Ассоциация РусКрипто

ОРГАНИЗАТОРЫ

АИС

РУСКРИПТО'2021

XXIII МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ПРОГРАММА

23-26 МАРТА 2021 Г.

БЛАГОДАРИМ СПОНСОРОВ И ПАРТНЕРОВ ЗА ОКАЗАННУЮ ПОДДЕРЖКУ!

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

КРИПТОПРО
ключевое слово в защите информации

ГЕНЕРАЛЬНЫЙ СПОНСОР

infotecs®

СЕРЕБРЯНЫЙ ПАРТНЕР

КОМПАНИЯ АКТИВ

НАУЧНЫЙ ПАРТНЕР

НЕОБИТ

ИННОВАЦИОННЫЙ ПАРТНЕР

РЖД

БРОНЗОВЫЕ ПАРТНЕРЫ

Информзащита
Системный интегратор

SPACE-BIT

ФАКТОР-ТС

КРИПТОНИТ

Ростелеком
Солар

ПАРТНЕРЫ КОНФЕРЕНЦИИ

КОД безопасности

Avanpost

АО ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

СПБ

kaspersky

АССОЦИАЦИЯ РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ

АБИСС
Ассоциация пользователей стандартов по информационной безопасности АБИСС

ЭЛВИС

CROSSTECH SOLUTIONS GROUP

TESSIS

THALES

АПКИТ

STAFFCOP

ГЛАВНЫЙ ИНТЕРНЕТ-ПАРТНЕР

BIS JOURNAL

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

ВСЕ МЕРОПРИЯТИЯ ИТ НА ICT2GO

ICT ONLINE
ИНФОКОММУНИКАЦИИ ОНЛАЙН

Единый портал Электронной подписи

Системный администратор

AIS EVENT

Отсканируйте QR-код
или введите название
приложения AIS EVENT
в App Store и Google Play.

И далее, следуя инструкции,
авторизируйтесь в приложении.

Вся информация о мероприятии в вашем телефоне

Всегда актуальная программа, информация о спикерах
и участниках, общение и нетворкинг.

Загрузить в App Store

Загрузить на Google Play

конференция РусКрипто

ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ

ОБЩИЕ ПРАВИЛА ДЛЯ УЧАСТНИКОВ

- Пропуск на территорию отеля в период проведения конференции осуществляется строго по спискам зарегистрированных участников.
- Питание на территории отеля организовано по системе «все включено» с 08:00 до 23:00. Время завтраков, обедов и ужинов для участников «РусКрипто'2021» указано в программе.

ОРГАНИЗОВАННЫЙ ЗАЕЗД И ВЫЕЗД ИЗ ОТЕЛЯ «СОЛНЕЧНЫЙ PARK HOTEL & SPA»

24 марта в 08:00 утра трансфер м. Тимирязевская - отель «Солнечный Park Hotel & SPA»

24 марта в 20:00 вечера трансфер отель «Солнечный Park Hotel & SPA» - м. Тимирязевская

25 марта в 08:00 утра трансфер м. Тимирязевская - отель «Солнечный Park Hotel & SPA»

25 марта в 20:00 вечера трансфер отель «Солнечный Park Hotel & SPA» - м. Тимирязевская

Внимание! *Указано время отправления автобусов, просим подъезжать за 10-15 минут до времени отправления. В случае опоздания, просьба заранее предупредить организаторов.*

26 марта в 12:15 трансфер отель «Солнечный Park Hotel & SPA» - м. Тимирязевская
Подача автобусов в 12:00 у ворот отеля.

Внимание! *Автобусы с табличкой «РусКрипто'2021» отправятся ровно в 12:15. Просьба заранее сдать номера и не опаздывать.*

АДРЕС ОТЕЛЯ «СОЛНЕЧНЫЙ PARK HOTEL & SPA»

Московская обл, Солнечногорский р-н, деревня Дулепово, стр 21 (отель Солнечный)
Телефон: +7 (925) 922-42-00

Расчетный час:
Заезд - 23 марта с 16:00
Выезд - 26 марта до 12:00

24 и 25 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»

ОБЩАЯ ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ

- На стойке регистрации в получите индивидуальный бейдж.
  Напоминаем, что посещение всех мероприятий конференции возможно только при наличии бейджа.

- Официальный хэштег конференции **#RusCrypto**
  Мы будем рады, если вы будете упоминать наше мероприятие с этим хэштегом.

- Получить закрывающие документы вы сможете на стойке регистрации 24-25 марта.

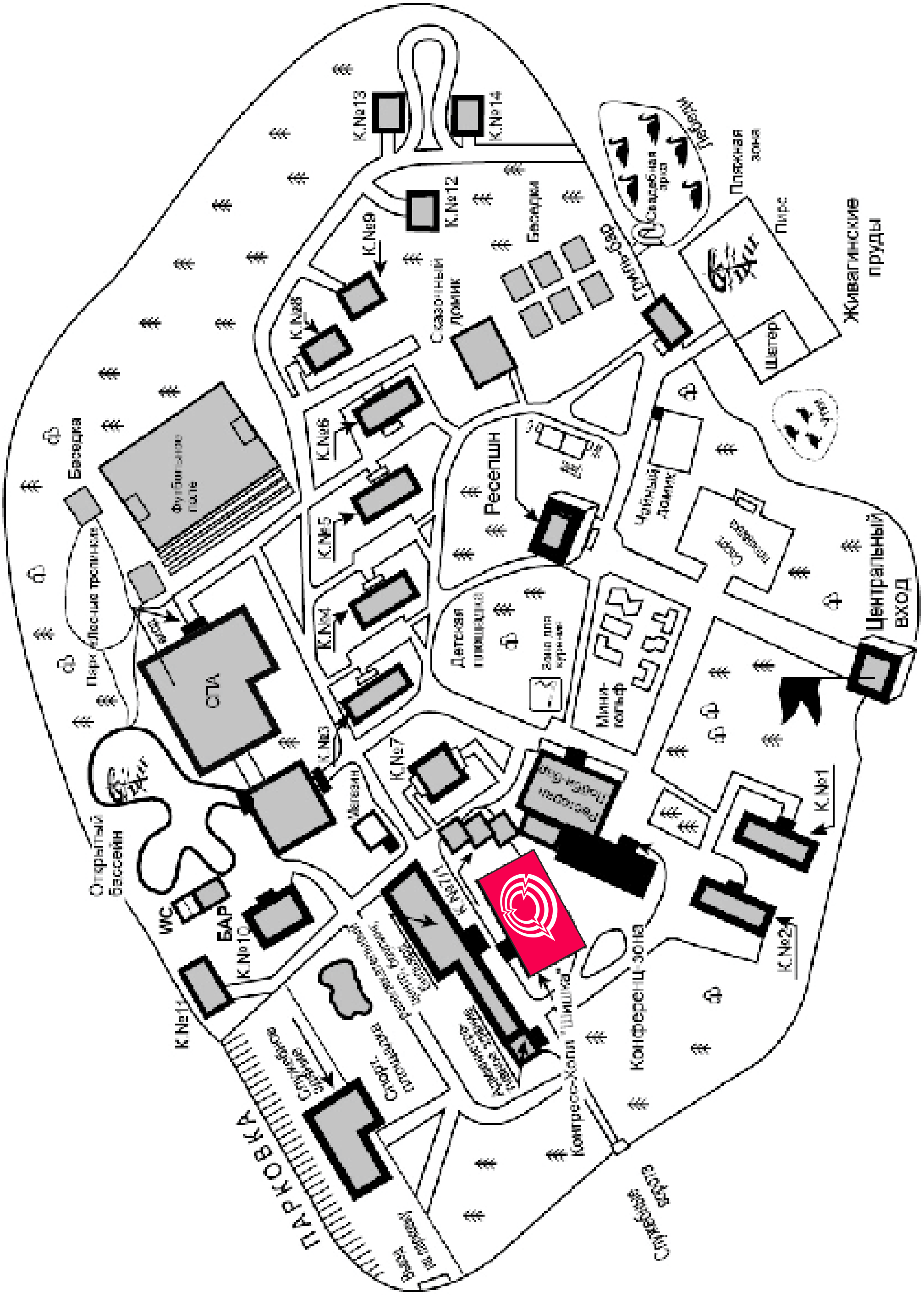
ОБСЛУЖИВАНИЕ В ОТЕЛЕ ПО СИСТЕМЕ «ALL INCLUSIVE»:

- расширенный шведский стол: завтрак (08:00-11:00), обед (13:00-16:00), ужин (19:00-23:00);
- в течение всего дня с 8-00 до 23-00 кофе, чай, выпечка, мороженое, соки, лимонады, разливное пиво, алкогольные напитки;
- бильярд, боулинг, пинг-понг;
- посещение термальной зоны SPA-комплекса (10 бассейнов и 16 термальных комнат, бассейны в виде грибов – зона без спасателей);
- тренажерный зал (посещение в спортивной обуви);
- сквош-корт, скалодром (посещение в спортивной обуви);
- детский развлекательный центр, игровые автоматы.

ДОПОЛНИТЕЛЬНЫЙ СЕРВИС (ОПЛАЧИВАЕТСЯ ДОПОЛНИТЕЛЬНО):

- Лобби-бар;
- ресторан Чердак LOFT;
- ресторан Гриль-бар;
- Snack-bar;
- ресторан Чайный домик;
- Book reader bar;
- Сигарная комната;
- Pool bar;
- Beauty зона SPA-комплекса.

24 и 25 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»



ПАРКОВКА
СПА
Открытый бассейн
БАР
WC
Беседка
Футбольное поле
Магазин
Ресепшн
Сказочный домик
Беседки
Гриль-бар
Пирс
Шатер
Пляжная зона
Живагинские пруды
Центральный вход
Чайный домик
Мини-гольф
Детская площадка
Конференц-зона
Конгресс-Холл "Шишка"
К.№1
К.№2
К.№3
К.№4
К.№5
К.№6
К.№7
К.№8
К.№9
К.№10
К.№11
К.№12
К.№13
К.№14

ТАЙМЛАЙН КОНФЕРЕНЦИИ

23 МАРТА, ВТОРНИК. ДЕНЬ ЗАЕЗДА

15:00 – 16:30	Трансфер: метро Тимирязевская – отель «Солнечный Park Hotel & SPA» Заезд и регистрация участников, проживающих в отеле
17:00 – 19:00	Соревнования в СПА-комплексе (плавание, сквош, армрестлинг) Спортивные турниры в развлекательном комплексе (бильярд, настольный теннис, боулинг)
19:30 – 23:00	Караоке баттл. Чайный домик
20:00 – 22:00	Устричный вечер. Лобби ресторанного комплекса, 1 этаж

24 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

09:00 – 10:00	Регистрация участников		
10:00 – 12:30	**Официальное открытие конференции. Пленарное заседание** *Зал «Шишка», 2 этаж* *10 стр.*		
12:30 – 12:50	Кофе-брейк		
12:50 – 14:30	Секция **«Электронная подпись для гражданина, бизнеса и государства»** Ведущий: Малинин Ю.В., Ассоциация «РОСЭУ» *Зал «Шишка»* *11 стр.*	Секция **«Инженерно-технические и правовые аспекты цифровой криминалистики и судебной экспертизы»** Ведущие: • Чиликов А.А., МГТУ им. Баумана • Абрамец А.С., ФГБУ «ЦЭКИ» *Зал «Еловый»* *11-12 стр.*	**Закрытая секция АБИСС. Для представителей финансовых организаций. Часть I.** Ведущий: Харыбина А.А., Ассоциация «АБИСС», AKTIV.CONSULTING *Зал «Сосновый»* *13 стр.*
14:30 – 15:30	Обед		
15:30 – 17:00	Секция **«Требования к криптографическим средствам защиты информации»** Ведущий: Петров А.В., ФСБ России *Зал «Шишка»* *13 стр.*	Секция **«Перспективные решения российских разработчиков средств информационной безопасности»** Ведущий: Смирнов Н.В., АО «ИнфоТеКС» *Зал «Еловый»* *14 стр.*	**Закрытая секция АБИСС. Для представителей финансовых организаций. Часть II.** Ведущий: Харыбина А.А., Ассоциация «АБИСС», AKTIV.CONSULTING *Зал «Сосновый»* *15 стр.*
17:00 – 17:30	Кофе-брейк		
17:30 – 19:30	Секция **«Криптография и информационная безопасность в банковской сфере»** Ведущие: • Простов В.М., ТК26 • Голованов В.Б., ТК 122 • Сычев А.М., Банк России *Зал «Сосновый»* *16 стр.*	Секция **«Криптография и криптоанализ», 1 часть** Ведущие: • Матюхин Д.В., ФСБ России • Алексеев Е.К., КриптоПро • Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Зал «Еловый»* *17 стр.*	Круглый стол **«Пространство доверия ЭП, ЭДО и цифровых услуг»** Ведущие: • Новиков Ф.В., ФНС России • Малинин Ю.В., Ассоциация «РОСЭУ» *Зал «Стеклянный»* *18 стр.*

19:30 – 20:00	Ужин
20:00 – 22:00	**Торжественное открытие «РусКрипто'2021».** Зал «Шишка», 2 этаж

25 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 09:30	Завтрак		
09:30 – 11:30	Секция **«Российская и международная стандартизация»** Ведущий: • Бондаренко А.И., ТК 26 • Смышляев С.В., КриптоПро *Зал «Шишка»* *19 стр.*	Секция **«Криптография и криптоанализ», 2 часть** Ведущие: • Матюхин Д.В., ФСБ России • Алексеев Е.К., КриптоПро • Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Зал «Еловый»* *21 стр.*	Секция «**Перспективные подходы к обеспечению безопасности киберфизических систем**» Ведущие: • Зегжда Д.П., ИКиЗИ СПбПУ Петра Великого • Иванов Д.В., НеоБИТ *Зал «Сосновый»* *22 стр.*
11:30 – 11:50	Кофе-брейк		
11:50 – 13:10	Секция **«Информационная безопасность и криптография в государственных информационных системах»** Ведущие: • Пьянченко А.А., НИИ «Восход» • Горелов Д.Л., компания «Актив» *Зал «Шишка»* *23 стр.*	Секция **«Криптография и криптоанализ», 3 часть** Ведущие: • Матюхин Д.В., ФСБ России • Алексеев Е.К., КриптоПро • Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Зал «Еловый»* *24 стр.*	Секция **«Развитие высокотехнологичной области «Квантовые коммуникации» 1 часть** Ведущие: • Глейм А.В., ОАО «РЖД» • Уривский А.В., АО «ИнфоТеКС» *Зал «Сосновый»* *25 стр.*
13:10 – 13:30	Кофе-брейк		
13:30 – 14:30	Круглый стол **«Проблемы обезличивания персональных данных»** Ведущий: Маршалко Г. Б., ФСБ России *Зал «Шишка»* *26 стр.*	Секция **«Российская электроника и информационная безопасность»** Ведущий: Карантаев В., Лаборатория Касперского *Зал «Еловый»* *26 стр.*	Секция **«Развитие высокотехнологичной области «Квантовые коммуникации» 2 часть** Ведущие: • Глейм А.В., ОАО «РЖД» • Уривский А.В., АО «ИнфоТеКС» *Зал «Сосновый»* *27 стр.*
14:30 – 15:30	Обед		
15:30 – 17:00	Круглый стол **«Технологии дистанционного электронного голосования. Задачи и перспективы»** Ведущие: • Шумский Л.С., Ассоциация ФинТех • Смышляев С.В., КриптоПро *Зал «Шишка»* *28 стр.*	Секция **«Криптография и криптоанализ», 4 часть** Ведущие: • Матюхин Д.В., ФСБ России • Алексеев Е.К., КриптоПро • Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Зал «Еловый»* *28 стр.*	Секция **«Блок гуманитарных вопросов»** Ведущие: • Аронова А.С., АО «ГЛОНАСС» • Елисеев И.Ю., АИС *Зал «Сосновый»* *29 стр.*

17:00 – 17:30	Кофе-брейк		
17:30 – 19:30	Секция **«Информационная безопасность и криптография в робототехнических системах»** Ведущий: Новиков В.А., Технологии Радиоконтроля *Зал «Еловый»* *30 стр.*	Секция **«Перспективные исследования в области кибербезопасности»** Ведущий: Котенко И.В., СПИИРАН *Зал «Сосновый»* *32 стр.*	Секция **«Подготовка специалистов по защите информации для решения задач цифровой экономики»** Ведущие: • Белов Е.Б., ФУМО ВО ИБ • Лось В.П., МОО «АЗИ» • Хайров И.Е., АИС *Зал «Стеклянный»* *33 стр.*
19:30 – 20:00	Ужин		
20:00 – 22:00	Интеллектуальный криптографический квиз «Игра в имитацию». Зал «Шишка», 2 этаж		

26 МАРТА, ПЯТНИЦА. ДЕНЬ ОТЪЕЗДА

09:00 – 11:00	Завтрак
12:00	Трансфер отель «Солнечный Park Hotel & SPA» – м. Тимирязевская

ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 12:30 **Пленарное заседание**
Зал «Шишка»

Официальное открытие конференции. Приветственные слова

Данные, интеллект и безопасность
***Маршалко Григорий Борисович**, ФСБ России*
Безопасность оборота данных и их использования в системах искусственного интеллекта. Возможные технологические решения, направления развития, тенденции и проблемы, российский и мировой опыт.

Криптографические протоколы нового десятилетия с поддержкой российских алгоритмов
***Смышляев Станислав Витальевич**, к.ф.-м.н., заместитель генерального директора, КриптоПро*
Близок к завершению продолжавшийся более десяти лет процесс по внедрению и стандартизации российских алгоритмов в основных криптографических протоколах сети Интернет. Важно не упустить момент и обеспечивать поддержку ГОСТ теперь и в тех протокольных решениях, которые пока в международном сообществе находятся в процессе разработки, в том числе протоколов с применением постквантовых механизмов, решений для дистанционного электронного голосования, перспективных протоколов защиты соединений, хранимых данных и сообщений в мессенджерах. Обзор направлений международных исследований и стандартизации в области протоколов, а также перспективы разработки и анализа версий с поддержкой российских криптографических алгоритмов.

Идентификация личности - ключевая проблема облачной подписи
***Баранов Александр Павлович,** д.ф-м.н., Академия криптографии Российской Федерации, РГУ нефти и газа (НИУ) имени И.М. Губкина*

Квантовые вычисления в России и мире
***Кулик Сергей Павлович,** д.ф-м.н., профессор кафедры квантовой электроники, МГУ имени М.В. Ломоносова*
О современном состоянии и перспективах развития квантовых вычислений. Что умеют квантовые компьютеры уже сейчас и чему научатся в будущем? Влияние квантовых вычислений на науку в целом и информационные технологии в частности. Информационная безопасность и квантовые вычисления.

О связи прошедших столетий истории Криптографической службы России
***Столпаков Борис Владимирович,** историк криптографии, к.ф.-м.н, ведущий научный сотрудник НКО «ФСРБИТ»*
5 мая 2021 года отмечается столетие постановления Совнаркома о создании Специального отдела при ВЧК. Это событие принято считать той точкой отсчёта, начиная с которой заявила о себе Криптографическая служба Советской России, затем СССР, а с 1991 г. и современной России. Принятые решения положили начало созданию системы защиты информации в нашей стране, системы, усвоившей богатое наследие имперского периода. Почти 400-летнюю историю российской криптографии отсчитывают от 8 (18) августа 1633 г., времени указа о безусловной необходимости использования шифрования в переписке с представителями государства за границей. Указа, немедленно подкреплённого комплексом документов и неукоснительно выполняемого. Каждое из трёх столетий имперского периода по-своему примечательно, но особенно значимым представляется последнее, завершившееся в 1917 г. Это время признанных высоких достижений криптографов России, а также её учёных, создавших мощный теоретический фундамент, ставший основой успехов советской криптографии.

12:50 – 14:30 Секция «Электронная подпись для гражданина, бизнеса и государства»

Зал «Шишка»

Изменения в Федеральный закон «Об электронной подписи» уже оказывают влияние на технические и на организационные аспекты применения квалифицированной электронной подписи. Текущий 2021 год является переломным для всех информационных систем, использующих КЭП. В рамках круглого стола эксперты обсудят новые возможности и сложности этого переходного периода, сценарии работы в новых условиях, варианты минимизации возможных рисков для граждан и юридических лиц. В обсуждениях примут участие представители Министерства цифрового развития, связи и массовых коммуникаций, ФСБ России, Федеральной налоговой службы, Федерального казначейства, Федеральной таможенной службы.

Ведущий: **Малинин Юрий Витальевич,** президент Ассоциации «РОСЭУ»

Участники дискуссии:

- **Кузнецов Роман Валерьевич**, директор правового департамента, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- **Бражко Вячеслав Сергеевич**, начальник Управления режима секретности и безопасности информации, Федеральное казначейство
- **Новиков Федор Вадимович**, начальник управления электронного документооборота, Федеральная налоговая служба
- **Романов Кирилл Олегович**, начальник отдела информационной безопасности и технической защиты информации, Федеральная таможенная служба
- **Маслов Юрий Геннадьевич**, коммерческий директор, КриптоПро
- **Мелузов Антон Сергеевич**, заместитель генерального директора по развитию бизнеса, ИнфоТеКС Интернет Траст

Есть ли жизнь после монополии ГосУЦ?

Маслов Юрий Геннадьевич, *коммерческий директор, КриптоПро*

С введением государственной монополии на создание и выдачу квалифицированных сертификатов ключей проверки электронных подписей для государственных и муниципальных служащих, юридических лиц и индивидуальных предпринимателей, и прочих категорий согласно поправкам в 63-ФЗ, создаётся впечатление, что рынок услуг PKI начнёт сокращаться, как шагреневая кожа, до невозможных значений. Компания «КРИПТО-ПРО», как разработчик и поставщик решений для технологии PKI, заглянула за линию горизонта будущих событий, провела оценку вероятностей и сделала свой прогноз развития.

Пространство доверия ЭП, как изменятся риски?

Мелузов Антон Сергеевич, *заместитель генерального директора по развитию бизнеса, Инфотекс Интернет Траст*

С изменением регулирования изменяется ландшафт рисков в пространстве доверия электронной подписи. Какие риски уйдут, какие новые риски появляются и как на них реагировать. Как учитываются технологические особенности различных информационных систем?

12:50 – 14:30 Секция «Инженерно-технические и правовые аспекты цифровой криминалистики и судебной экспертизы»

Зал «Еловый»

Компьютерно-техническая экспертиза является в наше время важнейшей частью расследования преступлений и инцидентов информационной безопасности. Методы цифровой криминалистики постоянно совершенствуются, а задачи усложняются. В рамках нашей секции ведущие специалисты отрасли расскажут о новых инструментах и технологиях цифровой криминалистики, поделятся практическим опытом, обсудят важные правовые моменты, связанные с экспертизой цифровых улик.

Ведущие:

- **Чиликов Алексей Анатольевич,** МГТУ им. Баумана, Passware
- **Абрамец Алексей Сергеевич,** начальник управления экспертизы информационных технологий департамента экспертиз ФГБУ «ЦЭКИ»

Особенности извлечения данных из Samsung Exynos устройств

***Каррондеев Андрей Михайлович**, Oxygen Software*

Компания Samsung является одним из крупнейших производителей мобильных устройств. В отличие от большинства других производителей, Samsung использует в своих смартфонах целый ряд собственных механизмов защиты, а также может позволить выпускать устройства на базе процессоров Exynos собственного производства. С одной стороны, это обеспечивает в среднем более высокий уровень безопасности, а с другой – приводит к возникновению уязвимостей характерных только для Samsung Exynos устройств. В докладе будут описаны уязвимые места Samsung Exynos устройств, а также показано, что в ряде случаев из них возможно извлечение пользовательских данных.

Особенности криминалистического анализа смартфонов на базе MediaTek чипсетов

***Бояркин Антон Михайлович**, Passware*

Доклад посвящен процессу анализа смартфонов под упрвалением ОС Android для получения возможности offline перебора извлеченных зашифрованных пользовательских данных. Интерес к данной теме обусловлен применением программно-аппаратных механизмов защиты при вычислении мастер-ключа шифрования. Криптографические системы, использующие аппаратную часть, затрудняют криминалистическую экспертизу, и поэтому особое внимание в докладе уделяется реализации криптографических механизмов безопасности для хранения пользовательских данных. При успешном извлечении данных с защищенного раздела можно организовать атаку перебором без участия смартфона и расшифровать раздел.

О применимости вероятностных методов в цифровой криминалистике (в том числе, в контексте правовой системы общего права)

***Гладышев Павел**, Университет Дублина, Ирландия*

Обзор принципов доказывания в состязательном разбирательстве и их применение к современным электронным доказательствам на примере информации из Google Location Services. Пример использования математического моделирования для анализа анализируемой системы. Пример использования вероятностной оценки для разработки алгоритма восстановления данных (DeCa).

Использование NTA-систем для форензики и Threat Hunting

***Гончаров Павел Игоревич**, руководитель направления ГосСОПКА, «Ростелеком-Солар»*

В докладе делается краткий экскурс в эволюцию современных высокоуровневых хакерских группировок, приводятся примеры их тактик, техник и процедур, которые свидетельствуют о необходимости повышения «площади» покрытия сетевого мониторинга. Делается вывод о недостаточности существующих источников на конечном оборудовании для выявления бокового передвижения злоумышленников по инфраструктуре, проведения расследований и проверки гипотез ThreatHunting. Показывается на примерах, как современные средства NTA могут добавить дополнительный контекст при расследовании киберинцидентов.

Контроль сотрудников в информационной среде компании

***Кандыбович Дмитрий Петрович**, генеральный директор, компания StaffCop*

Большая часть атак происходит изнутри корпоративной сети. Причинами здесь являются как умышленные, так и непредумышленные действия, в том числе неисполнение сотрудниками служебных обязанностей, использование ИТ-ресурсов в личных интересах, продажа конфиденциальной информации с целью получения прибыли, заражение рабочего ПК вредоносным ПО. Особенно эти угрозы актуальны в последнее время, из-за распространённости удалённой работы. На основании угроз, актуальных для любой организации, можно выявить функции, которыми должен обладать комплекс защиты информации: учет рабочего времени; контроль используемых ресурсов и интернет-трафика; контроль съёмных носителей; контроль доступа к файлам; контроль переписки; выявление нетипичного поведения, итд. В докладе будут раскрыты вопросы корреляции стоимости и технологий, отличия от классических систем DLP, «подводные камни», возникающие при внедрении и эксплуатации.

12:50 – 14:30 Закрытая секция АБИСС. Для представителей финансовых организаций. Часть I.

Зал «Сосновый»

Ассоциация пользователей стандартов по информационной безопасности АБИСС проводит Закрытую секцию для кредитных и некредитных финансовых организаций на площадке ежегодной конференции РусКрипто. Принять участие в секции и направить свои вопросы для обсуждения могут представители финансовых организаций, являющихся участниками Сообщества АБИСС. Информация о бесплатном присоединении к Сообществу на сайте Ассоциации АБИСС.

Ведущая: **Харыбина Анастасия Андреевна,** председатель Ассоциации АБИСС, директор по развитию AKTIV.CONSULTING

Эксперты:

- **Сычев Артем Михайлович,** первый заместитель директора департамента информационной безопасности, Банк России
- **Дудка Александр Борисович,** начальник отдела проверок Управления надзора и наблюдения, Банк России
- **Свинцицкий Антон Игоревич,** директор по консалтингу, ДиалогНаука
- **Царев Евгений Олегович ,** управляющий, RTM Group
- **Иванцов Александр Сергеевич,** старший инженер по защите информации, Deiteriy

Часть I - Разговор с регулятором

В рамках первой части Закрытой секции АБИСС состоится панельная дискуссия с участием представителей Департамента информационной безопасности Банка России, на которой будут обсуждаться вопросы обеспечения информационной безопасности финансовых организаций, опыт проведения киберучений, а также проблемы качества аудита информационной безопасности.

15:30 – 17:00 Секция «Требования к криптографическим средствам защиты информации»

Зал «Шишка»

Секция для разработчиков средств криптографической защиты информации и организаций, занимающихся внедрением и эксплуатацией российских СКЗИ.

Ведущий: **Петров Алексей Владимирович,** ФСБ России

Новые требования для российских разработчиков СКЗИ

Елистратов Андрей Алексеевич, *ФСБ России*

Детальный обзор новой редакции требований к средствам криптографической защиты информации, не содержащей сведения, составляющих государственную тайну.

Требования к средствам криптографической защиты информации, предназначенным для обеспечения защиты новых информационных технологий

Толстолуцкая Анастасия Васильевна, *ФСБ России*

Внедрение цифровых технологий в новые сферы жизни людей и бизнеса не укладывается в текущие требования к СКЗИ. В связи с этим для разных направлений развития цифровых решений регулятором утверждены специальные требования, такие как требования к некорректируемой регистрации информации, требования к защите квантовых технологий и т.п. Доклад будет посвящен определению роли и места СКЗИ в новых информационных технологиях и специфичных требований к ним.

Типовые правила пользования СКЗИ

Зинюк Борис Федорович, *ФСБ России*

В конце 2020 года технический комитет утвердил технические спецификации ТС 26.2.001-2020 «Состав и содержание правил пользования средств криптографической защиты информации». Доклад будет посвящен обзору данной технической спецификации и практике ее внедрения.

15:30 – 17:00 Секция «Перспективные решения российских разработчиков средств информационной безопасности»

Зал «Еловый»

Секция, посвященная продуктам и решениям российских разработчиков средств информационной безопасности. Подробные технические рассказы ведущих экспертов российских вендоров, презентации технологий, освещение новых тенденций и запросов рынка.

Ведущий: **Смирнов Николай Валерьевич,** директор по развитию продуктов, АО «ИнфоТеКС»

TLS ГОСТ - Прикладной, Мобильный, Серверный

Еранов Сергей Валерьевич, *начальник отдела разработки компонентов инфраструктуры открытых ключей, АО «ИнфоТеКС»*

В докладе рассказывается о продуктах компании «ИнфоТеКС», решающих задачи организации защищенных соединений по протоколу TLS с использованием российских криптографических алгоритмов. Будут представлены продукты как для конечных пользователей, так и для системных интеграторов и компаний-разработчиков.

Проблемы автоматизации учета СКЗИ в современных условиях и пути их решения

Акушевич Дмитрий Валерьевич, *технический директор Spacebit*

Современное развитие и изменение бизнес-процессов в значительной мере повысили потребность в СКЗИ и нагрузку на Органы Криптографической Защиты Информации организаций. Необходимость следовать требованиям регуляторов и сложность учета, особенно для территориально-распределенных организаций и организаций со сложной организационной структурой, в современных условиях – задачи, которые могут быть решены эффективной автоматизацией.

Программно-аппаратные решения Рутокен для мобильных платформ

Иванов Владимир Евгеньевич*, директор по развитию, компания «Актив»*

Рассказ о перспективных разработках компании «Актив» для мобильных операционных систем. Контактные и бесконтактные средства аутентификации и электронной подписи для смартфонов, планшетов и смарт-терминалов. Интеграционные решения и инструментарий для разработчиков продуктов информационной безопасности.

«Аврора» для ЭЦП - поддержка устройств электронной подписи в операционной системе «Аврора»

Караваев Алексей Владимирович*, ведущий аналитик, Открытая Мобильная Платформа*

Разработчики массовых мобильных операционных систем не уделяли внимания поддержке устройств электронной подписи, и как таковой альтернативы на рынке не было. Цель данного доклада – рассказать о поддержке электронной подписи в ОС «Аврора» и о новых возможностях, которые, в связи с этим возникают.

Особенности применения российских криптографических алгоритмов для аутентификации абонентов мобильных устройств с eSIM

Александров Сергей Викторович, *ООО «Системы практической безопасности»*

В настоящее время в сотовой связи для аутентификации мобильных устройств в сети используются зарубежные алгоритмы, такие как MILENAGE, TUAK, CAVE. В то же время, в РФ разработан протокол для аутентификации мобильных устройств на основе отечественной хэш-функции «Стрибог». Рассматриваются результаты макетирования реализации набора российских и зарубежных криптоалгоритмов в составе апплета аутентификации для нескольких типов eSIM (eUICC) и рассматриваются меры, использованные для оптимизации времени их выполнения.

15:30 – 17:00 Закрытая секция АБИСС. Для представителей финансовых организаций. Часть II.

Зал «Сосновый»

Ассоциация пользователей стандартов по информационной безопасности АБИСС проводит Закрытую секцию для кредитных и некредитных финансовых организаций на площадке ежегодной конференции РусКрипто. Принять участие в секции и направить свои вопросы для обсуждения могут представители финансовых организаций, являющихся участниками Сообщества АБИСС. Информация о бесплатном присоединении к Сообществу на сайте Ассоциации АБИСС.

Ведущая: **Харыбина Анастасия Андреевна,** Председатель Ассоциации АБИСС, директор по развитию AKTIV.CONSULTING

Эксперты:

- **Сычев Артем Михайлович,** первый заместитель директора департамента информационной безопасности, Банк России
- **Дудка Александр Борисович,** начальник отдела проверок Управления надзора и наблюдения,
- Банк России
- **Свинцицкий Антон Игоревич,** директор по консалтингу, ДиалогНаука
- **Царев Евгений Олегович ,** управляющий, RTM Group
- **Иванцов Александр Сергеевич,** старший инженер по защите информации, Deiteriy

Часть II - Практические аспекты

В рамках второй части команда экспертов в области информационной безопасности под управлением Ассоциации АБИСС поделится практическими советами по формированию и реализации дорожной карты по ИБ-комплаенсу на 2021-2022г.г. В рамках круглого стола будут рассмотрены следующие вопросы:

- Новые требования Банка России по защите информации для кредитных и некредитных финансовых организаций.
- Повышение эффективности работы сотрудников финансовых организаций за счет объединения аудитов. Опыт проведения аудитов по PCI DSS, SWIFT и ГОСТ 57580.
- Проведение анализа уязвимостей программного обеспечения на ОУД4. Область оценки и пути ее прохождения.
- Тестирование на проникновение и (или) анализ защищенности.
- Выбор мер защиты информации путем составления модели нарушителя и модели угроз для финансовой организации.
- Особенности проведения оценки соответствия. Как подготовиться и пройти оценку соответствия в эпоху дистанционной работы.

Принять участие в Закрытой секции и направить свои вопросы для обсуждения могут представители финансовых организаций, являющихся участниками Сообщества АБИСС. Информация о бесплатном присоединении к Сообществу на сайте Ассоциации АБИСС.

17:30 – 19:30 Секция «Криптография и информационная безопасность в банковской сфере»

Зал «Сосновый»

Обеспечение безопасности банковской деятельности и финансовых операций. Использование средств криптографической защиты информации в организациях кредитно-финансовой сферы. ИБ и криптография в платежных системах. Стандарты и требования.

Ведущие:

- **Сычев Артем Михайлович,** первый заместитель директора департамента информационной безопасности, Банк России
- **Простов Владимир Михайлович,** ТК 26
- **Голованов Владимир Борисович,** ТК 122

Требования к СКЗИ в национально значимых платежных системах и переход на отечественные криптографические решения в банковской сфере

Елистратов Андрей Алексеевич, *ФСБ России*

Доклад посвящен обзору требований предъявляемым к средствам криптографической защиты информации, которые должны использоваться в национально значимых платежных системах Российской Федерации и в банковской сфере в целом.

Платежные HSM: выполнение российских и международных требований

Простов Владимир Михайлович, *ТК 26*

Создание аппаратных модулей безопасности информационной инфраструктуры платёжных систем HSM, удовлетворяющих одновременно требованиям российских регуляторов и документов PCI HSM, а также способных полноценно заменить в начале 2024 года используемые в настоящее время в банках HSM иностранного производства, является крайне непростой задачей. Доклад посвящен задачам, возникающим на этом пути, а также путям их решения.

Практика получения одобрения (сертификации) банковского оборудования в международных платежных системах

Шибина Ольга Михайловна*, начальник отдела экспертизы, группа компаний Штрих-М*

Регулирование применения банковского оборудования в большинстве стран возложено на платежные системы. Доклад рассматривает установившиеся принципы регулирования и систему подтверждения соответствия требованиям (объединения участников рынка, авторизованные лаборатории, программы безопасности международных платежных систем). Роль государственных органов в регулировании сейчас и в будущем.

О становлении и развитии системы отраслевых стандартов безопасности финансовых (банковских) операций для инновационных финансовых технологий в России

Шумский Лев Станиславович, *директор по информационной безопасности, Ассоциация ФинТех*

Сейчас на российском рынке мы видим явный тренд на развитие экосистем, интерес к финансовым технологиям и оказанию финансовых услуг проявляют игроки из небанковского сектора. Безопасности обмена данными через открытые API уделяется пристальное внимание. После того, как в Евросоюзе была принята Вторая платежная директива, обязывающая банки открыть API, была создана международная рабочая группа Financial-grade API (FAPI), целью которой является разработка стандартов безопасного обмена данными через открытые API в финансовом секторе. Группа разработала свод правил, который сейчас имплементируют более 30 государств, развивающих открытый банкинг. В конце октября Банк России опубликовал стандарт информационной безопасности открытых API, который учитывает рекомендации FAPI, а также профильных технических комитетов ТК26 и ТК 122.

17:30 – 19:30 Секция «Криптография и криптоанализ», 1 часть

Зал «Еловый»

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

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Алексеев Евгений Константинович,** начальник отдела криптографических исследований, КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

Криптография как реализация полезных интерфейсов

Агиевич Сергей Валерьевич, *к.ф.-м.н., НИИ прикладных проблем математики и информатики Белорусского государственного университета*

Криптографическая система/алгоритм/протокол — это реализация полезного интерфейса: шифрование с секретным ключом, с открытым ключом, гомоморфное шифрование, etc. Задача криптографа – найти реализацию интерфейса, надежную и эффективную. Но на практике реализация не важна, программисты просто "дергают интерфейс". В докладе рассматривается трансформация и усложнение криптографических интерфейсов на примере стандартов РБ. Кроме этого, будет затронут редукционистский подход современной криптографии, согласно которому атака также описывается интерфейсом: если существует его реализация, то атаку можно превратить в алгоритм решения трудной задачи.

Открытое научное сотрудничество России и Франции в области криптографии и информационной безопасности

Коренева Алиса Михайловна*, к.ф.-м.н., компания «Код Безопасности»*

Фомичёв Владимир Михайлович*, д.ф.-м.н., профессор, Финансовый университет при Правительстве РФ, компания «Код Безопасности», ФИЦ ИУ РАН*

В докладе рассматривается опыт сотрудничества с французским научно-техническим журналом Journal of Computer Virology and Hacking Techniques (JICV), главный редактор – профессор Эрик Филиоль (Eric Filiol). Журнал выпускается всемирно известным издательством Springer и входит во второй квартиль (Q2) Scopus. В рамках проекта авторы доклада подготовили специальный выпуск “Special Issue: Russian Research in Cryptology and Information Security Systems”, посвящённый современным исследованиям российских ученых в области криптографии и информационной безопасности. Целью совместного проекта является повышение осведомлённости международного научного сообщества о российской исследовательской деятельности. В докладе анонсируются новые предложения Эрика Филиоля по подготовке специальных выпусков журнала JICV с результатами российских исследований.

Кандидат в национальные стандарты республики Казахстан – алгоритм шифрования Qalqan

Горлов Лев Владимирович*, Satbayev University, Казахстан*

Ибраев Ренат Булатович*, Satbayev University, Казахстан*

Рассказ про алгоритм блочного симметричного шифрования Qalqan разработанный в 2020 году Научно-исследовательской лабораторией информационной безопасности при Satbayev University в рамках программно-целевого финансирования Министерством цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Алгоритм блочного симметричного шифрования Qalqan выдвигается в качестве национального стандарта шифрования.

Шифрование носителей информации. Режим DEC

Богданов Дмитрий Сергеевич*, НИЯУ МИФИ*

Ноздрунов Владислав Игоревич*, ТК 26*

Освещаются вопросы обеспечения безопасности данных при их хранении на носителях информации с блочно-ориентированной структурой. Описываются типовые угрозы и модель нарушителя. Приводится описание нового режима работы блочных шифров для шифрования данных на носителях информации с блочно-ориентированной структурой.

Шифрование, сохраняющее формат – задачи, подходы, схемы

Алексеев Евгений Константинович*, начальник отдела криптографических исследований, КриптоПро*

Ахметзянова Лилия Руслановна*, заместитель начальника отдела криптографических исследований, КриптоПро*

Елистратов Андрей Алексеевич*, эксперт ТК 26*

Никифорова Лидия Олеговна*, инженер-аналитик, КриптоПро*

Данная работа посвящена такому направлению прикладной криптографии, как шифрование, сохраняющее формат (FPE). Задача построения таких схем имеет заметный практический интерес. Традиционно упоминаются задачи зашифрования некоторой базы данных, записи которой имеют фиксированный формат (например, дата и время или номер ИНН), и зашифрования номеров кредитных карт при проведении различных финансовых операций.

О программной реализации алгоритмов шифрования с аутентификацией

Нестеренко Алексей Юрьевич, *доцент кафедры Компьютерной безопасности МИЭМ НИУ ВШЭ*

Программные реализации существующих отечественных алгоритмов аутентифицирующего шифрования (MGM, ctr+cmac, ctr+hmac), особенности и результаты сравнения по скорости реализации, описание модификации алгоритма, разработанного автором. Будут рассмотрены вопросы, влияющие как на стойкость разработанного алгоритма, так и на его быстродействие.

О контроле целостности хранимых данных с использованием хэширования

Фомичёв Владимир Михайлович, *д.ф.-м.н., профессор, Финансовый университет при Правительстве РФ, компания «Код Безопасности», ФИЦ ИУ РАН*

Бобровский Дмитрий Александрович*, Финансовый университет при Правительстве РФ, компания «Код Безопасности»*

Задорожный Дмитрий Игоревич*, компания «Код Безопасности»*

Коренева Алиса Михайловна*, к.ф.-м.н., компания «Код Безопасности»*

Набиев Тимур Русланович*, компания «Код Безопасности»*

Описан способ встраивания высокопроизводительного алгоритма генерации кода контроля целостности, представленного авторами на РусКрипто'2020, в функцию хэширования, определенную в ГОСТ 34.11–2018 (256 бит). Представленные ранее результаты получили существенное развитие. Проведены экспериментальные исследования производительности и криптографических свойств нового алгоритма.

17:30 – 19:30 Круглый стол «Пространство доверия ЭП, ЭДО и цифровых услуг»

Зал «Стеклянный»

Ведущие:

- **Новиков Федор Вадимович,** начальник управления электронного документооборота, Федеральная налоговая служба
- **Малинин Юрий Витальевич,** президент Ассоциации «РОСЭУ»

Участники дискуссии:

- **Петров Михаил Викторович,** директор Департамента цифровой трансформации, Счетная палата Российской Федерации
- **Москалев Дмитрий Владимирович,** заместитель начальника РУЦ Республиканское унитарное предприятие «Национальный центр электронных услуг», Республика Беларусь
- **Тумель Сергей Александрович,** член Комитета по электронной торговле и логистике «Конфедерации Цифрового Бизнеса» Беларуси, партнер Европейской сети EDI-операторов EEDIN, Республика Беларусь
- **Кирюшкин Сергей Анатольевич,** советник генерального директора ООО «Газинформсервис», Ассоциация «РОСЭУ»
- **Ткаченко Елена Юрьевна,** руководитель проекта, Экспертный совет «Электронные документы» «Автоматизированное управление полномочиями. Готовность нормативная и техническая»

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

09:30 – 11:30 **Секция «Российская и международная стандартизация»**
Зал «Шишка»

Секция посвящена стандартизации криптографических алгоритмов, протоколов, технологий информационной безопасности и цифровых технологий в целом. В работе секции принимают участие эксперты ТК 26, ТК 194, ТК 098 , ТК 164 .

Ведущие:

- **Бондаренко Александр Иванович,** ТК 26
- **Смышляев Станислав Витальевич,** к.ф.-м.н., заместитель генерального директора, КриптоПро

Стандартизация IPlir: итоги и перспективы развития
***Шемякина Ольга Викторовна**, системный аналитик, АО «ИнфоТеКС»*
Доклад посвящен протоколу криптографической защиты IP-пакетов, который может применяться для создания виртуальных частных сетей. К особенностям протокола IPlir относятся простота, отсутствие установки соединения между двумя взаимодействующими узлами, поддержка различных ключевых систем и различных вариантов информационного взаимодействия. Протокол IPlir имеет более чем двадцатилетнюю историю и используется для защиты большого количества корпоративных и государственных информационных систем.

Разработка проекта МР «Доверенная третья сторона. Протокол проверки и удостоверения данных»
***Драло Мария Павловна**, руководитель группы, ООО «Газинформсервис»*
Доклад посвящен разработке проекта методических рекомендаций протокола проверки и удостоверения данных, описанию протокола проверки и удостоверения данных доверенной третьей стороны, выполняемым функциям, примерам его использования с применением российской криптографии.

Об участии российских специалистов в развитии протокола IPsec в IETF
***Смыслов Валерий Анатольевич**, архитектор системы, ЭЛВИС-ПЛЮС*
В докладе рассказывается о состоянии и перспективах развития протокола IPsec в IETF. В частности, делается краткий обзор основных направлений развития IPsec: противодействие квантовым компьютерам, использование постквантовых криптографических механизмов, защита широковещательного трафика. Особое внимание в докладе уделено той роли, которую в развитии протокола IPsec играют российские специалисты.

Криптографические аспекты протокола TSP
***Алексеев Евгений Константинович**, начальник отдела криптографических исследований, КриптоПро*
***Бабуева Александра Алексеевна**, старший инженер-аналитик, КриптоПро*
***Никифорова Лидия Олеговна**, инженер-аналитик, КриптоПро*
***Смирнов Павел Владимирович**, директор по развитию, КриптоПро*
Доклад посвящен стандартизируемому в настоящий момент в ТК 26 протоколу создания доверенных штампов времени (TSP). Будут описаны сам протокол, его современный статус в различных стандартизирующих организациях и типичные примеры применения. Отдельное внимание будет уделено его криптографическим свойствам.

Стандартизация российских криптографических механизмов в сетях связи 5G/IMT-2020: задачи, перспективы
***Грибоедова Екатерина Сергеевна**, руководитель направления стандартизации, АО «НПК «Криптонит»*
***Дрынкин Антон Викторович**, руководитель направления практической криптографии, АО «НПК «Криптонит»*

В ноябре 2020 года в рамках заседания Президиума Правительственной комиссии по цифровому развитию была утверждена дорожная карта развития мобильных сетей 5G. Целью данного проекта является ускорение развертывания телекоммуникационной сети нового поколения на базе отечественного оборудования. Важнейшей частью обеспечения технологической независимости такой сети является не только разработка российских аналогов криптографических алгоритмов, но и стандартизация данных механизмов как в России (в рамках ТК 26 и Росстандарта), так и в соответствующих международных организациях (3GPP, O-RAN и др.). В докладе будет рассказано о структуре и порядке функционирования основных стандартизирующих организаций в рассматриваемой области, а также о плане работ в направлении стандартизации российских криптографических механизмов в сетях связи 5G/IMT-2020, запланированных на 2021 год.

Актуальные проблемы стандартизации по управлению доступом и защите персональных данных

***Сабанов Алексей Геннадьевич**, заместитель генерального директора, АО «Аладдин Р.Д.»*

В отличие от защиты от НСД, по которой имеется обширная нормативная база, вопросы типовой архитектуры системы управления доступом в автоматизированных ИС различного назначения, применяемые модели разграничения доступа (кроме дискреционной, мандатной и ролевой) и механизмы авторизации не формализованы и не описаны. Для частичного восполнения данного пробела в настоящее время на основе ISO/IEC 29146 разрабатывается национальный стандарт. Также необходимо обсудить вопрос: готовы ли мы адаптировать международный опыт 20 стандартов по защите ПДн в систему ГОСТ Р и в какой степени.

Разработка проектов рекомендаций по стандартизации криптографических механизмов для реализации сервисов электронной коммерции в значимых платежных системах РФ

***Шкоркина Елена Николаевна**, ООО «Системы практической безопасности»*

Требования Банка России по постепенному внедрению российских криптографических алгоритмов диктуют необходимость разработки и стандартизации соответствующих криптографических механизмов, в том числе, для внедрения в сервисы электронной коммерции. В докладе будут рассмотрены следующие механизмы: формирование одноразовых паролей, метод управления ключами транзакции, а также формирование контейнера для передачи и безопасного хранения ключей и других чувствительных данных платёжных систем.

Особенности нормативного регулирования вопросов создания и применения систем ИБ на основе технологий искусственного интеллекта

***Гарбук Сергей Владимирович**, к.т.н., директор по научным проектам НИУ «Высшая школа экономики», председатель технического комитета по стандартизации ТК 164 «Искусственный интеллект»*

В докладе рассмотрены основные задачи информационной безопасности, эффективность решения которых может быть повышена с использованием методов искусственного интеллекта (ИИ). Сформулированы направления стандартизации в области создания и применения интеллектуальных систем информационной безопасности. Выявлены особенности стандартов, определяющих способы оценки соответствия интеллектуальных систем ИБ установленным требованиям. Показано, что применение предлагаемых стандартов позволит обеспечить гарантированный уровень качества таких систем.

Стандарты: как обеспечить глобальную бесшовность цифровых технологий

***Уткин Никита Александрович**, ТК 194*

Развитие цифровых технологий происходит в условиях повышенной конкуренции между корпорациями и сообществами, странами и регионами. При этом успех экспоненциального развития цифровых технологий кроется в подходах, основанных не только на самих технологиях, но и на степени их открытости. Открытые стандарты противопоставляют себя миру проприетарных решений, формируя вокруг себя платформенные решения и экосистемные кооперации. Об инструментарии стандартов для обеспечения бесшовности развития цифровых технологий, обеспечении совместимости и гармонизированности как на уровне страны и макрорегиона, так и на международном уровне пойдет речь в данном выступлении.

Национальная и международная нормативно-техническая база в области открытых испытаний биометрических технологий

***Николаев Данила Евгеньевич**, ТК 098*

***Мамаев Василий Юрьевич**, ТК 098*

Отсутствие открытых научных исследований и результатов испытаний, действующих/внедряемых биометрических систем не вызывает доверие у пользователей к технологии и, как следствие, к биометрической системе в целом и предоставляемому сервису/услуге. Зачастую при внедрении самой биометрической системы разработчики руководствуются только результатами технологических испытаний (тестирование алгоритма распознавания) и упускают из вида сценарные (тестирование макета системы с самозванцами и атаками на биометрические предъявление) и оперативные испытания (тестирование действующей биометрической системы с самозванцами и атаками на биометрические предъявление). Фактически биометрическая система может быть запущена в работу без тестирования известных видов атак на биометрическое предъявление. В рамках выступления будет уделено внимание национальной и международной нормативно-технической базе в области открытых испытаний биометрических технологий.

09:30 – 11:30 Секция «Криптография и криптоанализ», 2 часть

Зал «Еловый»

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Алексеев Евгений Константинович,** начальник отдела криптографических исследований, КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

О кодировках неабелевых 2-групп наложения ключа с циклической подгруппой индекса 2

***Пудовкина Марина Александровна**, д.ф.-м.н., профессор МГТУ им. Н.Э. Баумана*

Во многих блочных шифрсистемах используются просто реализуемые операции «сложения» в различных абелевых 2-группах. В данной работе для произвольной неабелевой 2-группы H с циклической подгруппой индекса 2 описываются групповые свойства биективного отображения v:H->{0,…,2^m-1}. Получены условия вложения v(H) в силовскую 2-подгруппу симметрической группы S_2^m, а также критерий примитивности группы, порожденной всеми подстановками из v(H). Приведены примеры «естественных» кодировок v и их свойства.

Поиск эффективно реализуемых подстановок с оптимальными криптографическими характеристиками

***Чичаева Анастасия Александровна**, младший специалист-исследователь лаборатории криптографии НПК «Криптонит», ВМК МГУ*

Работа сфокусирована на битовом представлении 4-битовых подстановок. Рассматривается подход к поиску эффективно реализуемых подстановок из 30 классов аффинной эквивалентности, для которых ранее не были обнаружены представители. Приведены примеры найденных подстановок с хорошими криптографическими и эксплуатационными характеристиками.

Разложение рекурсивных матриц и его применение к реализации XSL-схем

***Шишкин Василий Алексеевич,** специалист-исследователь лаборатории криптографии НПК «Криптонит»*

***Давыдов Степан Андреевич,** руководитель лаборатории криптографии НПК «Криптонит»*

В работе предложен общий вид разложения рекурсивных матриц. В некоторых частных случаях такого разложения предложены новые варианты реализации рекурсивных матриц. Для шифрсистемы Кузнечик приведена сводная таблица различных реализаций, включающая предлагаемые новые реализации.

Дешифруем или недешифруем шифр случайного гаммирования?

***Бабаш Александр Владимирович,** НИУ ВШЭ, РЭУ им. Г.В. Плеханова*

Считается, что шифр случайного гаммирования (ШСГ) недешифруем, так как он является совершенным шифром. Однако в докладе РусКрипто'2020 и МиТСОБИ 20 «Об одной атаке на модель шифров гаммирования» была представлена атака на ШСГ с расчетом трудоемкости и надежности. В данной статье обосновывается, что дешифруемость ШСГ, или недешифруемость зависит от выбора его математической модели. Дается формализация понятия дешифруемости шифра. Приводится новая атака на ШСГ, имеющая лучшие параметры, чем предложенные ранее атаки, имеющая возможности дальнейшего ее развития.

Алгоритм восстановления отдельных частей текстовых сообщений по информации о возможных вариантах его знаков

***Малашина Анастасия Геннадьевна**, Национальный исследовательский университет «Высшая школа экономики», Аспирантская школа по техническим наукам, специальность «Информационная безопасность»*

Исследование процедуры восстановления отдельных отрезков неизвестного исходного сообщения по информации о возможных вариантах каждого знака. Предлагается алгоритм, основанный на составлении словарей соответствующих длин, поиске участков текста с общим количеством вариантов знаков, не превосходящих заданную границу, и последующем переборе, и отсеве ложных вариантов словарных величин. Исследуются статистические свойства словарей текстов коротких длин, проводятся экстраполяционные оценки для текстов большой длины. Описаны основные математические свойства данного алгоритма. Проведены теоретические исследования эффективности рассматриваемой процедуры в рамках определенной теоретико-вероятностной модели.

Доказательство с нулевым разглашением для аутентификации в Мастерчейн

***Цветков Алексей Игоревич,** руководитель разработки платформы Мастерчейн, Ассоциация ФинТех*

Предлагается разработать альтернативные способы аутентификации и верификации записей в распределённом реестре, позволяющие сохранить анонимность автора. Протоколы доказательства с нулевым разглашением поддерживают данные свойства и в настоящее время имеют эффективные реализации для применения на практике. В докладе будет рассмотрен прототип доказательства с нулевым разглашением для аутентификации в приложениях на платформе Мастерчейн.

Квантовый алгоритм Саймона и его применение в задачах криптоанализа

***Денисенко Денис Витальевич**, МГТУ им. Н.Э. Баумана*

В докладе рассмотрены квантовый алгоритм Саймона, особенности его применения в моделях Q1 и Q2. Представлены примеры применения квантового алгоритма Саймона для поиска ключей в схеме Эвена-Мансура, верифицированные в квантовом симуляторе Quipper, на основании которых уточнены условия возможности применения квантового алгоритма Саймона, а так же комбинации квантовых алгоритмов Саймона и Гровера в задачах криптоанализа.

09:30 – 11:30 Секция «Перспективные подходы к обеспечению безопасности киберфизических систем»

Зал «Сосновый»

Ведущие:

- **Зегжда Дмитрий Петрович**, д.т.н., профессор РАН, директор Института кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого, Санкт-Петербург
- **Иванов Денис Вадимович**, к.т.н. ООО «НеоБИТ», Санкт-Петербург

Современные вызовы и тенденции развития подходов к обеспечению информационной безопасности киберфизических систем

***Иванов Денис Вадимович**, к.т.н., руководитель проектов, ООО «НеоБИТ», Санкт-Петербург*

В докладе рассматриваются новые вызовы информационной безопасности, продиктованные глобальными событиями современного мира. Поднимается вопрос обеспечения безопасности и готовности существующей инфраструктуры к переходу к дистанционным форматам обучения, работы, взаимодействия с государственными структурами и др. Описываются современные подходы к построению и обеспечению киберустойчивости информационных систем.

Выявление аномалий в работе киберфизических систем на основе механизма гиперкуба

***Фатин Александр Денисович**, ассистент, Санкт-Петербургский Политехнический университет Петра Великого, Санкт-Петербург*

В работе рассматривается метод выявления аномального поведения в работе киберфизических систем с помощью предсказания и анализа многомерных временных рядов средствами нейроэволюционных алгоритмов на основе развития субстрата гиперкуба. Метод основан на выявлении отклонений между текущими значениями состояния КФС и предсказанных гиперкубом результатов. Приводятся результаты исследований описанного метода, демонстрирующие корректность и точность его работы. Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1689.2019.5.

Противодействие информационным угрозам с использованием honeypot-систем на основе графа потенциальных атак

***Завадский Евгений Владимирович**, специалист по ИБ, ООО «Лаборатория кибербезопасности», Санкт-Петербург*

В работе предложен метод построения Honeypot-системы на основе графа потенциальных атак, реализован прототип данной системы на базе гипервизора KVM и проведено сравнение ее ресурсозатрат с традиционной Honeypot-системой.

Интенционно-ориентированные сети: угрозы безопасности и возможные подходы к защите

***Попова Елена Александровна**, ассистент, Санкт-Петербургский Политехнический университет Петра Великого, Санкт-Петербург*

Рассмотрены назначение и основные характеристики интенционно-ориентированных сетей (Intent-Based Networking, IBN). Выделены основные отличия IBN от традиционного подхода к построению сетевых архитектур, сформулированы основные преимущества использования IBN. Проанализированы актуальные исследования в области обеспечения безопасности таких сетей, выделены основные проблемы безопасности, возникающие при переходе к построению сетевых инфраструктур к парадигме IBN. Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1932.2019.5.

11:50 – 13:10 Секция «Информационная безопасность и криптография в государственных информационных системах»

Зал «Шишка»

Государство – один из главных заказчиков решений в области информационной безопасности. Процессы цифрового преобразования государственного управления и реализации национальной программы «Цифровая экономика Российской Федерации» ставят новые вызовы перед игроками рынка информационной безопасности. Растет масштаб проектов, повышаются требования. Какие значимые проекты идут уже сейчас и что ожидается в ближайшем будущем. Что разработчики и интеграторы в области информационной безопасности могут сделать в государственных проектах.

Ведущие:

- **Пьянченко Андрей Андреевич,** заместитель директора НИИ «Восход»
- **Горелов Дмитрий Львович**, управляющий партнер компании «Актив», директор ассоциации «РусКрипто»

Требования о защите информации, содержащейся в государственных информационных системах, с использованием средств криптографической защиты информации

***Петров Алексей Владимирович,** ФСБ РФ*

Обзор новых требований к СКЗИ в государственных информационных системах.

Перспективные планы по развитию института усиленной электронной подписи для взаимодействия граждан и государства

***Пьянченко Андрей Андреевич,** заместитель директора НИИ «Восход»*

В докладе будет рассказано о планах по созданию единого цифрового контура идентификации в масштабе страны, о вариантах выдачи и применения неквалифицированной электронной подписи для получения государственных и муниципальных услуг. Будут освещены перспективные проекты по массовому применению квалифицированной усиленной электронной подписи гражданами России.

Технология дистанционной идентификации личности в УЦ с использованием заграничного паспорта

***Чижевский Игорь Евгеньевич**, заместитель руководителя департамента по вопросам технического развития разрабатываемых продуктов, НИИ «Восход»*

Рассказ о технологии идентификации личности гражданина при помощи заграничного паспорта, содержащего электронный носитель информации.

Как организовать защищенный удаленный VPN-доступ к корпоративным ресурсам с учетом требований законодательства и не переплатить?

Луцик Павел Иванович, *директор по продажам и развитию бизнеса, КриптоПро*

Особенности организации защищенного, с учетом требований законодательства РФ по информационной безопасности, VPN-доступа к корпоративным ресурсам с сохранением инвестиций, вложенных в ИТ-инфраструктуру и лицензии на СКЗИ, а также вопросы организации безопасного доступа к веб-сайтам по протоколу TLS с ГОСТ.

Сложность выявления семантических доменов или как понять какие данные необходимо обезличивать

Татевосян Айк*, руководитель департамента цифровой трансформации, Crosstech Solutions Group*

Обезличивание данных, в том числе персональных и чувствительных, является крайне важной процедурой при проведении различного рода работ, особенно в государственных информационных системах. Однако часто, в высоконагруженных и распределенных решениях невозможно однозначно сказать где именно и какие данные хранятся. Для определения именно тех типов данных, которые необходимо обезличивать используются инструменты семантического и контекстного анализа данных, определяющих соответствующие семантические домены. Они позволяют предварительно проверить источники на наличие коллизий и несоответствий в семантике данных и названиях полей в таблицах и индексах, выявить семантические коллизии и сформировать перечень данных, необходимых к обезличиванию.

11:50 – 13:10 Секция «Криптография и криптоанализ», 3 часть

Зал «Еловый»

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Алексеев Евгений Константинович,** начальник отдела криптографических исследований, КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

Оценка эффективности атаки «Trojan Horse» для протокола квантового распределения ключей на геометрически однородных квантовых состояниях

Гузаирова Диана Маратовна, *специалист, ООО «СФБ Лаб»*

Сущев Иван Сергеевич, *специалист, ООО «СФБ Лаб»*

В докладе рассматривается способ оценки эффективности атаки «Trojan Horse» для протокола квантового распределения ключей (КРК) на геометрически однородных квантовых состояниях. Предложена методика расчета вероятности различения злоумышленником квантовых чистых состояний и методика оценки защищенности систем КРК от атаки «Trojan Horse», позволяющая экспериментально определить среднее число фотонов в отраженном сигнале.

Форзиция: протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых

Гребнев Сергей Владимирович, QAPP

Ключарёв Петр Георгиевич, к.т.н., МГТУ им. Н.Э. Баумана

Коренева Алиса Михайловна, к.ф.-м.н., компания «Код Безопасности»

Кошелев Дмитрий Игоревич, Télécom Paris, АО «ИнфоТеКС»

Тараскин Олег Геннадьевич, Waves Enterprise

Тулебаев Азат Ирикович, компания «Код Безопасности»

В докладе описывается проект квантово-устойчивого протокола выработки общего ключа “Форзиция”, разработанного в рамках деятельности рабочей подгруппы по изогениям суперсингулярных эллиптических кривых РГ 2.5 «Постквантовые криптографические механизмы» ТК26. Рассматриваются необходимые математические определения, описан протокол, дается обоснованный выбор его параметров.

Применение альтернативных моделей эллиптических кривых в криптографии на основе изогений
***Гребнев Сергей Владимирович**, QApp*
***Тулебаев Азат Ирикович**,компания «Код Безопасности»*
В докладе рассматриваются эллиптические кривые, представленные в форме Монтгомери, Эдвардса и Хаффа. Проводится сравнительный анализ этих представлений с точки зрения эффективности их применения в криптографических схемах, основанных на математическом аппарате изогений суперсингулярных эллиптических кривых.

Схема постквантовой электронной подписи на основе протокола идентификации Штерна
***Высоцкая Виктория Владимировна**, АО НПК «Криптонит»*
***Чижов Иван Владимирович**, АО НПК «Криптонит»*
В работе представлена схема электронной подписи, построенная с помощью применения преобразования Фиата-Шамира к схеме идентификации Штерна. Предложено два алгоритма выбора параметров подписи. Первый основан на использовании теории доказуемой стойкости, а второй — учитывает только известные в настоящий момент атаки. В зависимости от требуемого уровня стойкости на основе алгоритмов выбора были построены наборы параметров для практического использования схемы.

Доказательство подделки подписей на основе хэш-функций
***Киктенко Евгений Олегович**, Российский Квантовый Центр, МИАН им В.А. Стеклова РАН, МФТИ*
***Кудинов Михаил Александрович**, Российский Квантовый Центр, МГТУ им. Н. Э. Баумана*
***Федоров Алексей Константинович**, Российский Квантовый Центр, МФТИ*
В работе исследуется свойство подписей на основе хэш-функций, позволяющее детектировать их подделку. Это свойство основывается на том факте, что успешная подделка подписи на основе хеш-функции со значительной вероятностью приведет к коллизии в отношении используемой хеш-функции, в то время как демонстрация этой коллизии может служить убедительным доказательством подделки. Доказывается, что при правильно настроенных параметрах, схемы одноразовых подписей Лампорта и Винтерница могут демонстрировать свойство возможности обнаружения подделок. Это свойство имеет большое значение в рамках парадигмы крипто-гибкости, поскольку рассматриваемое обнаружение подделки служит сигналом тревоги о том, что используемая функция криптографического хеширования становится небезопасной для использования и соответствующая схема должна быть заменена.

11:50 – 13:10 Секция «Развитие высокотехнологичной области «Квантовые коммуникации» 1 часть

Зал «Сосновый»

Ведущие:

- **Глейм Артур Викторович**, директор департамента квантовых коммуникаций ОАО «РЖД»
- **Уривский Алексей Викторович,** заместитель генерального директора по науке и инновациям, АО «ИнфоТеКС»

Приветственные слова

Стратегия развития ОАО «РЖД» по направлению «Квантовые коммуникации» и ее соотношение с существующими достижениями в отрасли
***Глейм Артур Викторович**, директор департамента квантовых коммуникаций, ОАО «РЖД»*

Квантовое распределение ключей через атмосферные каналы связи
***Кулик Сергей Павлович,** д.ф-м.н., профессор кафедры квантовой электроники, МГУ имени М.В. Ломоносова*

Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации (ProtoQa)
***Бородин Михаил Алексеевич**, старший исследователь, центр научных исследований и перспективных разработок, АО «ИнфоТеКС»*
***Науменко Антон Павлович,** руководитель направления, отдел специальных исследований и разработок, АО «ИнфоТеКС»*

Маршрутизация в волоконно-оптических сетях квантового распределения ключей
***Хоружников Сергей Эдуардович**, руководитель ЛИЦ НЦКИ ФГАОУ ВО «Национальный исследовательский университет ИТМО»*

Безопасность квантово-криптографических ключей при их масштабировании
***Молотков Сергей Николаевич**, ведущий научный сотрудник Центра квантовых технологий Физического факультета МГУ имени М.В. Ломоносова*

Внедрение и коммерциализация сервисов квантовых коммуникаций на рынках информационных технологий
***Болтрушевич Константин,** советник директора по развитию отраслевых решений АО «Компания ТрансТелеКом»*

Построение квантово-криптографических средств защиты информации класса КА
***Букин Евгений Геннадьевич**, Заместитель генерального директора, ООО «Криптософт»*

13:30 – 14:30 Круглый стол «Проблемы обезличивания персональных данных»

Зал «Шишка»

Круглый стол, посвященный подходам к обезличиванию персональных данных. В дискуссии примут участие эксперты в области защиты информации, криптографии и крупные операторы, обрабатывающие большие массивы персональных данных, представители регуляторов. За последний год тематика обезличивания стала одним из основных трендов при обсуждении вопросов оборота и защиты персональных данных. Участники круглого стола постараются ответить на вопросы: что такое обезличивание и как оно может (и может ли вообще) защитить персональные данные пользователей, почему его использование может быть интересным операторам персональных данных и осуществляется ли оно в настоящее время, каковы перспективы использования, какие существуют требования и подходы к обезличиванию и насколько они практически осуществимы, каково влияние обезличивания на обработку больших данных методами искусственного интеллекта.

Ведущий: **Маршалко Григорий Борисович,** ФСБ России
Эксперты круглого стола:

- **Орехович Александра Владимировна,** директор по правовым инициативам Фонда развития интернет-инициатив
- **Шишмарев Владислав Борисович,** директор департамента управления данными ГКУ «Инфогород»
- **Бодров Александр Геннадьевич,** ФСБ России
- **Левова Ирина Юрьевна,** Директор по стратегическим проектам Ассоциации больших данных

13:30 – 14:30 Секция «Российская электроника и информационная безопасность»

Зал «Еловый»

Обсуждение вопросов совершенствования механизмов безопасности в российских процессорах и микроконтроллерах. Оптимизации российских криптографических алгоритмов, разработка российских микросхем с расширенными криптографическими возможностями и перспективными механизмами обеспечения информационной безопасности. Открытая дискуссия разработчиков средств ИБ и производителей электроники.

Ведущий: **Карантаев Владимир Геннадьевич,** к.т.н., ведущий менеджер продуктов, Лаборатория Касперского

Перспективы аппаратного ускорения криптографии в процессорах архитектуры «Эльбрус»
***Советов Петр Николаевич**, АО «МЦСТ», РТУ МИРЭА*
Приводятся оценки производительности программных реализаций криптографических алгоритмов российских стандартов в современных процессорах архитектуры «Эльбрус». Рассматриваются вопросы выбора перспективных криптографических алгоритмов и способы их аппаратного ускорения в новых поколениях архитектуры «Эльбрус». Предлагаются методы автоматизации синтеза криптографических команд.

Высокопроизводительные реализации алгоритмов шифрования Кузнечик и Магма на российских процессорах с учётом архитектурных особенностей.

***Русев Андрей Андреевич**, начальник отдела системных разработок, КриптоПро*

***Сонина Лолита Александровна**, начальник отдела криптографических разработок, КриптоПро*

***Щербаков Дмитрий Андреевич**, инженер-программист, КриптоПро*

В докладе проводится обзор особенностей архитектуры процессоров Эльбрус в контексте высокопроизводительной программной реализации ГОСТ алгоритмов симметричного шифрования. Обсуждаются возможности процессоров в сравнении с семейством x86. В работе представлены результаты практической реализации алгоритмов Кузнечик и Магма на процессорах Эльбрус нескольких актуальных поколений в составе провайдера. Полученные результаты превосходят по производительности все известные реализации на архитектуре AMD64/Intel64 с использованием расширений AVX/AVX2.

Повышение защищённости доверенного хранилища GPD Trusted Storage на основе технологии ARM TrustZone и особенностей архитектуры СнК с ядрами ARM v.8

***Самоделов Андрей Сергеевич**, системный аналитик, Лаборатория Касперского*

В докладе рассмотрены результаты исследований и проектирования архитектуры системы управления ключами и секретами на основе Доверенного Хранилища в соответствии со спецификацией GP Trusted Storage. Для повышения защищённости операций используется СнК с кластером ядер ARM и расширениями безопасности. Такая архитектура позволяет изолировать среду общего назначения от доверенной среды исполнения криптографических операций. Для большей защищённости, в архитектуру добавлен дополнительный изолированный контур, который предназначен для генерации ключей, доверенного хранения/экспорта/импорта системных криптографических ключей, а также изоляции самих системных ключей и операций с ними. Предлагаемый подход может служить для уменьшения времени при разработке ПО для ПАК СЗИ, может использоваться для в текущих и будущих проектов на базе российских микропроцессоров и микроконтроллеров построенных на ARM-архитектуре.

Отечественные системы на кристалле от АО НПЦ «ЭЛВИС» с доверенным ядром

***Кузнецов Денис Александрович**, АО НПЦ «ЭЛВИС»*

13:30 – 14:30 Секция «Развитие высокотехнологичной области «Квантовые коммуникации» 2 часть

Зал «Сосновый»

Панельная дискуссия

Ведущий: **Макаров Валентин Леонидович,** президент НП «РУССОФТ»

Эксперты панельной дискуссии:

- **Глейм Артур Викторович**, ОАО «РЖД»
- **Уривский Алексей Викторович**, «ИнфоТеКС»
- **Хоружников Сергей Эдуардович**, Национальный центр квантового интернета НИУ ИТМО
- **Молотков Сергей Николаевич**, Физический факультет МГУ им. Ломоносова
- **Букин Евгений Геннадьевич**, ООО «Криптософт»
- **Кулик Сергей Павлович,** МГУ имени М.В. Ломоносова
- **Качалин Алексей Игоревич,** ПАО «Сбербанк»
- **Беловолов Андрей Михайлович,** ФСБ России
- **Матвеев Евгений Анатольевич,** ООО НТП «Криптософт»

15:30 – 17:00 Круглый стол «Технологии дистанционного электронного голосования. Задачи и перспективы»

Зал «Шишка»

Обсуждение путей повышения безопасности систем дистанционного голосования. Использование российских криптографических алгоритмов и протоколов в разрабатываемых решениях для осуществления электронного голосования. Текущие наработки и будущие проекты. Перспективы использования дистанционного электронного голосования в коммерческих и государственных проектах.

Ведущие:

- **Шумский Лев Станиславович,** директор по информационной безопасности, Ассоциация ФинТех
- **Смышляев Станислав Витальевич**, к.ф.-м.н., заместитель генерального директора, КриптоПро

Эксперты круглого стола:

- **Шишкин Василий Алексеевич,** руководитель лаборатории криптографии, АО НПК «Криптонит»
- **Калихов Артем Владимирович,** директор по продукту Waves Enterprise
- **Елистратов Андрей Алексеевич,** ФСБ России
- **Сазонов Александр Валентинович,** руководитель проекта Polys, Лаборатория Касперского
- **Сатиров Юрий Константинович,** заместитель генерального директора, РТЛабс
- **Шишмарев Владислав Борисович**, директор департамента управления данными ГКУ «Инфогород»
- **Грицай Георгий Анатольевич**, ЦИК России

15:30 – 17:00 Секция «Криптография и криптоанализ», 4 часть

Зал «Еловый»

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Алексеев Евгений Константинович,** начальник отдела криптографических исследований, КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

Стойкость алгоритма Кузнечик к обобщенной инвариантной атаке

Фомин Денис Бонславович, *Национальный исследовательский университет «Высшая школа экономики»*

В работе рассматривается один подход к построению инвариантных множеств раундовых преобразований отечественного стандарта шифрования «Кузнечик». Данный подход основывается на свойствах нелинейного слоя шифра. Приведен алгоритм нахождения инвариантных множеств в общем случае, а также экспериментальные результаты применительно к алгоритму «Кузнечик».

О вычислительных подходах к оценке вероятности дифференциалов в низкоресурсных XSPL-преобразованиях

Кирюхин Виталий Александрович*, старший специалист, АО «ИнфоТеКС»*

Рассматриваются вычислительные подходы к оценке стойкости низкоресурсных XSPL-преобразований к дифференциальному криптоанализу. Предложены алгоритмы для получения верхней оценки на максимальную вероятность (MEDP) дифференциала – совокупности дифференциальных путей. Соответствующие значения вычислены для низкоресурсной 64-битной хэш-функции (РусКрипто'2020) и 100-битного преобразования хэш-функции PHOTON.

Об одном подходе к оценке вероятности усеченных дифференциалов в низкоресурсной хэш-функции «Мора»

***Бондакова Ольга Сергеевна**, РТУ МИРЭА*

На «РусКрипто'2020» была представлена низкоресурсная хэш-функция «Мора», предназначенная для обеспечения контроля целостности данных в каналах связи полевых устройств автоматизированных систем управления технологическим процессом. Анализ такой хэш-функции может быть сведен к анализу блочного шифра, на котором основана её функция сжатия. Одним из методов, применяемых для оценки стойкости блочных шифров, является дифференциальный метод криптографического анализа. Доклад посвящен исследованию возможности применения подходов предложенных Eichlseder M., Leander G., Rasoolzadeh S для анализа хэш-функции «Мора» и модификации их с учётом особенностей строения соответствующего блочного шифра. Приведена оценка трудоемкости вычисления EDP для усеченного дифференциала, подходящего для построения коллизии и успешности атаки поиска коллизий для сообщения, отличающихся в малом количестве полубайт, что является наиболее актуальным в рассматриваемой модели угроз, характерной для области применения хэш-функции «Мора».

Об уязвимостях протокола интернета вещей NB-Fi в новом проекте национального стандарта

***Ноздрунов Владислав Игоревич**, ТК 26*

Описываются уязвимости MAC-уровня протокола NB-Fi, описанного в проекте национального стандарта, которые могут привести к нарушению работы устройств в системе, навязыванию ложной информации, нарушению конфиденциальности передаваемой информации.

Использование атрибутной подписи в двухуровневой информационной системе с динамической структурой

***Беззатеев Сергей Валентинович**, д.т.н., Санкт-Петербургский Государственный Университет Аэрокосмического Приборостроения*

Рассматривается информационная система с динамической структурой, состоящая из узлов (устройств, элементов) двух типов, образующих два уровня. Узлы первого уровня получают, собирают и обрабатывают информацию. Устройства второго уровня образуют распределенную систему, использующую криптографические протоколы на базе атрибутов и обеспечивающую верификацию передаваемой информации. При этом для предотвращения сговора узлов второго уровня для каждого сеанса верификации выполняется протокол голосования, использующий атрибуты текущего сеанса.

15:30 – 17:00 Секция «Блок гуманитарных вопросов»

Зал «Сосновый»

Секция, посвященная важным нетехническим аспектам ведения деятельности и защиты интересов бизнеса в высокотехнологических отраслях – взаимоотношениям с государственными органами, охране интеллектуальной собственности и методам информационного противоборства в цифровой среде.

Ведущие:

- **Аронова Александра Сергеевна**, заместитель генерального директора по взаимодействию с органами государственной власти АО «ГЛОНАСС»
- **Елисеев Игорь Юрьевич,** заместитель директора по развитию Академии Информационных Систем

Полезные советы по GR для высокотехнологичных компаний

***Аронова Александра Сергеевна**, заместитель генерального директора по взаимодействию с органами государственной власти АО «ГЛОНАСС»*

Что такое Government Relationship (GR) для многих уже не секрет, но вот нужно ли системно выстраивать взаимоотношения с государственными органами компаниям, работающим на рынке ИТ/ИБ, зачем и как это делать – ответы на эти вопросы пока мало кто знает. Между тем, отрасли ИТ и ИБ все сильнее зависят от государства, поэтому роль GR в высокотехнологичных компаниях трудно переоценить. GR – история не о том, как выиграть тендер, а о легальных долгосрочных преференциях. Мы обсудим стратегию GR на сильно регулируемых рынках; болевые точки корпоративного имиджа и социальной ответственности; особенности выстраивания отношений с властями на федеральном и региональном уровнях.

Охрана интеллектуальной собственности в сфере ИТ и ИБ

***Благополучная Камила Владимировна**, юрист, патентный поверенный, член Ассоциации юристов России и международных организаций по охране интеллектуальной собственности AIPPI, LES, INTA, ADVOC*

Сегодня ясно, что без должной правовой охраны интеллектуальной собственности выход компании на рынок с новым продуктом или технологией чреват неблагоприятными правовыми последствиями: нарушение прав третьих лиц, копирование технологий, контрафакт, незаконное использование бренда или домена, утечка данных, захват бизнеса и др. На выступлении будут затронуты вопросы охраны интеллектуальной собственности и конфиденциальной информации организаций, выстраивания взаимоотношений работодателя и автора-разработчика технологий с точки зрения правовых механизмов, а также использования дополнительных мер технической защиты для предотвращения утечек данных наиболее чувствительной информации.

Информационные войны в цифровом мире

***Масалович Андрей Игоревич**, к.ф-м.н., ведущий эксперт по конкурентной разведке и OSINT Академии Информационных Систем*

Цифровой век существенно изменил привычные методы информационного противоборства на рынке. Раньше популярным инструментом был «черный пиар», распространяемый в официальных СМИ. Сейчас информационные атаки начинаются с социальных сетей, развиваются очень стремительно и способны нанести огромный ущерб репутации компании, если их не выявить и не купировать в самом зародыше. Для этого существует ряд специальных инструментов, позволяющих реализовывать как оборонительную, так и наступательную тактику противоборства.

17:30 – 19:30 Секция «Информационная безопасность и криптография в робототехнических системах»

Зал «Еловый»

Робототехнические комплексы и системы с каждым годом все шире применяются государством и бизнесом. Беспилотные летательные аппараты и наземные робототехнические комплексы решают сложные задачи, обрабатывают и передают чувствительную информацию. Оператору данных систем нельзя допускать потери управления и несанкционированного доступа к информации объекта, который находится в открытом пространстве. Такие системы предъявляют повышенные и во многом специфические требования к механизмам криптографической защиты и к информационной безопасности в целом.

Ведущий: **Новиков Владимир Александрович,** д.т.н., директор по разработке, производству и испытаниям, АО «Технологии Радиоконтроля»

Особенности разграничения прав доступа в автономной группировке беспилотных летательных аппаратов

***Куракин Александр Сергеевич**, к.т.н, заместитель директора ООО «Специальный технологический центр» по ТЗИ*

Высокотехнологичность полезных нагрузок размещаемых на БЛА, способных осуществлять первичную и вторичную обработку получаемых данных, зачастую требует обеспечения информационного взаимодействия между ними с учетом требований по защите информации. Сложность процессов управления указанными полезными нагрузками заставило ввести понятие виртуального экипажа, наделяемого перечнем допустимых функций. Рассматривается подход решения актуальной проблемы разграничения прав доступа внутри автономной группировки БЛА.

Особенности внедрения средств криптографической защиты информации в робототехнические комплексы с беспилотными летательными аппаратами малой дальности

***Поликарпов Александр Алексеевич**, начальник отдела ООО «Специальный технологический центр»*

Имеющаяся фактография многочисленных инцидентов, связанных с атаками на информационную систему робототехнического комплекса с беспилотным летательным аппаратом малой дальности (БЛА МД), направленные на нарушение функционирования, компрометацию передаваемой информации и завладение техническими средствами показали, что одной из наиболее актуальных задач при разработке БЛА МД является внедрение средств криптографической защиты информации (СКЗИ), обеспечивающих не только сохранение информации, но безопасное взаимодействие элементов робототехнической системы в целом. Рассматривается методология формирования единого подхода к построению топологии сети, алгоритмов обработки информационных потоков, унификации физических и логических интерфейсов сопряжения электронного оборудования БЛА МД с СКЗИ.

Имитозащита радиоканалов робототехнических комплексов на основе теоретико-числовых преобразований в комплексной плоскости

***Самойленко Дмитрий Владимирович**, заместитель начальника кафедры краснодарского ВВУ имени генерала армии С.М.Штеменко*

Недостатки современных шифров, применяемых в радиоканалах - отсутствие комплексного обеспечения классических требований: криптостойкости, помехоустойчивости и имитостойкости. Существующие методы противодействия имитации злоумышленника, такие как: выработка имитовставки или хэш-кода, использование режимов шифрования, таких как гаммирование с обратной связью в полной мере не решают этой задачи, поскольку осуществляют функцию контроля, сводящуюся к установлению различий между информационными объектами и не отражают регенеративного механизма восстановления искаженных данных. Предлагаемое решение для РТК основывается на использовании системы криптокодового преобразования информации (криптокодовых конструкций), синтез которых основан на агрегированном применении сертифицированных блочных шифров и кодов системы остаточных классов».

Способ сопряжения сетей разного уровня «открытости», организованных робототехническими комплексами и системами

***Полегенько Анастасия Михайловна**, начальник отдела ООО «Специальный технологический центр»*

Развитие робототехнических комплексов (РТК) определялось решаемыми ими задачами, полученные достижения определили необходимость учёта требований по защите информации, а существующие решения по защите информации не учитывают специфику РТК, даже если массо-габаритные размеры и условия функционирования РТК позволяют использовать сертифицированные отечественные решения по ЗИ, то как таковых, решений обеспечивающих выполнение комплекса всех требований, в данный момент, еще не существует и их предстоит разрабатывать. Рассматривается подход по выполнению первоочередных требований, предъявляемых к РТК».

Особенности защиты информации от утечки по техническим каналам в робототехнических комплексах

***Шенчелов Федор Петрович**, начальник отдела АО «Технологии радиоконтроля»*

Самые передовые многофункциональные решения стали основой современных малых робототехнических комплексов (РТК) БЛА в которых из-за ограничений фюзеляжного пространства и требования обеспечения температурных режимов блоки устанавливаются без корпуса, что вывело практически на первый план проблему электромагнитной совместимости и электромагнитных излучений, особенно в вопросе защиты информации от утечек по техническим каналам. Рассматривается подход решения проблемной ситуации по защите информации на борту БЛА.

Обеспечение защиты информации в системе цифровых пространственных моделей местности

***Назаров Михаил Сергеевич**, к.т.н., начальник лаборатории АО «Институт телекоммуникаций»*

Формирование цифровых пространственных моделей местности с разрешением необходимым для строительства и выполнения другой деятельности с применением БЛА требует учета положений по защите информации предъявляемых к формируемым моделям. Рассматриваются проблемные вопросы формирования и передачи моделей местности и подходы по их решению».

17:30 – 19:30 Секция «Перспективные исследования в области кибербезопасности»

Зал «Сосновый»

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

Ведущий: **Котенко Игорь Витальевич,** д.т.н., профессор, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности, СПб ФИЦ РАН

Методика раннего обнаружения кибератак на компьютерные сети

***Котенко Игорь Витальевич**, д.т.н., профессор, СПб ФИЦ РАН*

***Саенко Игорь Борисович**, д.т.н., профессор, СПб ФИЦ РАН*

***Крибель Александр Михайлович**, военная академия связи им. С.М. Буденного*

***Лаута Олег Сергеевич**, д.т.н., Военная академия связи им. С.М. Буденного*

Рассматривается методика обнаружения кибератак, основанная на выявлении аномалий в сетевом трафике на основе оценки его свойства самоподобия, идентификации в аномалиях кибератак, их классификации и принятии контрмер. Методика базируется на использовании методов фрактального анализа, математической статистики и нейронных сетей с долгой краткосрочной памятью. Рассмотрены вопросы программной реализации предлагаемой системы и формирования набора данных для проведения экспериментов. Экспериментальные результаты продемонстрировали достаточно высокую эффективность предлагаемой методики при обнаружении кибератак и выработке контрмер.

Методы противодействия разведывательному этапу сетевого вторжения

***Сагатов Евгений Собирович**, к.т.н., доцент, НИУ «Высшая школа экономики»*

***Майхуб Самара**, Самарский национальный исследовательский университет им. С.П. Королева*

***Сухов Андрей Михайлович**, д.т.н, профессор, МИЭМ, НИУ «Высшая школа экономики»*

Представляется метод противодействия начальному этапу любой сетевой атаки, на котором производится сканирование портов. Для того, чтобы разработать алгоритмы определения IP-адресов, с которых ведется сканирование, формулируются квалификационные признаки. Данные квалификационные признаки были положены в основу разработанных алгоритмов для созданных специализированных программных продуктов. Один из этих продуктов реализован в виде Linux утилиты, другой представляет собой SDN-модуль. Для того, чтобы понять эффективность защиты с помощью разработанных программных комплексов была проведена серия тестов. Предполагается, что спектр действия программных комплексов не ограничен только сканированием портов. Эти комплексы могут быть применены против различных типов атак, например, DDoS атак по типу TCP и UDP флуда.

Выявление скрытых ботов в социальных сетях

***Чечулин Андрей Алексеевич**, к.т.н., доцент, ИТМО*

***Коломеец Максим Вадимович**, ИТМО*

Обнаружение ботов в социальной сети является сложной задачей, особенно если данные их профилей скрыты настройками приватности. В докладе рассматривается подход к обнаружению ботов, основанный на анализе косвенных данных о профиле, скрыть которые с помощью настроек приватности невозможно. Приведены результаты экспериментов, подтверждающих эффективность предложенного подхода.

Повышение эффективности противодействия вредоносной информации в социальных сетях

***Виткова Лилия Андреевна**, СПбГУТ им. М.А. Бонч-Бруевича*

Известные средства противодействия вредоносной информации в социальных сетях не отвечают требованиям к оперативности, полноте, точности и адекватности принимаемых решений. Это обуславливает необходимость повышения эффективности противодействия вредоносной информации в социальных сетях. В докладе предлагается методика, позволяющая повысить оперативности и обоснованность противодействия вредоносной информации в социальных сетях. Приводятся результаты экспериментов, выделяются перспективные направления исследований и разработок.

Асимметричная криптографическая изоляция сегментов облачной среды, гарантированно предотвращающая возможность утечки служебной информации через Интернет

***Тимофеев Юрий Андреевич**, к.т.н., с.н.с, Национальный технический Комитет по стандартизации, ТК 22*

В докладе предлагается архитектурное решение БОЗОН, обеспечивающее возможность выделения в облачной среде нескольких изолированных вычислительных зон, из которых только одна имеет выход в Интернет, а остальные работают исключительно в рамках самостоятельно изолированных сегментов внутренней локальной сети, не имеющих подключения к интернету. За счет применения современных облачных решений VDI все процессы обработки информации каждой вычислительной зоны, включая клиентские вычисления, сосредотачиваются внутри защищенных помещений Центра обработки данных. Все вычислительные процессы, которые традиционно выполняются непосредственно на рабочих местах пользователей, переносятся на выполнение в серверные фермы, находящиеся внутри защищенного периметра.

Система обнаружения вредоносного программного обеспечения с использованием методов компьютерного зрения

***Полосухин Никита Владимирович**, Академия ФСО России*

Проводится исследование подхода детектирования вредоносного программного обеспечения на основе технологий компьютерного зрения. Приводятся достоинства и недостатки современных подходов и способы их улучшения.

Пороговые значения для системы сетевой безопасности на базе SDN

***Майхуб Самара**, Самарский национальный исследовательский университет им. С.П. Королева*

***Алексеев Кирилл Павлович**, НИУ «Высшая школа экономики», МИЭМ*

Предлагается использовать метод пороговых значений и технологии NetFlow и SDN для создания системы обнаружения сетевых вторжений и противодействия атакам. Статистика sflow применяется для определения пороговых значений сетевых переменных, при превышении которых можно говорить об атаке. SDN-контроллер служит для блокирования трафика с атакующих IP адресов.

17:30 – 19:30 Секция «Подготовка специалистов по защите информации для решения задач цифровой экономики»

Зал «Стеклянный»

Ведущие:

- **Белов Евгений Борисович,** заместитель председателя Федерального учебно-методического объединения в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ), председатель ФУМО СПО ИБ
- **Лось Владимир Павлович,** председатель правления Ассоциации Защиты Информации, Комиссия ИБ СПК-ИТ
- **Хайров Игорь Евгеньевич,** заместитель директора Академии Информационных Систем

Обсуждение проекта профессионального стандарта «Специалист по криптографической деятельности»

***Белов Евгений Борисович**, заместитель председателя ФУМО ВО ИБ, председатель ФУМО СПО ИБ*

***Лось Владимир Павлович**, председатель правления Ассоциации Защиты Информации, Комиссия ИБ СПК-ИТ*

Актуализация профессиональных стандартов в области информационной безопасности и информационно-коммуникационных технологий

***Белов Евгений Борисович**, заместитель председателя ФУМО ВО ИБ, председатель ФУМО СПО ИБ*

***Лось Владимир Павлович**, председатель правления Ассоциации Защиты Информации, Комиссия ИБ СПК-ИТ*

Новые ФГОС ВО 3++ в области информационной безопасности (характеристики, особенности реализации)
***Белов Евгений Борисович**, заместитель председателя ФУМО ВО ИБ, председатель ФУМО СПО ИБ*

Формирование программы социологического исследования по определению потребности в кадрах в области информационной безопасности для решения задач цифровой экономики
***Белов Евгений Борисович**, заместитель председателя ФУМО ВО ИБ, председатель ФУМО СПО ИБ*
***Хайров Игорь Евгеньевич,** заместитель директора Академии Информационных Систем*

Опыт проведения демонстрационного экзамена по программам СПО в области информационной безопасности
***Книга Ольга Владимировна**, директор колледжа приборостроения и информационных технологий РТУ МИРЭА*

Особенности подготовки техников по защите информации
***Садыкова Елена Васильевна**, заместитель директора колледжа приборостроения и информационных технологий РТУ МИРЭА*

Что можно посмотреть в Музее криптографии за один час
***Лобанова Лидия Валерьевна,** руководитель проекта по разработке Музея криптографии*
В 2021 году в Москве откроется первый в России Музей криптографии.
Широкой аудитории будет представлено прошлое, настоящее и будущее криптографии, математики и смежных дисциплин. Музей криптографии станет новой точкой притяжения на карте города — местом, где доступно и просто говорят о развитии современных технологий.

Доклады призеров конкурса студенческих работ:

Об одном симметричном алгоритме шифрования с возможностью мутаций двоичного кода при сохранении однозначности расшифрования
***Фомич Александр Вячеславович**, магистрант по направлению «Информационная безопасность» Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.*

Атака различения на шифрсистему GRANULE
***Захаров Дмитрий Александрович**, НИЯУ МИФИ*

Круглый стол/дискуссия
Информационная безопасность. Профессии будущего
Для участия приглашаются представители работодателей.

+7 (495) 120-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru