, как юридического лица, по данному IP-адресу.

Задачи работы:

- формирование списка признаков, позволяющих определить расположение объекта;
- обзор сервисов, представляющих подобные услуги;
- разработка методики нахождения георасположения объекта по известному IP-адресу;
- разработке инструмента, основанного на сильных и слабых сторонах прямых аналогов, выполняющего данного рода задачи.

11. **Полтавцева Мария Анатольевна,** федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», профессор Высшей школы кибербезопасности, д.т.н., доцент
    Калинин Максим Олегович, федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет

Петра Великого», профессор Высшей школы кибербезопасности, д.т.н., профессор

МОДЕЛИРОВАНИЕ ДАННЫХ И ПРОЦЕССОВ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ БОЛЬШИХ ДАННЫХ

В докладе рассматривается современная экосистема больших данных, выделяются основные архитектурные уровни и связанные с ними проблемы кибербезопасности.

Обозначается проблема обеспечения безопасности систем управления большими данными, которым свойственны распределенность, различная структуризация и сложных жизненный цикл данных. Ключевым шагом для ее решения является общая модель данных для консистентного представления данных и процессов в рассматриваемых архитектурах. Авторами анализируются модели данных современных СУБД и предлагается модель на основе теории множеств, включая соответствующие структуры данных, операции и ограничения.

12. **Богдалов Руслан Рамильевич,** Московский технический университет связи и информатики, студент
Большаков Александр Сергеевич, Московский технический университет связи и информатики, доцент кафедры информационная безопасность, кандидат технических наук

РАЗРАБОТКА ПРОГРАММНОГО ПРОДУКТА КЛАССИФИКАЦИИ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ В АРМ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Данная статья посвящена разработке программного продукта, предназначенного для классификации вычислительных процессов в автоматизированных рабочих местах (АРМ). В работе рассматривается применение методов машинного обучения в контексте анализа и категоризации операций, выполняемых пользователем на АРМ. Авторы представляют архитектуру разработанного программного решения, описывают используемые алгоритмы машинного обучения и предлагают методику подготовки данных. Разработанный продукт обладает потенциалом для повышения производительности и безопасности рабочих процессов на АРМ, что делает его актуальным для широкого круга организаций и предприятий.

13. **Епифанцев Сергей Владимирович,** Московский технический университет связи и информатики; магистрант
Верба Вера Алексеевна, Московский технический университет связи и информатики, к.т.н., доцент
Корабельников Данила Алексеевич, ГБОУ Школа 1770 города Москвы

СОРЕВНОВАНИЯ В ФОРМАТЕ CTF КАК ВАЖНЫЙ ИНСТРУМЕНТ ПРОФОРИЕНТАЦИОННОЙ ПОДГОТОВКИ ШКОЛЬНИКОВ ДЛЯ ПОСТУПЛЕНИЯ В ТЕХНИЧЕСКИЕ ВУЗЫ НА НАПРАВЛЕНИЯ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

С каждым днем информационные технологии входят в жизнь людей все больше и больше. Связано это с тем, что информационные технологии позволяют существенно упростить жизнь человека. Однако, информационные

технологии несут не только пользу, но и создают новые угрозы, с которыми необходимо бороться. Для борьбы с появляющимися угрозами, в свою очередь, нужны специалисты в области информационной безопасности. Однако, для подготовки хороших специалистов в области информационной безопасности, необходимо чтобы школьники, поступающие в ВУЗы целенаправленно шли на направления, связанные с информационной безопасностью. Но многие школьники после выпуска не знают какое направление при поступлении в ВУЗ выбрать. Связано это с тем, что школьники не имеют представления о различных направлениях. В данной статье предлагается методика работы со школьниками, которая позволит ВУЗам получать абитуриентов, которые будут иметь базовое представление о различных направлениях информационной безопасности и целенаправлено поступать на определенное направление.

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

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ РЕСУРСЫ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

В докладе проводится систематизация и анализ существующих информационно-аналитических ресурсов, применимых в практике специалистов по информационной безопасности в целях выявления угроз безопасности информационным системам и уязвимостей в программном обеспечении. Отмечается, что действующая методика оценки угроз безопасности информации ФСТЭК указывает на применение подобных ресурсов при выполнении работ по созданию моделей угроз безопасности информации. В процессе изложенного в докладе исследования проводится взаимосвязь задач по выявлению и противодействию угрозам безопасности с существующими фактическими условиями и нормативно-правовыми требованиями. Всего приводится 15 наиболее популярных, востребованных и содержательных ресурсов, содержащих систематизированные и упорядоченные сведения по компонентам безопасности.

15. **Крундышев Василий Михайлович,** Санкт-Петербургский политехнический университет Петра Великого, доцент, кандидат технических наук
Калинин Максим Олегович, Санкт-Петербургский политехнический университет Петра Великого, профессор, доктор технических наук, профессор

МЕТОД ОБНАРУЖЕНИЯ АТАК ИСКАЖЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЛЛЕКТА

Анализ существующих решений по обеспечению защищенности систем искусственного интеллекта от атак искажения показал, что все известные решения сводятся к повышению устойчивости вычислительных моделей в условиях целенаправленных деструктивных воздействий. Для обнаружения атак искажения предложен подход на основе поиска аномалий в тестовых данных. Разработанный метод базируется на анализе степени уверенности вычислительной модели при решении задачи классификации последовательности входных данных.

16. **Бортников Максим Валерьевич,** Алтайский государственный технический университетим. И. И. Ползунова
Алексей Григорьевич Якунин, Алтайский государственный технический университетим. И. И. Ползунова, заведующий кафедрой, д.т.н., профессор

ПРИМЕНЕНИЕ CIPHER BLOCK CHAINING ТЕХНОЛОГИИ ДЛЯ ОБМЕНА ДАННЫМИ В IOT УСТРОЙСТВАХ

В данной работе приведено описание криптографического протокола для безопасного беспроводного управления IoT устройствами и иными встраиваемыми системами, выполненными на базе микроконтроллеров с ограниченной вычислительной мощностью. Основу протокола составляет Superencryption – шифрование с последовательным применением алгоритмов AES, Blowfish и Serpent в соответствии с технологией Cipher Block Chaining, а также ключевая хэш – функция HMAC-SHA256, необходимая для аутентификации и контроля целостности передаваемых сообщений. Для деривации ключей вместо алгоритма Диффи – Хелллмана было предложено использовать алгоритм, основанный на трёхкратной модификации четырёх ключей, используемых в алгоритме шифрования и в HMAC. Данный протокол был испытан на простейшей IoT системе, выполненной на микроконтроллерах ESP32и позволяющей дистанционно по Wi-Fi управлять работой четырёх реле.