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)

Всероссийская студенческая научно-практическая конференция

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

1 ноября 2022 г.

Всероссийская студенческая научно-практическая конференция
«ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ»

*** * ***

ДАТА И МЕСТО ПРОВЕДЕНИЯ

1 ноября 2022 г.

МТУСИ, Конгресс-центр
г. Москва, ул. Авиамоторная, д. 8, стр. 39

*** * ***

ПРОГРАММА МЕРОПРИЯТИЙ

* * *

РЕГИСТРАЦИЯ УЧАСТНИКОВ
ПРИВЕТСВЕННЫЙ КОФЕ-БРЕЙК

09:00 – 10:00

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 39 (конгресс-центр), 1-й этаж

* * *

ТОРЖЕСТВЕННОЕ ОТКРЫТИЕ

10:00 – 10:10

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 39 (конгресс-центр), 2-й этаж

ВЕДУЩИЙ:

Безумнов Данил Николаевич, Московский технический университет связи и информатики, старший преподаватель кафедры «Интеллектуальные системы в управлении и автоматизации»

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

НАУЧНАЯ ПЛЕНАРНАЯ СЕССИЯ

10:10 – 12:10

Место проведения:
г. Москва, ул. Авиамоторная, д. 8а, стр. 39 (конгресс-центр), 2-й этаж

ВЕДУЩИЙ:

Безумнов Данил Николаевич, Московский технический университет связи и информатики, старший преподаватель кафедры «Интеллектуальные системы в управлении и автоматизации»

НАУЧНЫЕ ДОКЛАДЫ:

10:10 – 10:40
Хромова Анна Владимировна, системный аналитик АО «ПМ»
ТЕНДЕНЦИИ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ РОССИИ: СОЗДАНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА

10:40 – 11:10
Крылов Григорий Олегович, профессор кафедры «Безопасность телекоммуникаций» МТУСИ, профессор Финансового университета при Правительстве РФ, доктор физико-математических наук, профессор
ГЕНЕЗИС И ЭВОЛЮЦИЯ ПРОБЛЕМЫ ИБ

11:10 – 11:40
Буряков Виктор Михайлович, старший технолог ПАО «Мегафон»
ТЕХНОЛОГИИ КАК ПРОДОЛЖЕНИЕ ПОЛИТИКИ ИНЫМИ СРЕДСТВАМИ

11:40 – 12:10
Панков Константин Николаевич, врио заведующего кафедрой «Теория вероятностей и прикладная математика» МТУСИ, кандидат физико-математических наук
ПОСТКВАНТОВЫЕ АЛГОРИТМЫ КРИПТОГРАФИИ В РАЗРАБОТКАХ СОВРЕМЕННЫХ РОССИЙСКИХ УЧЁНЫХ

* * *

ДИСКУССИЯ ПО ПЛЕНАРНЫМ НАУЧНЫМ ДОКЛАДАМ

12:10 - 12:20

* * *

ПЕРЕРЫВ

12:20 - 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. **Анисимов Михаил Андреевич**, Московский технический университет связи и информатики, студент

АТАКА НА TERRA LUNA

Доклад посвящён экосистеме TerraLuna, её привлекательности, истории создания. Проведён обзор атак на UST и LUNA. Рассмотрена экосистема Terra 2.0.

2. **Гладких Егор Алексеевич**, Курганский государственный университет, студент
Ананьев Владислав Андреевич, Курганский государственный университет, студент
Наточий Никита Михайлович, Курганский государственный университет, студент

КВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ

В этой статье проводится анализ квантовых вычислений в криптографии и рассмотрены направления развития квантовой криптографии. Рассматриваются решения актуальных проблем с информационной безопасностью, новые возможности квантовых алгоритмов и их преимущества перед классическими алгоритмами шифрования. А также уровень развития квантовых технологий в Российской Федерации

3. **Кушнир Дмитрий Викторович**, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, доцент, к.т.н., доцент
Шемякин Сергей Николаевич, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, доцент, к.т.н., доцент

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ В РЕАЛИЗАЦИИ КВАНТОВОГО КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛА

Современные системы обеспечения безопасности разрабатываются с учетом последних достижений в области криптоанализа. Одним из способов повышения уровня защищенности передаваемых данных является построение совершенных систем с распределением ключей по квантовому каналу. Хотя в целом сама идея квантовой криптографии подробно изучена, отдельные аспекты реализации требуют дальнейшего исследования. Отдельного внимания требует обеспечение подлинности данных, которыми законные пользователи обмениваются по классическому каналу. Без взаимодействия по классическому каналу обмен по квантовому каналу становится бесполезен. В данной статье речь идет о возможности и целесообразности применения различных методов аутентификации в рамках выполнения квантового криптографического протокола.

4. **Романов Илья Владимирович**, Поволжский государственный технологический университет, ФГБОУ ВО «ПГТУ», Волгатех, аспирант
   Сидоркина Ирина Геннадьевна, Поволжский государственный технологический университет, ФГБОУ ВО «ПГТУ», Волгатех, профессор, д.т.н., заведующая кафедрой Информационной безопасности
   Масленников Артём Николаевич, Поволжский государственный технологический университет, ФГБОУ ВО «ПГТУ», Волгатех, студент

УНИВЕРСАЛЬНЫЕ ПАРАМЕТРЫ ДЛЯ МОДИФИКАЦИИ МУРАВЬИНОГО АЛГОРИТМА ПРИ РЕШЕНИИ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ

На сегодняшний день в задачах аналитического характера широко используются генетические алгоритмы. Ключевая задача – поиск приближенных решений. Для подобных задач могут быть задействованы самые различные методы, модели и алгоритмы, включая применение технологии искусственного интеллекта. В статье представлены элементы, выделенного для исследования муравьиного алгоритма для решения задач поиска оптимальных решений, в профессиональной сфере и в частности информационной безопасности (ИБ). Где необходимо вычислить вероятностное значение при использовании большого набора качественных данных при использовании метода машинного обучения.

5. **Новиченко Александр Владимирович,** Акционерное общество "Перспективный мониторинг"
   Хромова Анна Владимировна, Акционерное общество "Перспективный мониторинг"

«МИКРОЦИКЛЫ» В РАБОТЕ АНАЛИТИКА

В статье приводится определении «микроциклов» при проведении расследования аналитиком в отношении объекта интереса. Микроциклы являются своеобразным «разведывательными циклами», в рамках проведения исследования каждого имеющегося объекта, при котором повышает ценность информации и приводит к получению новых исходных информации для обогащения имеющейся информации и проведения дополнительного исследования. В ходе такого «микрорасследования» можно найти другие «сущности», которые, в свою очередь, становятся объектами расследования. В статье приведен пример работы аналитика по одному из проектов.

НАУЧНАЯ СЕКЦИЯ
«Безопасность телекоммуникационных систем»

Руководитель: **Перфилов Олег Юрьевич**,
Московский технический университет связи и информатики, доктор технических наук, старший научный сотрудник, профессор кафедры «Безопасность радиосвязи»

Секретарь: **Буряков Виктор Михайлович**,
Московский технический университет связи и информатики, аспирант

НАУЧНЫЕ ДОКЛАДЫ:

1. **Алейников Александр Витальевич,** ЮРГПУ(НПИ) им. М.И. Платова, студент
   Загорулько Анна Федоровна, ЮРГПУ(НПИ) им. М.И. Платова, студент
   Сухоносов Федор Александрович, ЮРГПУ(НПИ) им. М.И. Платова, доцент

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

В данной научной статье рассматривается структура современных систем обнаружения вторжений (СОВ), проводится анализ используемых методов и моделей структуры СОВ, перспективы роста и развития данной технологии.

2. **Данилова Юлия Сергеевна,** Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент

АНАЛИЗ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ SIEM MAXPATROL

В России в последние годы резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих организаций. Лучший подход для предотвращения киберугроз - организация Security Operation Center (SOC). Стоит отметить, что в качестве базовой платформы для организации SOC, как правило, покупается SIEM-система (Security Information and Event Management). SIEM традиционно используются для решения проблемы накопления и оперативной обработки данных о событиях безопасности, поэтому основной задачей, решаемой в каждом проекте, является сбор, хранение и обработка событий информационной безопасности. В текущем докладе будет рассмотрено SIEM решение MaxPatrol от компании Positive Technologies и продемонстрировано, каким образом данная система способна выявлять инциденты из тысячи событий, поступающих из разных систем.

3. **Елецкий Андрей Евгеньевич,** Московский технический университет связи и информатики, студент

ИМПОРТОЗАМЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Данный доклад посвящен теме импортозамещения в сфере информационной безопасности. Рассмотрены причины развивать собственные разработки, примеры проблем, которые возникают в связи с отсутствием отечественных решений. Рассмотрены подходы других стран к импортозамещению в сфере ИБ. Подробно рассмотрено импортозамещение в России, его успехи, проблемы и перспективы, также в докладе присутствует интервью с ведущим инженером/архитектором проектов в сфере ИБ компании softline

4. **Топчиев Глеб Вячеславович,** ЮРГПУ(НПИ) им. М.И. Платова, студент

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Цель работы заключается в изучении и анализе Российского ПО а также офисных приложений, в связи с актуальностью замены иностранного ПО в рамках санкций в сторону Российской Федерации, для полного обеспечения независимости нашей страны в плане информационных технологий. В ходе работы показано, как проводить анализ ПО и на какие вещи нужно ориентироваться в первую очередь; определены зарубежные продукты, используемые в организациях на территории Российской Федерации, которые подлежат замене отечественными аналогами (система управления базами данных Oracle, операционные системы Windows и VMware, офисное приложение Microsoft Office, почтовая система Outlook) ; как достигнуть полной независимости от иностранного ПО и почему это так важно. В результате работы, определены ПО, приложения и программы, наиболее подходящие для замещения используемых зарубежных на данный момент. Итогом работы является комплекс ПО, приложения и программы, наиболее подходящие для замещения используемых зарубежных на данный момент.

5 **Шульга Антон Андреевич,** Московский технический университет связи и информатики; студент

КВАНТОВЫЙ КОМПЬЮТЕР

Мой доклад посвящен рассмотрению квантового компьютера и его принципа работы. В докладе проведен обзор квантового компьютера, его сравнения с традиционными персональным компьютером. Также в нем рассказано про роль квантового компьютера в сфере информационной безопасности. Будет ясно, насколько квантовый компьютер практичен, в чем он лучше или хуже обычного цифрового компьютера.

6. **Бобрешов Антон Юрьевич,** ЮРГПУ(НПИ) имени М. И. Платова, студент
Лобов Борис Николаевич, ЮРГПУ(НПИ) им. М.И. Платова, студент

МЕТОДИКА СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ

В данной статье рассматриваются методы повышения безопасности самой распространённой беспроводной технологии сети - Wi-Fi. Для этого указывается предмет исследования, объект исследования и цель исследования для более точной разработки методики совершенствования. Также выявляются проблемы этой технологии и стандартные меры по защите информации в ее сетях

7. **Жарова Анна Константиновна,** д.ю.н.
Елина Василиса Владимировна, Московский технический университет связи и информатики, студент

ОБЕСПЕЧЕНИЕ АТРИБУЦИИ КИБЕРАТАК

Проблема противодействия компьютерным атакам, является общей для всех государств, все информационно развитые государства взаимозависимы от уязвимостей, ошибок, программных закладок которые возможны в информационных технологиях, а результатом компьютерной атаки может стать межгосударственный конфликт.

8. **Максимов Олег Витальевич,** Курганский государственный университет, студент
Человечкова Анна Владимировна, Курганский государственный университет, старший преподаватель

ПРОБЛЕМЫ БЕЗОПАСНОСТИ "УМНОГО ГОРОДА"

В статье анализируются информационные компоненты системы «умного города». Выделяются уязвимости компонентов, взаимодействующих с данными о ситуации города и о горожанах. Приводятся примеры способов реализации обнаруженных уязвимостей. Предлагаются меры защиты элементов системы «умного города» от несанкционированного доступа.

9. **Сухоносов Федор Александрович**, ЮРГПУ (НПИ) им. М.И. Платова, доцент
Ратушняк Александр Иванович, ЮРГПУ (НПИ) им. М.И. Платова, доцент
Дмитрий Игоревич Шабельник, ЮРГПУ (НПИ) им. М.И. Платова, студент

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОВЕРШЕНСТВОВАНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ ЮРГПУ (НПИ)

Разработка предложений по совершенствованию защиты информации в инфокоммуникационной сети ЮРГПУ (НПИ)

10. **Чубан Анна Сергеевна,** ЮРГПУ(НПИ) ЮРГПУ (НПИ) им. М.И. Платова, студент

РИСК-АНАЛИЗ ИССЛЕДУЕМЫХ СИСТЕМ, В ОТНОШЕНИИ КОТОРЫХ РЕАЛИЗУЕТСЯ МОДЕЛЬ УГРОЗ ИБ.

Достижение требуемого уровня информационной безопасности в любой организации должно базироваться на исследовании источников угроз информации, уязвимостей в ее защите, и проистекающих из их соотношений рисков. Механизм эффективного противодействия угрозам информационной безопасности содержится в доступных международных стандартах, прежде всего в современных риск-ориентированных стандартах ISO (International Organization for Standardization) и аналогичных национальных стандартах.

11. **Алейников Александр Витальевич,** ЮРГПУ(НПИ) им. М.И. Платова, студент
Загорулько Анна Федоровна, ЮРГПУ(НПИ) им.М.И. Платова, студент
Сухоносов Федор Александрович, ЮРГПУ(НПИ) им.М.И. Платова, доцент

РУТКИТЫ - РАЗВИТИЕ И СПОСОБ ИХ ОБНАРУЖЕНИЯ

В данной научной статье рассматривается структура современных систем обнаружения вторжений (СОВ), проводится анализ используемых методов и моделей структуры СОВ, перспективы роста и развития данной технологии.

12. **Мясищева Наталья Романовна,** Московский технический университет связи и информатики, студент
Николаев Владимир Владимирович, Московский технический университет связи и информатики, ассистент

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

В статье был проведен анализ развития руткитов за последние 10 лет, выявлены их особенности, а также сфера применения. В первой части дается характеристика данного вируса и приводится пример атаки с его использованием. Во второй части статьи обозначены типы руткитов, способы распространения и цели применения. Третья часть посвящена концепциям защиты и их эффективности в борьбе с атаками такого типа.

13. **Басак Валерий Васильевич,** ЮРГПУ(НПИ) им. М.И. Платова, студент
Сухоносов Федор Александрович, ЮРГПУ(НПИ) им. М.И. Платова, доцент

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕРКЕ ТЕЛЕКОММУНИКАЦИОННЫХ ПРЕДПРИЯТИЙ И ВЕДОМСТВ "УПРАВЛЕНИЯ ПЕРСОНАЛОМ"

Суть данной статьи сводится к совершенствованию методики проведения аудита информационной безопасности (ИБ) при проверке телекоммуникационных предприятий и ведомств «Управления персоналом». Объектом исследования являются процессы аудита информационной безопасности ведомств «Управления персоналом». Предметом исследования являются методы совершенствования внутреннего аудита информационной безопасности контрольной среды - подпроцесса «Формирование кадровой политики».

14. **Кашин Юрий Олегович,** Московский Университет МВД России им. В.Я. Кикотя, курсант
Рязанова Анна Максимовна, Московский Университет МВД России им. В.Я. Кикотя, курсант
Булгаков Владислав Владимирович, ГБОУ "Школа Свиблово" г. Москвы, ученик

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ ХРАНИЛИЩАХ ДАННЫХ

Доклад посвящен проблемам защиты облачных данных от несанкционированного доступа, а также обеспечению безопасности хранящихся данных. Рассматривается необходимость защиты данных в облачном пространстве и основные угрозы безопасности облачных данных, варианты их решения. В качестве проблем освещены небезопасные API, проблемы при репликации данных и внутренние угрозы. В качестве способов защиты данных предлагаются такие решения как: шифрование данных, правильное хранение конфиденциальных данных, зашифрованные облачные сервисы, непрерывное обновление системы, правила трансграничной передачи данных и другие.

15. **Потыкун Ника Александровна,** ЮРГПУ(НПИ) им. Платова М. И. студент кафедры ИБ

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

В статье рассказывается про то, как люди подвергаются информационно-психологической атаке. Приведены способы защиты от информационной-психологической угрозы в обществе. Приводится таблица сравнения ежегодных подсчётов в сравнении онкобольных и людей с нарушенной психикой. Рассказывается как проводятся тренинги с потерпевшими, которые нуждаются в помощи после атак.

16. **Стецко Даниил Богданович,** МТУСИ, студент 1 курса

КРИПТОДЖЕКИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЗАРАЖЕНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

НАУЧНАЯ СЕКЦИЯ
«Кибербезопасность автоматизированных и компьютерных систем»

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

НАУЧНЫЕ ДОКЛАДЫ:

1. **Ананьев Владислав Андреевич**, Курганский государственный университет, студент
Гладких Егор Алексеевич, Курганский государственный университет, студент
Наточий Никита Михайлович, Курганский государственный университет, студент

CSRF-АТАКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

В данной статье приведены основные методы по обеспечению безопасности от CSRF–атак. В статье описаны решения по борьбе с ними, такие как: использование токенов авторизации и SameSite атрибута, задействование заголовков Origin и Referer, создание пресессий, подтверждение запроса капчей или кодом, применение двухфакторной аутентификации.

2. **Желобенко Кирилл Андреевич**, РТУ МИРЭА, студент 5 курс, специалитет

АВТОМАТИЗИРОВАННАЯ СИСТЕМА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ СОТРУДНИКОВ КОМПАНИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Актуальность: Компьютерная безопасность это область знаний, охватывающая модели, методы, программные, аппаратно - программные средства, системы защиты информации при ее обработке, хранении и передаче с использованием информационных технологий. Компьютерная безопасность это защита информации на компьютере, на мобильных устройствах от различного рода случайных или умышленных её повреждений, удаления, а также защита персональных данных на компьютере от взлома и кражи. К задачам компьютерной безопасности относится стабильность работы программ, операционных систем, компьютерных сетей. Безопасность информационных систем является частью более широкой проблемы: безопасность компьютерных систем или еще более общей проблемы информационной безопасности. Задачи: Основными угрозами для системы электронного документооборота, как и для любой другой информационной системы, являются:

Угроза целостности информации – повреждение, искажение или уничтожение информации;

Угроза доступности информации – ошибки пользователей, внешние сетевые атаки, вредоносное ПО.

Угроза конфиденциальности – кража информации, подмена маршрутов обработки, несанкционированный доступ к информации.

Цель данного проекта создание защищённой изолированной системы. Также Основной целью, на достижение которой направлены все положения настоящей Концепции, является защита субъектов информационных отношений (интересы которых затрагиваются при

создании и функционировании АС ОРГАНИЗАЦИИ) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АС ОРГАНИЗАЦИИ или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной системы ее обработки.

3. Лупашко Роман Владимирович, Курганский государственный университет, Информационная безопасность автоматизированных систем, 4 курс

Лупашко Светлана Геннадьевна, Курганский государственный университет, доцент, к.ф.-м.н., доцент

Дик Дмитрий Иванович, Курганский государственный университет, доцент, к.т.н., доцент

АЛГЕБРАИЧЕСКИЙ ПОДХОД В АЛГОРИТМЕ МОДИФИКАЦИИ ЛОГИЧЕСКИХ ВЫРАЖЕНИЙ

Одной из задач, стоящей перед криптоаналитиками и реверс-инженерами является анализ, запутывание и сокрытие предназначения криптографических алгоритмов и алгоритмов в программно-аппаратных комплексах. В статье предложена классификация подходов к модификации булевых выражений и представлен новый обучающийся алгоритм, реализующий алгебраический подход.

4. Наточий Никита Михайлович, Курганский государственный университет, студент 2 курса

Ананьев Владислав, Курганский государственный университет, студент 2 курса

Гладких Егор Алексеевич, Курганский государственный университет, студент 2 курса

АНАЛИЗ МЕТОДОВ ГАРАНТИРОВАННОГО УДАЛЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

В данной статье приведён сравнительный анализ методов гарантированного удаления конфиденциальной информации на различных электронных носителях. В статье подробно рассмотрены особенности стирания данных с жестких дисков и твердотельных накопителях. Также особое внимание было уделено целесообразности применения данных методов в сфере бизнеса и государственного управления.

5. Хоромская Ангелина Юрьевна, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 193232, Санкт-Петербург, пр. Большевиков д.22, к.1 10.04.01 Информационная безопасность, 1 курс

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ПОЛЬЗОВАТЕЛЯ

Искусственный интеллект (ИИ) широко применяются в информационных системах для увеличения производительности труда, повышения продаж, обучения, его использование в защите от кибератак становится одним из ключевых направлений в информационной безопасности. На текущий момент количество атак растёт, а ландшафт угроз меняется с молниеносной скоростью. Продукты Kaspersky отражают более 700 млн. онлайн-атак в квартал по всему миру, а Cisco заявляет о блокировании 20 млрд. сетевых атак в день. При таких объёмах вредоносной деятельности активно применяют средства автоматизации кибератак, в том числе используют технологии искусственного интеллекта для их совершенствования и трансформации, а также для обхода известных средств защиты. Необходимо использовать ИИ для усиления атаки, встраиваясь в цепочки разговоров и используя анализ текста на естественном языке. Другой возможной сферой вредоносного применения искусственного интеллекта мог стать более эффективный подбор паролей или

обход аутентификации. Используя огромное количество различных источников, данных для формирования базы знаний искусственного разума, злоумышленники могут сделать атаки на человека по-настоящему действенными. Для того чтобы справиться с растущим объёмом атак, производители систем защиты тоже начинают активно внедрять технологии искусственного интеллекта для обнаружения, прогнозирования киберугроз, реагирования на них в режиме реального времени.

6. **Нефедов Виталий Владимирович,** Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, студент 2 курса магистратуры

МЕТОДЫ ВНЕДРЕНИЯ САМОМОДИФИЦИРУЮЩЕГОСЯ КОДА В ИСПОЛНЯЕМЫЕ ФАЙЛЫ PE-ФОРМАТА

Любая операционная система требует дополнительных специальных средств защиты информации помимо тех, которые имеются в стандартном наборе операционной системы. Обычно средства защиты информации работают в автоматизированном режиме, выполняя наиболее простые действия по защите информации, а сложные решения принимает человек на основе подготовленных шаблонов. В дополнение к имеющимся средствам защиты информации имеется возможность использовать самомодифицирующийся код, внедренный в исполняемые файлы.

7. **Задворьев Егор Федорович,** Московский Государственный Технический Университет Гражданской Авиации, студент
Савицкий Евгений Владимирович, Московский Государственный Технический Университет Гражданской Авиации, студент

МОДЕЛЬ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

В работе рассматривается игровая модель оценки злоумышленного воздействия на локальную вычислительную сеть при различных исходных условных состояниях информационной безопасности. Пользуясь антагонистическими моделями игры, определяется оптимальная стратегия для минимизации рисков потерь при возможной вариативности проведения атак злоумышленником.

8. **Лазорин Данил Сергеевич,** Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина», студент 2 курса

О ПОДХОДАХ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Статья посвящена рассмотрению существующих подходов к обеспечению информационной безопасности цифровых двойников и формулированию предложений по выбору средств противодействия различным угрозам, прежде всего угрозе искажения цифрового двойника. Показано, что ни один из существующих подходов и методов не обеспечивает полноценной безопасности цифровых двойников. Предложена реализация комплексного подхода для обеспечения безопасности цифровых двойников в рамках актуальных для них специфических моделей угроз и нарушителя.

9. **Воеводин Владислав Александрович,** Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», доцент кафедры "Информационная безопасность", к.т.н.
Виноградов Иван Вадимович, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», студент
Волков Даниил Игоревич, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», студент

О ПРОБЛЕМЕ ВНЕДРЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ПРИ РЕШЕНИИ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

В силу закона обладатель информации обязан принять меры по защите информации. На сегодняшний день для управления информационной безопасностью имеют место два подхода. Первый подход — директивный, при котором Регулятор формирует требования к защите информации и организует проверку их исполнения. Регулирование отношений осуществляется через институт ответственности за нарушения законодательства РФ об информации, информационных технологиях, т. е. в основном работает административный фактор. Второй подход — риск-ориентированный, при котором решение о допустимом уровне риска принимает владелец риска на основе оценки реальных угроз информационной безопасности и уязвимостей рубежей объекта защиты. Преимуществом второго подхода является то, что при его внедрении включается экономическая составляющая. Цель доклада – сообщить о результатах исследования правовой, организационной и методической составляющих, препятствующих внедрению риск-ориентированного подхода к управлению информационной безопасностью.

10. **Рязанова Анна Максимовна,** Курсант Московского Университета МВД России им. В. Я. Кикотя
Кашин Юрий Олегович, Курсант Московского Университета МВД России им. В. Я. Кикотя
Булгаков Владислав Владимирович, Ученик 11 класса ГБОУ "Школа Свиблово" г. Москвы

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ ХРАНИЛИЩАХ ДАННЫХ

Доклад посвящен проблемам защиты облачных данных от несанкционированного доступа, а также обеспечению безопасности хранящихся данных. Рассматривается необходимость защиты данных в облачном пространстве и основные угрозы безопасности облачных данных, варианты их решения. В качестве проблем освещены небезопасные API, проблемы при репликации данных и внутренние угрозы. В качестве способов защиты данных предлагаются такие решения как: шифрование данных, правильное хранение конфиденциальных данных, зашифрованные облачные сервисы, непрерывное обновление системы, правила трансграничной передачи данных и другие.

11. **Урванцев Данила Никитич,** ПГТУ, ст. группы БИ-51
Филонова Марина Владимировна, ПГТУ, ст. группы БИ-51
Петухова Элина Эдуардовна, ПГТУ, ст. группы БИ-51

ОРГАНИЗАЦИЯ ПРОГНОЗИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ БАНКА ДАННЫХ УГРОЗ

В данной научной статье представлен оригинальный подход к прогнозированию угроз информационной безопасности автоматизированных и компьютерных систем путём объединения двух методов прогнозирования: декомпозиции угрозы на составляющие, а также анализ безопасности критических точек инфраструктуры предприятия.

12. **Свиридов Владислав Витальевич,** Российский Технологический Университет - МИРЭА, институт кибербезопасности и цифровых технологий, Кафедра КБ-1 "Защита информации", студент
Головченко Дарья Андреевна, Российский Технологический Университет - МИРЭА, институт кибербезопасности и цифровых технологий, Кафедра КБ-1 "Защита информации", ст. преподаватель

ОТСЛЕЖИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ WEB-САЙТАМИ

Большинство web ресурсов собирают данные пользователей и более того, эти данные часто передаются третьим лицам, которые в основном используют их в рекламных целях, однако возможности их использования поистине безграничны. Рассмотрены способы отслеживания и принципы построения системы защиты, например, такую как:

установка специализированного программного обеспечение в совокупности с иными методами повышения конфиденциальности, такими как VPN, и регулярная очистка файлов cookies может обеспечивать высокий уровень борьбы с программными средствами отслеживания пользователей web ресурсов.

13. **Баулина Анна Алексеевна,** Федеральное государственное бюджетное образовательное учреждение высшего образования «Ярославский государственный университет им. П.Г. Демидова», студент

СПОСОБЫ ЗАЩИТЫ ОТ УЯЗВИМОСТЕЙ В ЯЗЫКЕ JAVA

В процессе разработки информационной инфраструктуры возникает много вопросов о работе с данными, в том числе, как сохранять информацию объекта даже в то время, когда программа не работает; как организовать распределенную обработку данных, где объекты передаются с одной виртуальной машины на другую; как реализовать восстановление после отказа и выравнивания нагрузки серверов. Для этих целей часто используют сериализацию.

Сериализация — это процесс преобразования объекта в поток байтов для сохранения или передачи в память, базу данных или файл. К сожалению, нельзя слепо полагаться на встроенные механизмы сериализации, которые есть во всех распространенных языках программирования. По данным Национальной базы данных уязвимостей США с начала 2022 года было зарегистрировано уже более 80 уязвимостей, возникших в процессе десериализации в различных программных продуктах.

Были выявлены уязвимости десериализации в языке программирования Java и предложены способы обеспечения безопасности ПО.