24 марта, вторник. День заезда

15:00	Трансфер от станции метро «Ховрино» до отеля «Солнечный Park Hotel & SPA»
16:00 – 22:00	Заезд и регистрация участников, проживающих в отеле. Ужин. Вечерняя программа

25 марта, среда. Первый день работы конференции

08:00 – 09:00	Завтрак		
09:00 – 10:00	Регистрация участников конференции		
10:00 –12:00	Официальное открытие конференции **10:00 –12:00 Пленарное заседание** **ЗАЛ «ШИШКА»**		
12:00 –12:30	Кофе-брейк		
12:30 – 14:00	**12:30 – 14:00** Секция «**Информационные системы государства, кибербезопасность и криптография»** **ЗАЛ «ШИШКА»** На сцене: **1. СКВОРЦОВА Т.В.**, Минцифры **2. СМЫШЛЯЕВ С.В.**, КриптоПро	**12:30 – 14:00** Секция **«Аппаратная безопасность»** **ЗАЛ «ЕЛОВЫЙ»** На сцене: **1. УСАНОВ А.Е.**, Positive Technologies	**12:30 – 14:00** Круглый стол «**Олимпиады и научные школы»** **КИНО-КОНЦЕРТНЫЙ ЗАЛ** На сцене: **1. ТОКАРЕВА Н.Н.**, НГУ **2. ПУДОВКИНА М.А.**, МИФИ **ЭКСПЕРТЫ** **3. ПРАВИКОВ Дмитрий Игоревич** РГУ нефти и газа (НИУ) имени И.М. Губкина **4. ПИЧКУР Андрей Борисович** Гарда Технологии **5. КЯЖИН Сергей Николаевич** НИЯУ МИФИ **6. КАТЫШЕВ Сергей Юрьевич** ФУМО ВО ИБ **7. ПАНАСЕНКО Сергей Петрович** Компания «Актив» **8. СЕЛИВАНОВА Анна Юрьевна** ИКНК СПбПУ **9. КОРЕНЕВА Алиса Михайловна** Код безопасности
14:00 –15:00	Обед		
15:00-16:30	**15:00 – 16:30** Секция **«РБПО и подпись ПО, построение единого пространства доверия к российскому программному обеспечению»** **ЗАЛ «ШИШКА»** **1. ГУСЕВ Дмитрий Михайлович** ИнфоТеКС **2. КАЧАЛИН Игорь Федорович** АНО «НТЦ ЦК» **3. СМЫШЛЯЕВ Станислав Витальевич** КриптоПро	**15:00 – 16:30** Секция **«Проекты, технологии и решения»** **ЗАЛ «ЕЛОВЫЙ»** **1. ПОТАШНИКОВ Александр Викторович** ИнфоТеКС	**15:00 – 16:30** Секция **«Интеллектуальные методы анализа безопасности программных и аппаратных систем»** **ЗАЛ «СОСНОВЫЙ»** **1. ПАВЛЕНКО Евгений Юрьевич** **Высшая школа кибербезопасности СПбПУ**
16:30 – 17:00	Кофе-брейк		

17:00 – 19:00	**17:00 – 19:00** Дискуссионная панель **«ЭДО в России»** **КИНО-КОНЦЕРТНЫЙ ЗАЛ** **1. МАЛИНИН Юрий Витальевич**, Ассоциация «РОСЭУ» **2. КИРЮШКИН Сергей Анатольевич**, Газинформсервис **ЭКСПЕРТЫ** **3. НОВИКОВ Фёдор Вадимович,** ФНС России **4. СМИРНОВ Павел Владимирович,** КриптоПро **5. ЛАБУЦКАЯ Анастасия Сергеевна,** СКБ Контур	**17:00 – 19:00** Секция **«Криптография и криптоанализ», 1 часть** **ЗАЛ «ЕЛОВЫЙ»** **1.МАТЮХИН Дмитрий Викторович,** ФСБ России **2. АЛЕКСЕЕВ Евгений Константинович,** КриптоПро, АНО «НТЦ ЦК» **3.ПОТАШНИКОВ Александр Викторович,** ИнфоТеКС	**17:00 – 19:00** Секция **«Криптография в медицине»** **ЗАЛ «СОСНОВЫЙ»** **1. МЕЛКУМЯН Наталья Директор по клиентскому сервису,** КриптоПро **2. НУРИАХМЕТОВ Дмитрий** ГК «Мать и дитя»
19:00– 23:00	Ужин. Вечерняя программа		

26 марта, четверг. Второй день работы конференции

08:00 – 10:00	Завтрак		
10:00 – 11:30	**10:00 –11:30** Секция **«Криптографические средства защиты информации: разработка, сертификация, внедрение и эксплуатация»** **ЗАЛ «ШИШКА»** **1. ПЕТРОВ Алексей Владимирович** ФСБ России	**10:00 –11:30** Секция **«Криптография и криптоанализ», 2 часть** **ЗАЛ «ЕЛОВЫЙ»** **1.МАТЮХИН Дмитрий Викторович,** ФСБ России **2. АЛЕКСЕЕВ Евгений Константинович,** КриптоПро, АНО «НТЦ ЦК» **3.ПОТАШНИКОВ Александр Викторович,** ИнфоТеКС	**10:00 –11:30** Секция **«Криптографические решения для киберфизических систем»** **ЗАЛ «СОСНОВЫЙ»** **1. СОРОКИНА Марина Викторовна,** ИнфоТеКС **2. ЛАЗАРЕВ Алексей Станиславович,** Компания «Актив»
11:30 – 12:00	Кофе-брейк		
12:00 – 14:00	**12:00 –14:00** Секция **«Информационная безопасность и криптография кредитно-финансовой сферы»** **ЗАЛ «ШИШКА»** **1. ЕЛИСТРАТОВ Андрей Алексеевич,** Банк России **2. ГОРЕЛОВ Дмитрий Львович,** Компания «Актив»	**12:00 –14:00** Секция **«Криптография и криптоанализ», 3 часть** **ЗАЛ «ЕЛОВЫЙ»** **1.МАТЮХИН Дмитрий Викторович,** ФСБ России **2. АЛЕКСЕЕВ Евгений Константинович,** КриптоПро, АНО «НТЦ ЦК» **3.ПОТАШНИКОВ Александр Викторович,** ИнфоТеКС	**12:00 –14:00** Секция **"Квантово-устойчивая защита информации. Наука, технологии, регуляторика и кадры"** **ЗАЛ «СОСНОВЫЙ»** **1. КОРОЛЬКОВ Андрей Вячеславович**, НКЦКИ, Академии криптографии РФ **2. ФЕДОРОВ Алексей Константинович PhD, вице-президент**, Газпромбанк
14:00 – 15:00	Обед		
15:00 – 16:30	**15:00 –16:30** Круглый стол **«Мобильные решения и криптография»** **ЗАЛ «ШИШКА»** **1. ПЬЯНЧЕНКО Андрей Андреевич**, MAX **2. ДЕГТЯРЕВ Алексей Валерьевич**, Сбер **3. АБРАМОВ Михаил Андреевич,** ФНС России **4. СЕМЕНОВ Евгений Николаевич,** Центр Биометрических Технологий **5 ГОРБУТ Андрей Александрович,** Сбер **6. ВЕРЕСТНИКОВА Дарья Дмитриевна**, СТ-Крипт **7. ЕЛИСТРАТОВ Андрей Алексеевич,** Банк России **8. ПЕТРОВ Алексей Владимирович,** ФСБ России	**15:00 –16:30** Секция **«Математические аспекты защиты информации в области синтеза и анализа генераторов случайных чисел»** **ЗАЛ «ЕЛОВЫЙ»** **1. МИРОНКИН Владимир Олегович,** ФСБ России	**15:00 –16:30** Секция **«Перспективные исследования в области кибербезопасности», 1 часть** **ЗАЛ «СОСНОВЫЙ»** **1. КОТЕНКО Игорь Витальевич,** СПб ФИЦ РАН
16:30 – 17:00	Кофе-брейк		

17:00 – 19:00	**17:00 – 19:00** Круглый стол **«Кибербезопасность и криптография в крупном бизнесе»** **ЗАЛ «ШИШКА»** **1.Качалин Алексей Игоревич**, эксперт по развитию информационной безопасности и инновациям. Советник руководителей и владельцев бизнеса. kachalin.com **2. Ярунин Александр Андреевич**, X5 Group **3.Дрозд Алексей Сергеевич**, ПАО «Вымпелком» **4.Дутов Кирилл Сергеевич**, Промсвязьбанк **5.Иванов Алексей Александрович**, АО "АЛЬФА-БАНК”	**17:00 – 19:00** Секция **«Криптография и криптоанализ», 4 часть** **ЗАЛ «ЕЛОВЫЙ»** **1.МАТЮХИН Дмитрий Викторович,** ФСБ России **2. АЛЕКСЕЕВ Евгений Константинович,** КриптоПро, АНО «НТЦ ЦК» **3.ПОТАШНИКОВ Александр Викторович,** ИнфоТеКС	**17:00 – 19:00** Секция **«Перспективные исследования в области кибербезопасности», 2 часть** **ЗАЛ «СОСНОВЫЙ»** **1. КОТЕНКО Игорь Витальевич,** СПб ФИЦ РАН
19:00 – 23:00	Ужин, вечерняя программа		

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

10:00 –12:00 Пленарное заседание

ЗАЛ «ШИШКА»

Официальное открытие конференции

Приветственные слова

Доклады:

1) **Если не ГОСТ, но очень хочется: "ПРАПОР-К" и "Рамен-К" - новые семейства (низкоресурсных) блочных шифров**

Матюхин Дмитрий Викторович, к.ф.-м.н., ФСБ России

2) **Российская криптография и технологическая независимость**

Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор КриптоПро

Обзор важнейшей для отрасли существенной трансформации российской криптографии, произошедшей за последние годы в связи с задачами достижения технологической независимости. Из области, которая для большого числа конечных потребителей была связана лишь с необходимостью выполнения требований различных НПА, она существенно преобразовалась в сторону закрытия реальных потребностей пользователей. Этому способствовало то, что к 2022-му году отрасль была уже настолько зрелой, что уход зарубежных ИТ- и ИБ- компаний привел к росту, а не к падению уровня применяемых решений. Примеры классов решений, иллюстрирующих данные изменения: системы защиты биометрических данных, средства защиты платежной инфраструктуры, средства электронной подписи и VPN-решения, а также многие другие (VPN, центры сертификации, ДЭГ, подтверждение банковских операций).

3) **Российская криптография в финансовых сервисах. Прошлое, настоящее, будущее.**

Елистратов Андрей Алексеевич, к.ф.-м.н., Банк России

Ретроспектива использования российских криптографических средств в финансовой сфере. Развитие финансовых технологий в разрезе реализации современных требований по информационной безопасности. Достигнутые результаты, чего удалось добиться на сегодняшний день. Особое внимание в докладе будет уделено проекту цифрового рубля и обеспечению безопасности как на стороне конечного клиента, так и на стороне финансового посредника и платформы. Будет рассказано о дальнейших шагах по укреплению информационной безопасности финансовой отрасли за счет более комплексного использования российской криптографии.

4) **Квантовые идеи в задачах криптоанализа и искусственного интеллекта**

Баранов Александр Павлович, д.ф.-м.н., действительный член Академии криптографии Российской Федерации

Исследования математических проблем криптографии последних лет выявили определенные тенденции применения идей квантовой физики для решения задач, связанных с различными аспектами оценки стойкости криптосистем. В докладе, на основе результатов ряда опубликованных работ отечественных авторов, излагается применение квантовых идеи для анализа широкого класса систем таких, как электронная подпись и «открытое» распределение ключей, базирующиеся на оценке трудоемкости логарифмирования в конечных полях, регистровые криптосхемы, а также оптимизационные задачи в системах искусственного интеллекта и др.

ЗАЛ «ШИШКА»

12:30 – 14:00

Секция «Информационные системы государства, кибербезопасность и криптография»

Криптографическая защита является фундаментом обеспечения информационной безопасности в современных информационных системах. Системы министерств, ведомств и служб создаются и развиваются с учётом требований к криптографической защите. Представители государственных органов и разработчики криптосредств работают вместе: лучшие из наработок, создаваемых на основе научно-технической базы разработчиков, внедряются в информационных системах государства. В рамках секции будут обсуждаться достижения и задачи этой сферы, а также будут намечены пути дальнейшего развития.

Ведущие:

1. **Скворцова Татьяна Владимировна,** директор департамента развития технологий цифровой идентификации**,** Минцифры
2. **Смышляев Станислав Витальевич,** д.ф.-м.н., генеральный директор, КриптоПро

1) Биометрия на транспорте: когда подписание важнее, чем найти выход на посадку

Поволоцкий Владислав Юрьевич, генеральный директор, Центр Биометрических Технологий

В докладе будет рассказано, как искали баланс между безопасностью и классным сервисом там, где цена ошибки крайне высока. Авторы поделятся муками поиска и итогами изысканий, а также планами, когда наконец на борту самолета и в вагоне поезда можно будет оказаться, не доставая паспорт (и немного про то, как биометрия уже стала обыденностью спускающихся в метро по всей стране каждый день и добирающихся на работу на автобусах). И, конечно, будет рассказано о том, как в короткий срок криптография нас незаметно спасла.

2) Развитие применения TLS с ГОСТ в отечественном сегменте Интернета

Хасин Евгений Владимирович, ВРИО директора департамента обеспечения кибербезопасности, Минцифры России

В докладе обсуждается проблематика перехода веб-сайтов на защиту с помощью протокола TLS с российскими криптоалгоритмами, отечественные сертификаты безопасности. Рассказывается о текущем состоянии работ по обеспечению поддержки на стороне сервера, а также клиентских компонентах – в браузерах и в модулях для мобильных приложений.

3) Перспективы развития технологий защиты информации в системах инфраструктуры электронного правительства

Мелузов Антон Сергеевич, заместитель генерального директора, АО "РТ Лабс"

Доклад посвящён новым механизмам защиты информации, действующим на уровне бизнес-процессов в информационных системах инфраструктуры электронного правительства. В докладе будут рассмотрены вопросы внедрения нового протокола OpenID Connect в ЕСИА, механизмы защиты мобильных приложений семейства Госуслуг и фактические результаты работы конвейера оценки влияния, новый механизм передачи документов пользователям для подписания в Госключе, нюансы «проставления» меток времени при работе с Госуслугами – в Госключе, при подписании на десктопе, при работе с МЧД.

4) Централизованные криптографические сервисы правительства Москвы: МЧД, мобильная электронная подпись и учет СКЗИ

Животворев Павел Геннадьевич, начальник отдела криптографической защиты информации, Департамент информационных технологий города Москвы

Доклад посвящен задачам, связанным с использованием средств криптографической защиты информации в масштабах мегаполиса, и опыту Москвы в их решении.

5) Обеспечение информационной безопасности в Федеральном казначействе

Бражко Вячеслав Сергеевич, начальник Управления режима секретности и безопасности информации, Федеральное казначейство

Доклад посвящен перспективным направлениям развития УЦ ФК, а также совершенствованию существующих механизмов аутентификации в ГИС Федерального казначейства: с применением криптографических средств и иных средств защиты информации, с учётом актуальных угроз информационной безопасности.

6) Биометрическая верификация и идентификация в государственных информационных системах: архитектура, технологические аспекты и межведомственное взаимодействие
Юртанов Сергей Михайлович, заместитель генерального директора АО "ФИНТЕХ"
Доклад посвящен проблематике перехода от «бумажного документа» к цифровому идентификатору личности. Будут рассмотрены вопросы сбора, хранения, обработки и обмена биометрическими данными между ведомствами, рассмотрим вопрос о том, какие изменения ждут нас завтра.

7) Встраивание СКЗИ в ГИС, просто или сложно?
Петров Алексей Владимирович, ФСБ России
В докладе рассматривается проблематика использования сертифицированных СКЗИ для защиты информационных систем. Будут рассказаны основные моменты, на которые стоит обращать внимание при создании защищенных информационных систем, в том числе государственных.

ЗАЛ «ЕЛОВЫЙ»

12:30 – 14:00

Секция «Аппаратная безопасность»

Научно-практическая секция на стыке аппаратного и программного обеспечения. Технологии анализа, реверсинга, механизмы атак на аппаратные решения. Практическая защищенность умных бытовых устройств, систем телеметрии, массовых микроконтроллеров и новые векторы атак на информационные системы.

Ведущий:

1. **Усанов Алексей Евгеньевич**, руководитель направления исследований безопасности аппаратных решений "Positive Labs", Positive Technologies

1) Выявление угроз и проектирование безопасной архитектуры сети на кристалле
Загартдинов Булат Назимович, руководитель отдела исследований, ООО «НТЦ «Вулкан», аспират НИУ «МЭИ»
Основные принципы построения сетей на кристалле, особенности реализации на примере протокола ARM Coherent Hub Interface (CHI). Типичные угрозы безопасности в таких системах – от атак по сторонним каналам до атак отказа в обслуживании на маршрутизаторы и манипуляции трафиком. Механизмы безопасности сети на кристалле для защиты от этих угроз: виртуальные каналы с управлением потоком на основе скользящего окна, проверка целостности пакетов и настраиваемые политики доступа.

2) Методология и проблематика fault injection атак: разбор на реальных примерах
Васин Юрий Олегович, руководитель группы направления исследований безопасности аппаратных решений "Positive Labs", Positive Technologies
Доклад посвящён методам и практическим аспектам проведения атак типа fault injection — преднамеренного внесения сбоев в работу аппаратных или программных систем с целью нарушения их нормального функционирования и обхода механизмов защиты. В ходе выступления будет рассмотрена методология проведения таких атак: от выбора цели и подготовки среды до анализа полученных результатов. В качестве практической основы будет выбрана одна серия микросхем, на примере которой будет показано, как одни и те же устройства могут быть атакованы различными способами fault injection.

3) Обзор аппаратных средств построения доверенной среды в системах на кристалле (СнК)
Колотников Алексей Владимирович, независимый исследователь
Доверие между компонентами СнК строится на базе изоляции между доверенной и общей (богатой по разнообразию приложений) средой. Такая изоляция может быть: физической, временной, логической, криптографической. Рассказ о каждом из способов с конкретными примерами.

4) **Обеспечение доверенной среды обновления микропрограммы в условиях дефицита аппаратных ресурсов**
Овтин Дмитрий Александрович, инженер-программист, Компания «Актив»
Реализация доверенной среды обновления программного обеспечения программно-аппаратных средств защиты информации в условиях дефицита ресурсов. Методология поэтапной загрузки кода, использование запатентованного механизма разделения микропрограммы на две функциональные части для защищенного обновления на устройствах с критически малым объемом FLASH-памяти, обеспечение гарантированной работоспособности даже при возникновении внештатных ситуаций в процессе записи.

5) **Корни доверия: Основные требования. Особенности реализации**

Самоделов Андрей Сергеевич, независимый эксперт

В докладе сделан обзор требований к корням доверия (КД) со стороны различных зарубежных регуляторов: GP, PSA, SESIP, а также требования к жизненному циклу и инфраструктуре КД. Кроме того, рассмотрены примеры различных вариантов архитектуры и аппаратной реализации КД. В конце презентации приведен список отечественных нормативных документов, непосредственно касающихся КД.

КИНО-КОНЦЕРТНЫЙ ЗАЛ

12:30 – 14:00

Круглый стол "Олимпиады и научные школы"

Круглый стол, посвященный широкому спектру вопросов, связанных с олимпиадным движением и научными школами в области информационной безопасности и криптографии. Вовлечение студентов и старших школьников. Роль и место научного сообщества и вузов, объединение усилий игроков рынка информационной безопасности, сферы образования и науки.

Ведущие:

1) **Токарева Наталья Николаевна**, к.ф.-м.н., доцент кафедры теоретической кибернетики ММФ Новосибирского государственного университета, руководитель Криптографического центра (Новосибирск);
2) **Пудовкина Марина Александровна,** д.ф.-м.н., профессор кафедры криптографии и безопасности компьютерных систем НИЯУ МИФИ, директор ассоциации РусКрипто.

Участники:

3) **Правиков Дмитрий Игоревич,** к.т.н., заведующий кафедрой комплексной безопасности критически важных объектов, РГУ нефти и газа (НИУ) имени И.М. Губкина
4) **Пичкур Андрей Борисович,** к.ф-м.н., директор образовательных программ, ОАО "Гарда Технологии"
5) **Кяжин Сергей Николаевич,** к.ф.-м.н., доцент, НИЯУ МИФИ
6) **Катышев Сергей Юрьевич,** к.ф.-м.н., ФУМО по ИБ
7) **Панасенко Сергей Петрович,** к.т.н., директор по научной работе, Компания «Актив»
8) **Селиванова Анна Юрьевна,** заместитель директора по связям с общественностью, ИКНК СПбПУ
9) **Коренева Алиса Михайловна,** к.ф.-м.н., заместитель руководителя службы сертификации по научно-техническому сотрудничеству, Код Безопасности

ЗАЛ «ШИШКА»

15:00 – 16:30

Секция «РБПО и подпись ПО, построение единого пространства доверия к российскому программному обеспечению»

Секция посвящена применению криптографических средств и решений для обеспечения целостности и аутентичности программного обеспечения на этапах его жизненного цикла: формирование требований, проектирование, разработка, производство и эксплуатация с учетом современных подходов к разработке безопасного ПО и требований регуляторов, включая вопросы регламентирования процедур подписи и ее проверки, требования к ключам и сертификатам, используемым в этих процедурах. Участники секции обсудят этапы построения единого пространства доверия к российскому программному обеспечению, вопросы нормативного регулирования, стандартизации, роли регуляторов, государственных и коммерческих организаций на каждом из этапов.

Ведущие:

1) **Гусев Дмитрий Михайлович,** к.т.н., первый заместитель генерального директора, ИнфоТеКС
2) **Качалин Игорь Федорович,** генеральный директор, АНО «Национальный технологический центр цифровой криптографии»
3) **Смышляев Станислав Витальевич,** д.ф.-м.н., генеральный директор, КриптоПро

1. **Подпись ПО и Единое пространство доверия. От идеи к реализации**

Качалин Игорь Федорович, генеральный директор, АНО «Национальный технологический центр цифровой криптографии»

2. **Проект регламента подписи дистрибутивов российского ПО**

Калугина Анастасия Валентиновна , руководитель направления безопасной разработки и инфраструктуры, ИнфоТеКС,
Петров Александр Олегович, ведущий инженер-аналитик отдела криптографических разработок, КриптоПро
Копылов Денис Викторович, руководитель направления прикладной криптографии, Код Безопасности

Участники дискуссии:

4) **Аносов Сергей Игоревич,** начальник отдела, Открытая мобильная платформа
5) **Соснин Юрий Владимирович,** заместитель генерального директора, Группа Астра
6) **Мелузов Антон Сергеевич,** заместитель генерального директора, РТ Лабс

ЗАЛ «ЕЛОВЫЙ»

15:00 – 16:30

Секция «Проекты, технологии и решения»

Секция, посвященная новым российским разработкам в области криптографии и информационной безопасности. Презентации решений, технологий и перспективных продуктов. Обмен мнениями, диалог производителей средств информационной безопасности и заказчиков.

Ведущие:

1. **Поташников Александр Викторович,** к.ф.-м.н., заместитель директора центра разработки, ИнфоТеКС

1) **Развитие интерфейсов встраиваемых криптографических библиотек для решения прикладных задач**

Эм Арина Николаевна, ведущий менеджер продуктов, ИнфоТеКС
В современном мире встраиваемые библиотеки стали неотъемлемой частью практически любого проекта. С ростом востребованности встраиваемой криптографии в сценариях современного бизнеса перед нами встает вопрос об использовании новых интерфейсов для обеспечения удобства работы с библиотеками, а также использовании и реализации актуальных технологий и форматов. В докладе расскажем о решениях на базе продукта ViPNet OSSL. К ним относятся криптобиблиотека для встраивания решений на Java и GO, модуль для работы с подписью XML, модули для шифрования баз данных.

2) **Особенности взаимодействия аппаратного модуля безопасности HSM, выполняющего криптографические функции аутентификации и идентификации абонентов, с оборудованием ядра сети ПРТС пятого поколения**

Емельянов-Гирс Виктор Михайлович, к.ф.-м.н., заместитель генерального директора по науке, ООО "Системы практической безопасности"

Рассмотрены проблемные вопросы взаимодействия оборудования ядра сети 5G с HSM для реализации схемы ECIES и протокола 5G-AKA. Представлены предложения по совмещению HSM, выполняющего криптографические функции аутентификации и идентификации абонентов, с HSM-SIDF, выполняющим криптографические функции расшифрования значения SUPI из SUCI, в едином устройстве.

3) **Сравнение эксплуатационных характеристик протоколов безопасности сетевого уровня IPsec и Wireguard в некоторых сценариях**

Васин Антон Романович, к.ф.-м.н старший аналитик-криптограф, Компания «Актив»

В работе представлено сравнительное исследование производительности и эффективности протоколов защиты сетевого уровня IPsec и WireGuard. Анализ проводился для реализаций в пространстве ядра Linux, а также для встраиваемой ОС реального времени. Методология тестирования включала измерение пропускной способности, загрузки CPU, потребления памяти, RTT, времени установки соединения в различных сетевых топологиях, при варьировании сетевых условий и конфигурации протоколов.

4) **Выстраивание системы учета СКЗИ в организации с нуля**

Дронов Дмитрий Витальевич, владелец продукта, ООО "Клируэй Текнолоджис"

Доклад посвящен автоматизации учета СКЗИ в рамках ответственности ОКЗ: рассматриваются технические сложности и риски, способы исключения человеческого фактора, пример комплексной автоматизации, преимущества удаленного доступа к АРМ пользователей и инструменты контроля жизненного цикла СКЗИ для обеспечения законодательного соответствия.

5) **Использование шлюза удаленного доступа и VPN для решения практических задач в проектах федерального масштаба**

Никитков Александр Александрович, руководитель группы развития отдела защиты сетей, КриптоПро

Реализация крупных инфраструктурных проектов требует комплексного подхода к подбору компонентов информационных систем, в том числе обеспечивающих защиту информации, которой обмениваются как компоненты самой системы, так и её пользователи. Во множестве информационных систем федерального масштаба задача организации такого защищённого взаимодействия успешно решается посредством использования шлюзов удалённого доступа и VPN. В докладе будут продемонстрированы примеры применения шлюза в различных сценариях, которыми множество граждан нашей страны уже пользуются на ежедневной основе.

ЗАЛ «СОСНОВЫЙ»

15:00 – 16:30

Секция «Интеллектуальные методы анализа безопасности программных и аппаратных систем»

Секция, сформированная экспертами Высшей школы кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, посвященная методам анализа безопасности информационных систем.

Ведущий:

1 **Павленко Евгений Юрьевич,** д.т.н., профессор, директор Высшей школы кибербезопасности Санкт-Петербургского политехнического университета Петра Великого

1) Поиск недокументированных инструкций в формальном описании сверхбольших интегральных схем

Пагуба Григорий Юрьевич, СПбПУ

В докладе представлен метод анализа формального описания аппаратного обеспечения на основе аппроксимации состояний его модулей. Представляемый метод позволяет определять множество возможных состояний механизма декодирования инструкций сверхбольших интегральных схем и определять их функциональные возможности.

2) Профилирование механизмов внешнего взаимодействия встраиваемого программного обеспечения

Кондачков Егор Дмитриевич, СПбПУ
В докладе рассмотрен метод определения механизмов внешнего взаимодействия встраиваемого программного обеспечения на основе интеллектуального анализа его программного кода и составления теоретико-множественной модели его функционирования. Рассматриваемый метод позволяет определять перечень протоколов взаимодействия (UART, I2C, SPI и т.д.), используемых анализируемым экземпляром встраиваемого ПО и их конфигурационные характеристики (например, baudrate для UART).

3) **Автоматизированный анализ безопасности программного обеспечения для операционной системы ANDROID**

Аношкин Илья Андреевич, СПбПУ
В эпоху стремительной цифровизации мобильные приложения превратились в ключевой интерфейс взаимодействия между бизнесом, государством и обществом. Ежедневно через смартфоны и планшеты осуществляются финансовые транзакции, обрабатываются персональные данные, ведется деловая переписка и управляются критически важные процессы. Однако высокая скорость разработки и выхода продуктов на рынок, конкуренция за внимание пользователя и ориентация на удобство использования становятся более приоритетными, чем обеспечение безопасности пользователей. Согласно статистике, 75% приложений из Google Play содержат хотя бы одну уязвимость высокого уровня критичности. Таким образом, систематический поиск и анализ уязвимостей в мобильных приложениях перестает быть узкоспециальной задачей — это актуальная необходимость для обеспечения цифрового суверенитета, доверия пользователей и устойчивости бизнеса в современном мире.

4) **Выявление honeypot-систем на основе комплексного анализа показателей функционирования узлов.**

Пономарев Данила Андреевич, СПбПУ
В докладе исследованы принципы построения и функционирования honeypot-систем. Проведен сравнительный анализ существующих методов обнаружения с выявлением их преимуществ и ограничений. Предложен метод обнаружения, основанный на анализе задержек исполнения команд. Разработан универсальный метод, предусматривающий агрегирование результатов различных методов обнаружения. Реализован программный прототип системы обнаружения и проведена оценка его эффективности

5) **Название: Статический и динамический анализ прошивок умных голосовых помощников с GNN - представлениями**

Болокан Амвросий Валерьевич, СПбПУ
С широким распространением умных голосовых помощников их прошивки становятся критической частью атакуемой поверхности: уязвимости на уровне прошивки позволяют получить длительный доступ к аудиопотокам, конфиденциальным данным и управлению устройством. Традиционные методы анализа, ориентированные только на статическую или только на динамическую информацию, часто недостаточно эффективны против современных техник обфускации и целенаправленных бэкдоров. Необходим интегрированный подход, который учитывает как структурные свойства кода, так и поведение прошивки при исполнении, для повышения точности обнаружения угроз и локализации вредоносных фрагментов. Таким образом, предлагаемый метод актуализирует такой подход к анализу безопасности прошивок умных голосовых устройств.

6) **Метод динамического бинарного морфинга исполняемого кода на уровне загрузчика исполняемых файлов**

Гололобов Никита Вячеславович, СПбПУ
Предложен метод динамического бинарного морфинга исполняемого кода на уровне загрузчика исполняемых файлов, который направлен на обеспечение защищенности исполняемых файлов от атак, связанных с эксплуатацией уязвимостей. Основным принципом является создание уровня абстракции над исполняемым кодом, который обеспечивает обратное преобразование исполняемого кода на уровне последовательности инструкций. Сценарий работы метода предполагает последовательность из загрузки, инструментации и морфинга кода. Использование морфинга на уровне загрузчика обеспечивать итеративный морфинг при каждом новом вызове функции. В результате динамического бинарного морфинга структура исполняемого кода и адреса вызова функциональных объектов изменяются. При этом метод обеспечивает сохранение семантики исполняемого кода исходному тексту программы.

КИНО-КОНЦЕРТНЫЙ ЗАЛ

17:00 – 19:00

Дискуссионная панель «ЭДО в России»

Ведущие:

1) **Малинин Юрий Витальевич,** президент ассоциации РОСЭУ, директор ассоциации РусКрипто
2) **Кирюшкин Сергей Анатольевич,** советник генерального директора, начальник УЦ, Газинформсервис, эксперт Ассоциации «РОСЭУ»

Участники дискуссии:

3) **Новиков Фёдор Вадимович,** начальник управления электронного документооборота, ФНС России
4) **Смирнов Павел Владимирович,** к.т.н., директор по развитию, КриптоПро, эксперт Ассоциации «РОСЭУ»
5) **Лабуцкая Анастасия Сергеевна,** советник генерального директора СКБ Контур, эксперт Ассоциации РОСЭУ

ЗАЛ «ЕЛОВЫЙ»

17:00 – 19:00

Секция «Криптография и криптоанализ» Часть №1

Классическая секция конференции, посвященная научным и практическим вопросам криптографии и криптоанализа.

Ведущие:

1) **Матюхин Дмитрий Викторович,** к.ф.-м.н., ФСБ России
2) **Алексеев Евгений Константинович,** к.ф.-м.н., КриптоПро, АНО «НТЦ ЦК»
3) **Поташников Александр Викторович,** к.ф.-м.н., ИнфоТеКС

1. **Оптимизация ресурсоемкости алгоритма «Гиперикум» при реализации в устройствах с ограниченными ресурсами за счет кеширования фрагментов подписи на управляющем устройстве**

Панасенко Сергей Петрович, к.т.н., директор по научной работе, Компания «Актив»
Турченко Олег, к.т.н., криптограф-исследователь, ООО «КуАпп»
В докладе рассматривается возможность использования постквантового алгоритма цифровой подписи «Гиперикум» в низкоресурсных устройствах за счет кеширования частей подписи на управляющем устройстве. Описан пример протокола вычисления ЦП при организации такого кеширования; приведены зависимости снижения ресурсоемкости операции вычисления ЦП от размера кеша для ряда параметров алгоритма «Гиперикум».

2. **Отличительные особенности отечественного постквантового механизма инкапсуляции ключа «Земляника» на основе задачи M-LWE**

Зеленецкий Алексей Сергеевич, старший криптограф-исследователь, ООО «КуАпп», МГТУ им. Н.Э. Баумана
Задача Learning With Errors (LWE) и её различные модификации относятся к числу наиболее известных вычислительно сложных задач в криптографии на решетках. На их основе к настоящему времени предложено множество постквантовых механизмов инкапсуляции ключа (МИК) — криптосистем, предназначенных для формирования общего секретного ключа по открытому каналу в условиях уязвимости протокола Диффи—Хеллмана к атакам с использованием квантового компьютера. Представленный на конференции «РусКрипто 2025» отечественный механизм инкапсуляции ключа «Земляника», основанный на задаче M-LWE, также относится к данному семейству криптосистем. Настоящая работа посвящена сравнению «Земляники» с другими представителями упомянутого семейства и ставит своей целью, в первую очередь, подчеркнуть отличительные особенности разработанного механизма. Кроме того, во время доклада будут представлены эксплуатационные характеристики «Земляники», а также будет доложено о текущем статусе процесса ее стандартизации в рамках РГ ПККМ ТК26.

3. **От решёток Барнса–Уолла к стандарту: текущий статус разработки постквантовой схемы «Облепиха»**

Кунинец Артём Андреевич, криптограф-исследователь, ООО «КуАпп»
Леевик Антон Георгиевич, криптограф-исследователь, ООО «КуАпп»
Малыгина Екатерина Сергеевна, к.ф.-м.н., старший криптограф-исследователь, ООО «КуАпп»
Мельничук Евгений Михайлович, криптограф-исследователь, ООО «КуАпп»

В работе описывается статус работ по разработке схемы цифровой подписи «Облепиха». Представлены основные алгоритмы, используемые в схеме, и приведена оценка ее криптографической стойкости.

4. «Спартиум» – постквантовая схема подписи с хранением состояния

Кирюхин Виталий Александрович, главный специалист, ООО «СФБ Лаб»

Анонсируется постквантовый алгоритм подписи «Спартиум», основанный на хэш-функции «Стрибог» и её функции сжатия. Рассматриваются принципы синтеза алгоритма, отличия от существующих аналогов, его достоинства и ограничения. Приводятся первичные результаты доказательного и конструктивного криптографического анализа.

5. Обзор алгоритмов, построенных на основе коммутативных изогений суперсингулярных эллиптических кривых

Полякова Полина Алексеевна, младший аналитик отдела криптографического анализа, Код Безопасности, НИЯУ МИФИ

Поляков Михаил Вадимович, заместитель начальника отдела криптографического анализа, Код Безопасности, НИЯУ МИФИ

Коренева Алиса Михайловна, к.ф.-м.н., заместитель руководителя службы сертификации по научно-техническому сотрудничеству, Код Безопасности

В 2022 году была опубликована достаточно эффективная атака на протокол SIDH, построенный на некоммутативных изогениях суперсингулярных эллиптических кривых. В результате почти все исследования в этой области были приостановлены. В рамках доклада будет проведен обзор криптографических алгоритмов на основе коммутативных изогений суперсингулярных эллиптических кривых, которые не обладают уязвимостями своих предшественников и при этом являются более удобными с точки зрения плавного перехода на постквантовые механизмы подписи и согласования ключа.

6. PQ/T-гибридные схемы цифровой подписи как этап миграции к постквантовой криптографии

Качмазов Руслан Александрович, старший инженер по информационной безопасности, Яндекс Облако, НИУ ВШЭ

В докладе рассматриваются PQ/T-гибридные схемы цифровой подписи как один из наиболее реалистичных сценариев миграции к постквантовой криптографии. Предлагается классификация таких схем, рассматриваются вопросы их безопасности, совместимости и интеграции в PKI. Отдельное внимание уделяется практическим рискам гибридизации, включая трудности формального обоснования безопасности и возможные атаки, возникающие при некорректном встраивании гибридных подписей в существующую инфраструктуру.

ЗАЛ «СОСНОВЫЙ»

17:00 – 19:00

Секция «Криптография в медицине»

Цифровые технологии в здравоохранении позволяют выйти на новый уровень оказания медицинской помощи, предоставляя врачам возможность больше уделять внимания пациентам и делая их клиентский путь более удобным и комфортным. При этом при построении информационных систем необходимо не забывать о защите врачебной тайны, сохранении целостности хранимых и передаваемых данных, а также других задачах информационной безопасности. Об этих вопросах, а также о законодательных нормах, их регулирующих, мы и поговорим на данной секции.

Ведущие:

1) **Мелкумян Наталья,** директор по клиентскому сервису, КриптоПро
2) **Нуриахметов Дмитрий,** группа компаний «Мать и дитя»

1. Особенности использования средств криптографической защиты информации в негосударственных медицинских организациях

Нуриахметов Дмитрий, группа компаний «Мать и дитя»

Доклад посвящен применению криптографических средств защиты информации в частном здравоохранении. Анализируются правовые риски, связанные с утечкой медицинских данных, и роль СКЗИ в их минимизации. Рассматриваются практические кейсы использования электронной подписи и шифрования в деятельности

негосударственных медицинских организаций, а также сформулированы основные требования к выбору СКЗИ для частной клиники.

2. **Особенности использования средств криптографической защиты информации в единой государственной информационной системе в сфере здравоохранения**

Алексей Валерьевич Пилюков, руководитель, Отраслевой центр информационной безопасности и импортозамещения Министерства здравоохранения

Доклад посвящен применению криптографических средств защиты информации в единой государственной информационной системе в сфере здравоохранения (далее - ЕГИСЗ). Рассматриваются особенности подключения, основные требования при подключении с использованием СКЗИ к ЕГИСЗ.

3. **Электронная подпись в медицине. Сервисы для оптимизации работы клиники**

Голубов Максим Иванович, Удостоверяющий центр ЭТП ГПБ Консалтинг

В докладе рассматриваются практические вопросы внедрения электронной подписи в медицинских организациях в условиях перехода отрасли на электронный документооборот. Будут рассмотрены типовые барьеры внедрения, а также представлен архитектурный подход к их преодолению на базе сервисов удостоверяющего центра, включая интеграцию посредством API-модулей и использование мобильной электронной подписи.

4. **Применение криптографии для защиты медтех-приложений**

Дмитрий Тараненко, директор по кибербезопасности, СберЗдоровье

Цель этого доклада — показать, как выстроить криптографическую защиту медтех-приложений: защищённые каналы связи, юридически значимая подпись электронных медицинских документов, защита врачебной тайны при хранении, а также контроль целостности и состава ПО (OSS, SBOM, provenance) в условиях критичности отрасли и потенциальной применимости требований по КИИ**.**

5. **Конфиденциальная обработка медицинских и генетических данных: возможности и ограничения современной криптографии**

Кяжин Сергей Николаевич, к.ф.-м.н., НИЯУ МИФИ, АНО «НТЦ ЦК»
Емельянов Петр Николаевич, АНО «НТЦ ЦК», Блумтех
Митрофанов Александр Александрович, АНО «НТЦ ЦК», Блумтех
Никифорова Лидия Олеговна, АНО «НТЦ ЦК», КриптоПро

Одной из прикладных исследовательских задач в медицине является оценка влияния генотипических признаков на фенотипические. Генетические лаборатории накапливают существенный объем генетических данных. Медицинские центры хранят огромное количество фенотипических данных. Объединение данных лабораторий и медицинских учреждений может значительно повысить качество медицинских исследований в соответствующей области. Но эти данные относятся к персональным и к врачебной тайне. Современные достижения криптографии могут позволить рассмотреть возможность решения подобной задачи с помощью протоколов конфиденциальных вычислений, которые используются для обработки конфиденциальных данных без их разглашения. В докладе мы поговорим об этой задаче на языке конфиденциальных вычислений, о криптографических протоколах, которые потенциально можно использовать для ее задачи и ограничениях им присущих.

---

26 МАРТА

ЗАЛ «ШИШКА»

10:00 –11:30

Секция «Криптографические средства защиты информации: разработка, сертификация, внедрение и эксплуатация»

Вопросы создания, сертификации, внедрения в информационные системы и эксплуатации российских криптографических решений. Диалог представителей регулятора с разработчиками криптографических продуктов, экспертным сообществом и заказчиками информационных систем, в которых применяются СКЗИ.

Ведущий:

1. **Петров Алексей Владимирович,** ФСБ России

1) **Применение задачи удовлетворения ограничений для автоматического анализа интерфейсов СКЗИ**
Тырнов Филипп Александрович, инженер-аналитик, КриптоПро, МГТУ им. Баумана
Доклад посвящен методу анализа безопасности криптографических интерфейсов с использованием инструментов, предназначенных для решения общей задачи удовлетворения ограничений, при встраивании СКЗИ в информационные системы.

2) **Особенности инструментальной и технологической поддержки фаззинг-тестирования функций криптографических библиотек с применением адаптивных биоинспирированных оптимизаций**
Гришин Максим Александрович, НИЯУ МИФИ
В работе предлагается метод повышения результативности фаззинга криптографических библиотек, основанный на семантически ориентированном применении операторов мутации к отдельным типам входных параметров в сочетании с биоинспирированными алгоритмами адаптивного выбора мутаций. Разработанная схема апробирована на ряде криптографических библиотек. Экспериментальные результаты показывают увеличение консолидированного покрытия кода и выявление ранее не обнаруженных уникальных ошибок в реализациях.

3) **Разработка и сертификация инфраструктуры отечественных сим-карт**
Агеенко Геннадий Максимович, ФСБ России

4) **Подходы к обеспечению надёжного хранения криптографических ключей**
Тыщенко Никита Сергеевич, ФСБ России

5) **Некоторые вопросы разработки и сертификации средств криптографической защиты информации**
Петров Алексей Владимирович, ФСБ России

ЗАЛ «ЕЛОВЫЙ»

10:00 –11:30

Секция «Криптография и криптоанализ» Часть №2

Классическая секция конференции, посвященная научным и практическим вопросам криптографии и криптоанализа.

Ведущие:

1. **Матюхин Дмитрий Викторович,** к.ф.-м.н., ФСБ России
2. **Алексеев Евгений Константинович,** к.ф.-м.н., КриптоПро, АНО «НТЦ ЦК»
3. **Поташников Александр Викторович,** к.ф.-м.н., ИнфоТеКС

1) **Об одной атаке на протокол IKEv2**
Смыслов Валерий Анатольевич, ЭЛВИС-ПЛЮС
Доклад описывает атаку на протокол IKEv2 (Internet Key Exchange protocol Version 2, протокол обмена ключами в IPsec), дающую возможность атакующему понизить стойкость создаваемого защищенного соединения и произвести перехват защищаемого трафика. Возможность проведения подобной атаки в общих чертах была описана в 2016 г., однако, ввиду нереально высоких требований к возможностям атакующего, эта

атака носила чисто теоретический характер. В 2025 г. атака была обобщена на случай использования атакующим квантового компьютера. В докладе описывается несколько вариантов атаки 2025 г. (с использованием квантового компьютера). В докладе также описываются изменения в протоколе IKEv2, предложенные автором доклада и одобренные экспертами IETF, которые делают все эти атаки (включая оригинальную атаку 2016 г.) невозможными.

2) **Конфиденциальное сложение данных: определение объекта и предмета исследования**

Никифорова Лидия Олеговна, ведущий инженер-аналитик, КриптоПро
Ахметзянова Лилия Руслановна, к.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро
Быстревский Сергей Андреевич, инженер-аналитик, КриптоПро
Мухортова Алёна Андреевна, инженер-аналитик, КриптоПро

Данный доклад посвящён схемам конфиденциального сложения данных (Private Stream Aggregation, PSA). В рамках доклада будут выделены классы схем в зависимости от интерфейса и обеспечиваемых свойств безопасности. Для выделенных классов будет представлена систематизация моделей угроз и нарушителя.

3) **Анализ применимости атак на протоколы аутентифицированной выработки ключа, основанные на механизме инкапсуляции ключа, к протоколу pqRTLS12**

Алексеев Евгений Константинович, к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро, АНО «НТЦ ЦК»
Кяжин Сергей Николаевич, к.ф.-м.н., доцент, НИЯУ МИФИ
Мухортова Алена Андреевна, инженер-аналитик, КриптоПро

В настоящей работе описываются результаты аналитического обзора атак на протоколы аутентифицированной выработки общего ключа с использованием механизма инкапсуляции ключа. Существующие атаки классифицированы по угрозам, а также требуемых для их реализации возможностям нарушителя. Также в работе приводятся результаты анализа применимости этих атак к текущей версии проекта документа протокола TLS 1.2 на основе механизма инкапсуляции ключа. Предложена модификация протокола, направленная на защиту от исследуемых атак.

4) **Протокол доставки ключей «БУРУНДУК»**

Кирюхин Виталий Александрович, главный специалист, ООО «СФБ Лаб»

Предлагается протокол «БУРУНДУК», предназначенный для смены общего секретного ключа в случае компрометации произвольного числа участников. Каждый пользователь получает исходно общий ключ и (небольшой) индивидуальный неизменяемый набор ключей. Новый общий ключ (ключи) все нескомпрометированные пользователи могут получить через широковещательный односторонний канал связи без интерактивного взаимодействия. Нагрузка на канал связи линейно зависит от числа скомпрометированных (групп) пользователей и не зависит от их общего числа. Протокол включает алгоритмы управления статусами участников, предусмотрены различные способы группировки пользователей и два возможных механизма аутентификации общего ключа. Для реализации протокола достаточно стойкого блочного шифра (к примеру, ГОСТ 34.12-2018 «Магма»).

5) **Протокол анонимного подтверждения наличия элемента в рассматриваемом множестве**

Хуцаева Алтана Феликсовна, ИТМО, ГУАП
Беззатеев Сергей Валентинович, д.т.н., профессор, ИТМО, ГУАП

Рассматривается модель анонимного подтверждения наличия элемента $m \in M$ в некотором подмножестве B, где множество M известно всем участникам. Для данной модели предлагается использовать протокол, использующий функцию $F: M \to M^n$ и забывчивую подпись 1-из-n сообщений. В модели сторона А проверяет принадлежность произвольного элемента конечному подмножеству элементов стороны Б, не раскрывая проверяемый элемент. В результате у стороны А имеется подпись, подтверждающая факт принадлежности запрошенного элемента некоторому подмножеству множества элементов стороны Б. Данная модель находит свое применение в задачах приватных проверок членства в множествах.

ЗАЛ «СОСНОВЫЙ»

10:00 –11:30

Секция «Криптографические решения для киберфизических систем»

Секция посвященная широкому кругу вопросов информационной безопасности киберфизических систем, роли и месту в них криптографии, расширению использования криптографических решений в существующих и создаваемых проектах.

Ведущая:

1. **Сорокина Марина Викторовна,** руководитель направления отдела развития продуктов, ИнфоТеКС
2. **Лазарев Алексей Станиславович**, руководитель департамента защиты киберфизических систем, Компания "Актив"

1) **Криптодирижёр: Об особенностях построения систем управления гетерогенными СКЗИ в промышленных системах и IIoT**

Сорокина Марина Викторовна, руководитель направления, ИнфоТеКС

Опыт компании ИнфоТеКС по созданию системы управления встраиваемыми продуктами линейки ViPNet SIES и превращению закрытого проприетарного решения в открытую платформу для гетерогентных СКЗИ. Мы обсудим почему так важно обеспечение наблюдаемости и прозрачности в управлении любыми средствами информационной безопасности в промышленных системах и IIoT и покажем, как мы прошли путь из философии с «собственное и закрытое» до «открытое с использованием стандартизованнанных механимов». Такие подходы позволяют превратить разрозненные устройства с криптомодулями и крипточипами от разных производителей в стройный наблюдаемый оркестр, где у каждого устройства есть своя партия, а у эксплуатации – не просто дирижерская палочка, а целый дирижёрский пульт.

2) **Обзор проблематики обеспечения безопасности киберфизических систем. От потребностей к требованиям, технологиям и нормативно-технической документации.**

Карантаев Владимир Геннадьевич, доцент, МГТУ имени Н.Э. Баумана.

Лазарев Алексей Станиславович, руководитель департамента защиты киберфизических систем, Компания "Актив"

Доклад посвящен связи нормативно-технических требований к безопасности киберфизических систем и тех технологических решений, которые используются или должны использоваться в промышленности. Отдельный акцент делается на роли доверенных компонентов безопасности (ДКБ) как базовых элементов инфраструктурного механизма контроля целостности и аутентичности устройств киберфизических систем, а также на типовых сценариях использования ДКБ. Будет показано, что формируемые требования к безопасной архитектуре задают направление для выбора подходов к внедрению механизмов доверия «от микросхемы до системы», и как криптографические механизмы помогают в реализации этих подходов. Также будут рассмотрены возможности смещения затрат на безопасность «влево» по жизненному циклу — от поздних доработок к изначальному проектированию архитектуры и элементной базы целевых систем.

3) **Векторное расширение системы команд RISC-V для ускорения алгоритмов ГОСТ-криптографии**

Матюков Андрей Викторович, руководитель рабочей группы, Альянс RISC-V

Высоконагруженные киберфизические системы накладывают достаточно жесткие требования к производительности и энергоэффективности реализаций криптографических алгоритмов. Но реализации отечественных алгоритмов на базе инструкций CPU общего назначения часто не могут похвастать высокой производительностью, сравнимой с производительностью зарубежных алгоритмов, для которых существует специализированная ISA. В данной работе показан подход к решению данной задачи на базе архитектуры RISC-V, и демонстрируется новое векторное расширение набора инструкций, позволяющее эффективно реализовывать основные преобразования отечественных криптографических алгоритмов.

4) **Возможности и практическое применение доверенного компонента безопасности.**

Чукарев Максим Владимирович, ведущий инженер, Компания "Актив"

Доклад посвящен аспектам практического применения универсального доверенного компонента безопасности Рутокен в целевых системах. Рассматриваются ключевые характеристики устройства, его криптографические возможности, совместимость с решениями партнеров за счет реализации утвержденных в Российской Федерации стандартов и широкого набора аппаратных и программных интерфейсов взаимодействия.

ЗАЛ «ШИШКА»

12:00 –14:00

Секция «Информационная безопасность и криптография кредитно-финансовой сферы»

На секции будут представлены доклады, раскрывающие тематику использования криптографических решений в финансовых сервисах, а также новое в регулировании информационной безопасности в кредитно-финансовой сфере.

Ведущие:
1) Елистратов Андрей Алексеевич, к.ф.-м.н., Банк России
2) Горелов Дмитрий Львович, управляющий партнер, Компания «Актив», директор Ассоциации «РусКрипто»

1. **Требования к техническим средствам и программному обеспечению, реализующим криптографические механизмы информационной инфраструктуры значимой платежной системы, используемых при осуществлении переводов денежных средств по карточным счетам**

Зинюк Борис Федорович, Академия криптографии Российской Федерации

2. **Дорожная карта мероприятий по переходу ПС "Мир" на новые криптографические алгоритмы**

Бобров Сергей Валерьевич, начальник управления сопровождения технологических проектов, АО «НСПК»

3. **Контактные и бесконтактные платежи: криптография под капотом**

Ахметзянова Лилия Руслановна, к.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро
Бабуева Александра Алексеевна, ведущий инженер-аналитик, КриптоПро
Никифорова Лидия Олеговна, ведущий инженер-аналитик, КриптоПро
Никонов Николай Владимирович, к.ф.-м.н., в.н.с. лаборатории НКО «Фонд содействия развитию безопасных информационных технологий»

4. **Модуль безопасности российского банкомата**

Евтушенко Владимир Олегович, управляющий партнер, АО «СмартКард-Сервис»

5. **Новеллы Банка России в регулировании финансовых биометрических сервисов и возможности их интеграции**

Литвинов Игорь Олегович, главный инженер, управление методологии и стандартизации информационной безопасности Департамента информационной безопасности, Банк России

6. **Задачи, решаемые Банком России в рамках использования СКЗИ в проекте цифровой рубль**

Кривоногов Антон Алексеевич, консультант, управление методологии и стандартизации информационной безопасности Департамента информационной безопасности, Банк России

7. **Концепция конфиденциального обмена данными на основе модифицированных фильтров Блума для противодействия мошенническим схемам**

Шевченко Вячеслав Андреевич, МИЭМ НИУ ВШЭ
Алмазбек уулу Тимур, МИЭМ НИУ ВШЭ
Сергеев Антон Валерьевич, МИЭМ НИУ ВШЭ
Стародубов Константин Владимирович, МИЭМ НИУ ВШЭ

8. **Постквантовая криптография и квантовое распределение ключей: защита финансовой индустрии от квантовой угрозы**

Голованов Владимир Борисович, отв. секретарь ПК1 ТК122, заместитель начальника аналитического отдела, ИнфоТеКС

ЗАЛ «ЕЛОВЫЙ»

12:00 –14:00

Секция «Криптография и криптоанализ» Часть №3

Классическая секция конференции, посвященная научным и практическим вопросам криптографии и криптоанализа.

Ведущие:

1) **Матюхин Дмитрий Викторович,** к.ф.-м.н., ФСБ России
2) **Алексеев Евгений Константинович,** к.ф.-м.н., КриптоПро, АНО «НТЦ ЦК»
3) **Поташников Александр Викторович,** к.ф.-м.н., ИнфоТеКС

1. **Схема подписи ГОСТ в условиях мультипликативно связанных ключей: о стойкости в модели UF-CM-sKRKA**

Бабуева Александра Алексеевна, ведущий инженер-аналитик, КриптоПро
Кяжин Сергей Николаевич, к.ф.-м.н., доцент, НИЯУ МИФИ
Махонин Илья Владимирович, инженер-аналитик, КриптоПро
Доклад посвящен адаптации результатов анализа схемы подписи ГОСТ в новой модели Mult-Hash, представленных Бахаревым А.О. и Царегородцевым К.Д. на РусКрипто 2025, к наиболее близкой среди часто используемых моделей для оценки схем подписи в условиях связанных ключей UF-CM-sKRKA. Определены задачи (для хэш-функции, используемой в схеме подписи), сложностью которых определяется стойкость схемы.

2. **Формальный анализ модифицированной версии протокола WireGuard на основе отечественных криптографических механизмов**

Скоробогатова Марина Андреевна, старший аналитик, Компания «Актив»
Царегородцев Кирилл Денисович, криптограф-исследователь, Компания «Актив»
В докладе рассматриваются свойства безопасности и подходы к формальной верификации протокола WireGuard. Представлены результаты анализа его адаптированной версии (Ru-WireGuard) с применением инструментов автоматизированной проверки Tamarin и Verifpal.

3. **Модель безопасности для протоколов делегированной аутентификации на основе HTTP**

Мурадян Давид Каренович, инженер-аналитик, КриптоПро
Ахметзянова Лилия Руслановна, к.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро
Алексеев Евгений Константинович, к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро, АНО «НТЦ ЦК»
Настоящая работа посвящена разработке алгоритмической модели безопасности на основе экспериментатора для протоколов делегированной аутентификации на основе HTTP, к которым относится протокол OpenID Connect. Необходимость построения оригинальной модели обусловлена спецификой данного класса протоколов, включая трёхстороннюю архитектуру, особенности взаимодействия по протоколу HTTP и использование TLS с односторонней аутентификацией. Разработанная модель позволяет формализовать угрозы ложной аутентификации и некорректной идентификации пользователя в рамках эксперимента.

4. **Об одной особенности формирования модели нарушителя из потенциально доступных ему возможностей на примере проекта протокола TLS 1.2 на основе механизма инкапсуляции ключа**

Алексеев Евгений Константинович, к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро, АНО «НТЦ ЦК»
Кяжин Сергей Николаевич, к.ф.-м.н., доцент, НИЯУ МИФИ
Мухортова Алена Андреевна, инженер-аналитик, КриптоПро
В настоящей работе приводится пример гипотетической ситуации, вдохновленной одной ранее опубликованной атакой на протокол GC и указывающей на то, что для формирования модели нарушителя недостаточно перечислить потенциально имеющиеся у него возможности по взаимодействию с криптосистемой, т.к. между ними могут существовать нетривиальные и обусловленные исключительно практикой применения зависимости. В рамках указанной практической ситуации (и продиктованной ей модели нарушителя) проводится анализ защищенности проекта протокола TLS 1.2 на основе механизмов инкапсуляции ключа, который в настоящее время разрабатывается в рамках технического комитета по

стандартизации №26. Показывается, что текущая версия протокола при рассматриваемых возможностях нарушителя допускает компрометацию вырабатываемого сеансового ключа. Предлагаются методы модификации протокола и требования к его реализации, которые позволяют добиться защищенности от подобной атаки.

5. Иллюзия теоретической безопасности: тайна памяти нарушителя

Новиков Антон Александрович, ТК 26, Академия криптографии Российской Федерации
Фомин Денис Бонифатович, ТК 26, Академия криптографии Российской Федерации

В алгоритмическом подходе на основе экспериментатора (game-based) сохраняется методологическая проблема: формально всегда существует противник, находящий коллизию с преимуществом 1, хотя явно он может быть неизвестен (парадигма Human Ignorance). Аналогичным образом, стандартные модели безопасности часто упускают, что нарушитель может использовать вспомогательную информацию, полученную на этапе предварительной обработки. Игнорирование этого факта завышает оценки теоретической стойкости, поскольку существование эффективных методов анализа, связанных с балансировкой по времени и памяти доказано теоретически. Это ставит вопрос о пересмотре традиционных предположений о возможностях нарушителя, используемых при получении оценок теоретической стойкости.

ЗАЛ «СОСНОВЫЙ»

12:00 –14:00

Секция "Квантово-устойчивая защита информации. Наука, технологии, регуляторика и кадры"

Секция посвящена вопросам внедрения и развития квантовых технологий для обеспечения безопасности цифровых данных и сервисов. В настоящий момент идут разработки, есть крупные заказчики, формируется нормативное поле. Университеты включают данную тематику в свой образовательный процесс и уже завершен целый ряд НИР и НИОКР проектов. В рамках сессии прозвучат доклады разработчиков, буден дан обзор международной практики и опыта индустриальных заказчиков, пройдет обсуждение инициатив 2025-2026 годов.

Ведущий:

1. **Корольков Андрей Вячеславович,** Национальный координационный центр по компьютерным инцидентам, член-корреспондент Академии криптографии Российской Федерации
2. **Федоров Алексей Константинович**, PhD, вице-президент, Газпромбанк

1) О перспективах использования систем квантового распределения ключей в государственных информационных системах

Науменко Антон Павлович, ООО «СФБ Лаб», АО «ИнфоТеКС»
Зызыкин Артём Павлович, ООО «СФБ Лаб»
Лохматов Роман Юрьевич, ООО «СФБ Лаб»

В докладе рассмотрены основные нормативно-технические предпосылки для использования систем КРК для защиты информации в государственных информационных системах, предложены конкретные сценарии указанного использования, в том числе с учетом перспективных систем КРК (квантовая космическая группировка) и перспективных угроз информационной безопасности («квантовая угроза»).

2) Реализация и исследование модульной системы квантового распределения ключей в атмосферном канале связи

Воробей Сергей Сергеевич, начальник отдела лицензирования и сертификации, ООО «КуРэйт»

В работе рассматриваются вопросы построения и полевых испытаний модульной системы квантового распределения ключей (КРК) на базе атмосферных оптических линий связи (АОЛС). Описан подход к интеграции коммерческих установок КРК, разработанных для волоконно-оптических линий, с терминалами АОЛС. Приведены результаты экспериментов в условиях Московской агломерации, проанализированы причины потерь и нестабильности синхронизации. Представлены методы оптимизации оптического тракта и алгоритмов постобработки для достижения стабильной генерации ключа.

3) Многопользовательские квантовые сети: от архитектуры к сервисам
Сантьев Алексей Альбертович, руководитель направления развития и продвижения продуктов, ООО «СМАРТС-Кванттелеком»
Козубов Антон Владимирович, руководитель центра прикладных квантовых технологий и инноваций, ООО «СМАРТС-Кванттелеком»
Архитектурные принципы построения многопользовательских квантовых сетей с промежуточными доверенными узлами. Мировой опыт развёртывания магистральных и городских квантовых инфраструктур, включая подходы к организации связи между узлами, маршрутизации и обеспечению отказоустойчивости. Переход к сервисной модели оказания услуг квантовой сети: выделению ресурсов под различные классы приложений, поддержке качества обслуживания (QoS), организации «последней мили» и доступа в формате «ключ как сервис». Подходы к управлению сетью как единой инфраструктурой. На примере реализованных пилотных проектов будут продемонстрированы возможности интеграции квантовых сетей в существующую телекоммуникационную инфраструктуру.

4) Модель сервисов и услуг квантовых коммуникаций с использованием Магистральной квантовой сети ОАО «РЖД»
Соколов Владислав Валерьевич, заместитель начальника Департамента квантовых коммуникаций ОАО «РЖД»
Доклад посвящен обзору модели сервисов, применяемых на текущей архитектуре магистральной квантовой сети ОАО «РЖД». Особенности организации сервисной модели, предоставления квантовозащищенных ключей и способа их распределения по квантовой сети с различными способами доставки до пользовательских средств криптографической защиты информации по протоколу ProtoQa.
Будут представлены продукты, применяемые на Магистральной квантовой сети. Рассмотрена схема оказания услуг с указанием участников и их ролей.

5)Постквантовая криптография: регуляторная и конкурентная среда, образование
Гугля Антон Павлович, генеральный директор**,** КуАпп
Полтавская Ирина Вячеславовна, коммерческий директор КуАпп, РУДН
В докладе рассматривается постквантовая криптография как практическая задача для цифровой экономики и государственной безопасности.

6)Опыт пилотирования квантово-устойчивых продуктов в Газпромбанке. Экспериментальный правовой режим (ЭПР) как возможный инструмент для последующего тестирования технологии
Ливашвили Илья Абрамович, начальник Департамента аналитики и внедрения технологий, Газпромбанк
В ходе доклада будет озвучен практический опыт пилотных интеграционных проектов по реализации квантово-устойчивой защиты ИТ-систем Банка: квантово-устойчивые мобильные BLE-платежи, постквантовая защита канала API дистанционного банковского обслуживания физических лиц. Будут рассмотрены вызовы и подходы к их решению в рамках пилотирования.Будет инициирована дискуссия о технологической и правовой возможности последующего внедрения гибридной криптографии (сопряжение классических и постквантовых алгоритмов).

ЗАЛ «ШИШКА»

15:00 –16:30

Круглый стол «Мобильные решения и криптография»

Круглый стол, посвященный российской криптографии в приложениях для мобильных платформ. Выбор технологий, встраивание и эксплуатация, выполнение требований и жизненный цикл приложений, пользовательские сценарии. Открытый диалог с участием разработчиков СКЗИ и мобильных приложений, регуляторов рынка и владельцев информационных систем.

Ведущие:

1. **Пьянченко Андрей Андреевич**, руководитель команды криптографии, MAX
2. **Дегтярев Алексей Валерьевич,** начальник управления криптографии, аутентификации и идентификации, Сбер

Эксперты круглого стола:

3. **Абрамов Михаил Андреевич,** начальник Управления информационной безопасности Федеральной налоговой службы
4. **Семенов Евгений Николаевич,** заместитель генерального директора, АО «ЦБТ»
5. **Горбут Андрей Александрович,** исполнительный директор - начальник отдела развития технологий криптозащиты, Сбер
6. **Верестникова Дарья Дмитриевна,** генеральный директор, ООО «СТ-Крипт»
7. **Елистратов Андрей Алексеевич,** Банк России
8. **Петров Алексей Владимирович,** ФСБ России

ЗАЛ «ЕЛОВЫЙ»

15:00 –16:30

Секция «Математические аспекты защиты информации в области синтеза и анализа генераторов случайных чисел»

Секция, посвященная проблематике, находящейся на стыке прикладных и теоретических аспектов информационной безопасности. В рамках секции обсуждаются вопросы, связанные с задачами, возникающими в процессе разработки и обоснования качества генераторов случайных чисел, входящих в состав широкого класса средств защиты информации.

Ведущий:

1. **Миронкин Владимир Олегович,** к.ф.-м.н.**,** ФСБ России

1) **Физико-техническая модель – первый шаг к обоснованию качества физических генераторов случайных чисел**

Охлюев Олег Александрович, ФСБ России

Предлагается методология построения физико-технической модели (ФТМ), выступающей в качестве промежуточного звена между схемотехнической реализацией генератора и его теоретико-вероятностной моделью (ТВМ). В рамках ФТМ формализуется исходный процесс, описывается прохождение сигнала через аналоговый тракт с учётом передаточных функций и собственных шумов компонентов, а также моделируются процедуры дискретизации и квантования. В докладе предлагается структура ФТМ, включающая формализацию физического процесса, модели аналогового тракта и аналого-цифрового преобразования, а также методологию экспериментальной валидации выдвигаемой статистической гипотезы. Применение данного подхода позволяет перейти от постулирования случайности к её прогнозированию в наихудших условиях эксплуатации.

2) **Об оценке влияния алгоритма статистического выравнивания Бабкина на качество физических генераторов случайных чисел**

Зайцев Александр Владимирович, МИРЭА

Миронкин Владимир Олегович, к.ф.-м.н., ФСБ России

В рамках математической модели двоичного дискретного источника, приближенной к практическим условиям функционирования широкого класса физических генераторов случайных чисел, исследовано влияние алгоритма статистического выравнивания Бабкина на распределение знаков формируемых

последовательностей. Установлено, что в ряде случаев ожидаемого приближения к равновероятности распределения за счет применения указанного алгоритма не наблюдается.

3) О влиянии дискретизации на практическую секретность ключей, формируемых по схеме интервалов
Богданов Дмитрий Сергеевич, ФСБ России
Зачастую биты ключа, формируемые физическими генераторами случайных чисел (ФГСЧ), не являются реализациями независимой равновероятной схемы, в связи с чем возникает понятие «практическая секретность ключа». Для некоторых ФГСЧ, построенных по схеме интервалов, указанное отличие может быть обусловлено дискретностью времени, измеряемого электронными компонентами. В докладе для модели ФГСЧ, основанной на суммировании независимых одинаково распределенных случайных величин (интервалов времени), получены оценки сверху на параметр ε, характеризующий практическую секретность ключа, с учётом влияния дискретизации.

4) О доверительном оценивании практической секретности для некоторых вероятностных моделей
Царегородцев Кирилл Денисович, Компания «Актив»
Скоробогатова Марина Андреевна, Компания «Актив»
В связи с тем, что иногда конкретные характеристики вероятностной модели неизвестны, представляют интерес не только точечные оценки практической секретности ключа, но и доверительные интервалы для него. В рамках доклада рассмотрены вопросы доверительного оценивания значения логарифма практической секретности для схемы Бернулли и цепей Маркова.

5) Построение теоретико-вероятностной модели для физического датчика случайных чисел на базе кольцевых осцилляторов
Бобровский Дмитрий Александрович, ООО «Код Безопасности»
Задорожный Дмитрий Игоревич, ООО «Код Безопасности»
Недомолкин Илья Эдуардович, ООО «Код Безопасности»
В докладе представлена теоретико-вероятностная модель ФДСЧ на основе КО. Получена оценка отклонения вырабатываемой последовательности от равновероятного распределения. На основе оценки определены параметры датчика, обеспечивающие практическую секретность формируемого ключа, близкую к максимальной. Корректность модели подтверждена экспериментально на физически реализованном датчике; выходная последовательность проанализирована с использованием статистических тестов NIST.

ЗАЛ «СОСНОВЫЙ»

15:00 –16:30

Секция «Перспективные исследования в области кибербезопасности» Часть №1

Научная секция, посвященная широкому кругу вопросов информационной безопасности. Академические исследования и прикладные проекты.

Ведущий:

1. **Котенко Игорь Витальевич,** д.т.н., профессор, заслуженный деятель науки РФ, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН, профессор Университета ИТМО и Университета Иннополис

1) Объяснимое обнаружение вторжений: анализ современных исследований и основные тренды
Котенко Игорь Витальевич, д.т.н., профессор, заслуженный деятель науки РФ, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН, профессор Университета ИТМО и Университета Иннополис
Растущая изощренность кибератак подчеркивает жизненно важную необходимость в надежных и подотчетных системах обнаружения вторжений (СОЗ). В докладе анализируется развитие методов объяснимого искусственного интеллекта (ОИИ) в исследованиях по созданию СОЗ, охватывающее традиционные статистические методы, классическое машинное обучение, глубокое обучение и большие языковые модели. Помимо освещения основных разработок в области СОЗ на основе ОИИ, в докладе обобщены сравнительные результаты по объяснимости, вычислительной эффективности и точности обнаружения для различных подходов.

2) **Обнаружение сетевых атак на основе многозначных зависимостей**

Шелухин Олег Иванович, д.т.н., профессор, заведующий кафедрой ИБ, МТУСИ
Раковский Дмитрий Игоревич, к.т.н., доцент, доцент кафедры ИБ, МТУСИ
В докладе представлена концепция многозначной классификации сетевого трафика, учитывающая свойство многозначности целевых атрибутов - одновременную ассоциацию одной записи трафика с несколькими типами атак. Рассматриваются проблемы учета многозначных зависимостей в контексте решения задачи классификации и их взаимосвязь с редкими аномальными событиями.

3) **LLM как инструмент аналитика информационной безопасности: анализ применимости и перспективных направлений**

Минзов Анатолий Степанович, профессор, д.т.н, профессор кафедры БИТ, НИУ МЭИ
Невский Александр Юрьевич, доцент, к.т.н, заведующий кафедрой БИТ, НИУ МЭИ
Баронов Олег Рюрикович, доцент, к.т.н, доцент кафедры БИТ, НИУ МЭИ
Использование генеративного искусственного интеллекта в сфере кибербезопасности к началу 2026 года стало не просто трендом, а необходимостью для работы аналитиков в этой сфере деятельности. В докладе рассматриваются вопросы определения уровня проникновения больших лингвистических моделей (LLM) в работу аналитиков различных стран, приводится классификация задач, решаемых с использованием LLM, и примеры решения отдельных задач. Рассматриваются также вопросы применения LLM при проведении перспективных исследований в научных и образовательных учреждениях.

4) **Биометрическая аутентификация пользователей на основе анализа электрической активности мозга с помощью нейросетевых моделей искусственного интеллекта**

Сулавко Алексей Евгеньевич, д.т.н., профессор каф. Комплексная защита информации, Омский государственный технический университет
Предлагается метод идентификации человека с использованием параметров электроэнцефалограмм (ЭЭГ), получаемых различными способами. В лабораторных условиях создана база данных ЭЭГ испытуемых с использованием профессионального оборудования (нейроэнцефалографов). Обработка сигналов ЭЭГ осуществляется ансамблем нейросетевых моделей, извлекающих признаки и осуществляющих распознавание образов пользователей. Предложены нейросетевые модели, позволяющие формировать длинные пароли на основе обработки ЭЭГ, используемые в дальнейшем для аутентификации пользователей. Эксперименты показали уникальность образов ЭЭГ и возможность их использования для осуществления аутентификации с высокой точностью. Так как на сегодняшний день не существует хорошо проработанных атак по перехвату (сделать это дистанционно либо скрыто невозможно) и интерпретации сигналов ЭЭГ, то можно считать данный вид биометрических образов наиболее защищенными от атак посредника, биометрического предъявления и состязательных атак.

5) **Интеллектуальное обнаружение редкой аномальной активности пользователей в информационных системах**

Шелухин Олег Иванович, д.т.н., профессор, заведующий кафедрой ИБ, МТУСИ
Осин Андрей Владимирович, к.т.н., доцент, доцент кафедры ИБ, МТУСИ
На фоне роста объёма и ценности персональных данных в информационных системах усиливаются риски их компрометации. Одним из ранних индикаторов инцидентов может выступать аномальная поведенческая активность пользователей, включая действия внутреннего нарушителя (инсайдера). В докладе сформулировано направление исследований, связанное с разработкой и внедрением интеллектуальных методов выявления редких поведенческих аномалий на основе использования машинного обучения и поведенческого анализа для снижения рисков утечек и повышения эффективности мониторинга безопасности. Обсуждаются результаты экспериментальной проверки предложенных подходов на реальных данных, подтверждающие их практическую применимость.

6) **Факторы деградации архитектуры сегментации LAN: организационные барьеры, легаси-системы и проблемы управления политиками безопасности**

Митрофанов Михаил Валерьевич, д.т.н., доцент, Университет ИТМО
Сетевая сегментация проектируется как изолированная архитектура, однако бизнес-процессы требуют постоянного обмена данными между зонами безопасности, что порождает накопление исключений в политиках и систематическую деградацию изоляции. Для решения этой проблемы разработана математическая модель, описывающая динамику накопления исключений под влиянием организационного сопротивления, эволюцию структуры сети от упорядоченной к хаотической, влияние унаследованных систем

и коэффициент эффективной изоляции как количественную метрику защитного эффекта. Вычислительный эксперимент доказал закономерную деградацию типичной корпоративной архитектуры менее чем за два года и установил критическое условие стабильности: скорость аудита должна превышать скорость генерации исключений. Результаты показали, что устойчивость достигается только комплексной стратегией, объединяющей технологическую модернизацию, процессный контроль и снижение организационных барьеров, что создает инструментарий прогнозирования критических состояний для корпоративных инфраструктур.

7) Облачные и туманные технологии для обеспечения безопасности устройств интернета вещей

Колядин Игорь Витальевич, Самарский национальный исследовательский университет им. академика С.П. Королева
Хайрулов Максим Алексеевич, Самарский национальный исследовательский университет им. академика С.П. Королева
Сухов Андрей Михайлович, д.т.н., профессор, Самарский национальный исследовательский университет им. академика С.П. Королева

Разработка моделей и методов защиты устройств Интернета вещей (IoT) — это важная задача, учитывая многочисленные уязвимости IoT-устройств и их растущее распространение. В докладе представлен анализ технологий, применяемых для обеспечения безопасности IoT решений. Предлагается подход к обеспечению безопасности устройств IoT, состоящий в ограничении запросов к устройству IoT. Для проверки подхода создан экспериментальный полигон. IoT устройство реализовано как мини компьютер под управлением ОС GNU/Linux с подключенными к нему датчиками проводного промышленного интернета вещей. Ключевую роль в этой схеме играет туманный сервер. Основные способы определения компрометации устройства IoT базируются на проверке ограничений на сетевое соединение и измерении объема переданного трафика на сетевом интерфейсе.

8) Методика оценки безопасности значимых объектов критической информационной инфраструктуры

Бондаренко Андрей Владимирович, Уральский Федеральный Университет
Богданов Валентин Викторович, Уральский Федеральный Университет
Домуховский Николай Анатольевич, зам. директора Учебно-научного центра «Информационная безопасность», Уральский Федеральный Университет
Поршнев Сергей Владимирович, профессор, Уральский Федеральный Университет
Кондратенко Марина Александровна, Уральский Федеральный Университет

В докладе обсуждается методика и способ вычисления количественной оценки безопасности значимых объектов критической информационной инфраструктуры, которые обеспечивают переход от качественной оценки выполнения требований нормативно-правовых актов (НПА) в области защиты значимых объектов (ЗО) КИИ к количественной оценке с целью повышения объективности и достоверности процесса контроля обеспечения безопасности ЗО КИИ. Методика обеспечивает возможность сравнительного анализа выполнения требований НПА в области защиты ЗО КИИ в различных субъектах КИИ и группах предприятий, выявлять возможные несоответствия требованиям НПА и выдачу обоснованных рекомендаций по их устранению. Обсуждается алгоритм вычисления итоговой оценки состояния безопасности ЗО КИИ. Приведен пример использования данной методики для вычисления оценки безопасности информации на предприятии, где установлено соответствие между требованиями НПА, процессами и подпроцессам обеспечения безопасности ЗО КИИ и заданы весовые коэффициенты требований, исходя из их важности.

ЗАЛ «ШИШКА»

17:00 – 19:00

Круглый стол «Кибербезопасность и криптография в крупном бизнесе»

Круглый стол, посвященный обеспечению безопасности информационных систем крупных организаций, нюансам использования криптографических средств в этих организациях, возникающим проблемам и их решениям.

Ведущий:

2. **Качалин Алексей Игоревич**, эксперт по развитию информационной безопасности и инновациям. Советник руководителей и владельцев бизнеса. kachalin.com

Участники:

3. **Ярунин Александр Андреевич**, Начальник управления криптографии, Департамент информационной безопасности, X5 Group
4. **Дрозд Алексей Сергеевич**, Руководитель службы криптографической защиты, Дирекции информационной безопасности, ПАО «Вымпелком»
5. **Дутов Кирилл Сергеевич**, Заместитель директора департамента – директор по криптографии и развитию сервисов защиты информации, Промсвязьбанк
6. **Иванов Алексей Александрович**, Управление криптографической защиты, Департамент кибербезопасности, АО "АЛЬФА-БАНК”

ЗАЛ «ЕЛОВЫЙ»

17:00 – 19:00

Секция «Криптография и криптоанализ» Часть №4

Классическая секция конференции, посвященная научным и практическим вопросам криптографии и криптоанализа.

Ведущие:

1) **Матюхин Дмитрий Викторович,** к.ф.-м.н., ФСБ России
2) **Алексеев Евгений Константинович,** к.ф.-м.н., КриптоПро, АНО «НТЦ ЦК»
3) **Поташников Александр Викторович,** к.ф.-м.н., ИнфоТеКС

1) **"Стрибог" под прицелом квантового криптоанализа: итоги и прогнозы**

Орлов Алексей Максимович, ТК 26, Академия криптографии Российской Федерации
Фомин Денис Бонославович, ТК 26, Академия криптографии Российской Федерации
Анализируется стойкость хэш-функции «Стрибог» против квантового нарушителя в модели Q1. Основное внимание уделено устойчивости к нахождению прообраза, второго прообраза и коллизий посредством адаптации классических методов криптоанализа, применяемых к широкому классу хэш-функций. Оценены сценарии наличия и отсутствия у нарушителя значительного объема квантовой памяти. На основе анализа опубликованных работ по криптоанализу хэш-функций показано, что широкий спектр методов анализа, включая исследование функции сжатия с «меньшим количеством раундов», потенциально поддаётся ускорению при наличии у нарушителя доступа к квантовому вычислителю. Выделены направления дальнейших исследований.

2) **Алгебраический анализ шифрсистемы UFHE-ILC на основе свойств дзета-функции Дедекинда и сумм идеалов**

Коновалов Александр, НИЯУ МИФИ
В работе проведён алгебраический анализ неограниченной полностью гомоморфной шифрсистемы UFHE-ILC (An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder Theorem), базирующейся на идеальных решетках. Главными результатами работы являются сформулированные и доказанные теоремы: первая описывает полиномиальный алгоритм восстановления уязвимого ключа, вторая позволяет ограничить снизу вероятность генерации уязвимого ключа алгоритмом, предложенным разработчиками шифрсистемы UFHE-ILC.

3) **Оценка стойкости упрощенной реализации модели блочного алгоритма КБ-256 методом линейных аппроксимаций**

Винокуров Владимир Иванович, к.ф.м.н., в.н.с., Академия Криптографии РФ
Бобровский Дмитрий Александрович, начальник отдела криптоанализа, Код безопасности
В работе исследуется оценка стойкости блочного алгоритма шифрования КБ-256-3 с длиной блока 256 бит путём применения линейного метода анализа к упрощённой (линеаризованной) модели алгоритма. Указан способ построения линейных следов (линейных аппроксимаций) со статистическими преобладаниями, позволяющими для линеаризованной 8-ти раундовой модели алгоритма получить корневую по сравнению с тотальным перебором трудоемкость определения долговременного ключа по известным 2^128 парам 256-битных блоков открытого и шифрованного текстов. Доказана неэффективность рассматриваемого подхода для 9-ти и выше раундовых упрощенных моделей алгоритма КБ-256 по сравнению с методом тотального опробования даже на материале 2^256 пар открытого и шифрованного текста.

4) **О проблематике выбора режимов работы блочных шифров для защиты системного раздела диска**

Коренева Алиса Михайловна, к.ф.-м.н., заместитель руководителя службы сертификации по научно-техническому сотрудничеству ООО «Код Безопасности»
Минаков Сергей Сергеевич, старший научный сотрудник, Академия криптографии Российской Федерации
Фирсов Георгий Валентинович, начальник отдела разработки платформы средств защиты конечных точек ООО «Код Безопасности», Национальный исследовательский ядерный университет «МИФИ»
В рамках деятельности рабочей группы «Сопутствующие криптографические алгоритмы и протоколы» ТК 26 проходит период изучения по вопросу использования ГОСТ 34.12–2018 в режиме XEH. Одной из задач исследовательского периода является сравнение этого режима со стандартизированными. В докладе приведены результаты сравнительного анализа режима XEH с режимами DEC, CTR, CFB, CTR, OFB, CTR-ACPKM, MGM применительно к задаче обеспечения конфиденциальности информации на системном носителе с блочно-ориентированной структурой.

5) **Memory-Hard функции: обзор подходов к построению и анализу**

Чичаева Анастасия Александровна, специалист-исследователь лаборатории криптографии АО «НПК «Криптонит»
Давыдов Степан Андреевич, старший специалист-исследователь лаборатории криптографии АО «НПК «Криптонит»
В докладе представлен обзор криптографических функций, реализация которых требует значительных объёмов памяти (Memory-hard функций, MHF). Рассматриваются современные подходы к построению MHF, в частности изучаются конструкции функций Scrypt, Argon2 и др. Исследуются вопросы формализации свойства memory-hardness, методы анализа безопасности, и перспективы создания отечественной MHF.

ЗАЛ «СОСНОВЫЙ»

17:00 – 19:00

Секция «Перспективные исследования в области кибербезопасности» Часть №2

Научная секция, посвященная широкому кругу вопросов информационной безопасности. Академические исследования и прикладные проекты.

Ведущий:

1. **Котенко Игорь Витальевич,** д.т.н., профессор, заслуженный деятель науки РФ, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН, профессор Университета ИТМО и Университета Иннополис