Ассоциация РусКрипто

ОРГАНИЗАТОРЫ

АИС

РУСКРИПТО'2022

XXIV МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ПРОГРАММА

22-25 МАРТА 2022 Г.

БЛАГОДАРИМ СПОНСОРОВ И ПАРТНЕРОВ ЗА ОКАЗАННУЮ ПОДДЕРЖКУ!

ЗОЛОТОЙ ПАРТНЕР

КРИПТОПРО
ключевое слово в защите информации

ЗОЛОТОЙ ПАРТНЕР

infotecs®

НАУЧНЫЙ ПАРТНЕР

НЕОБИТ

БРОНЗОВЫЕ ПАРТНЕРЫ

КОМПАНИЯ АКТИВ
s•terra®
КРИПТОНИТ
QRATE QUANTUM SOLUTIONS
СМАРТС КВАНТТЕЛЕКОМ

ПАРТНЕРЫ КОНФЕРЕНЦИИ

SPACE-BIT
АССОЦИАЦИЯ РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ
КОД безопасности
CROSSTECH SOLUTIONS GROUP
Ростелеком Солар
ANSWER pro
СПЕЦИАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР
СПБ
ОПКИТ
QApp
ФАКТОР-ТС

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

CISOCLUB
BIS JOURNAL
NBJ

Event.Rocks

Отсканируйте QR-код
или введите название
приложения Event.Rocks
в App Store и Google Play.

В приложении введите
ID события —

РУСКРИПТО2022

и далее, следуя инструкции,
авторизуйтесь в вашем профиле

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

При поддержке Цветницее

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» указано в программе.

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

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

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

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

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

25 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» 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 - 22 марта с 16:00
Выезд - 25 марта до 12:00

23 и 24 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 23-24 марта.

ОБСЛУЖИВАНИЕ В ОТЕЛЕ ПО СИСТЕМЕ «ALL INCLUSIVE»:

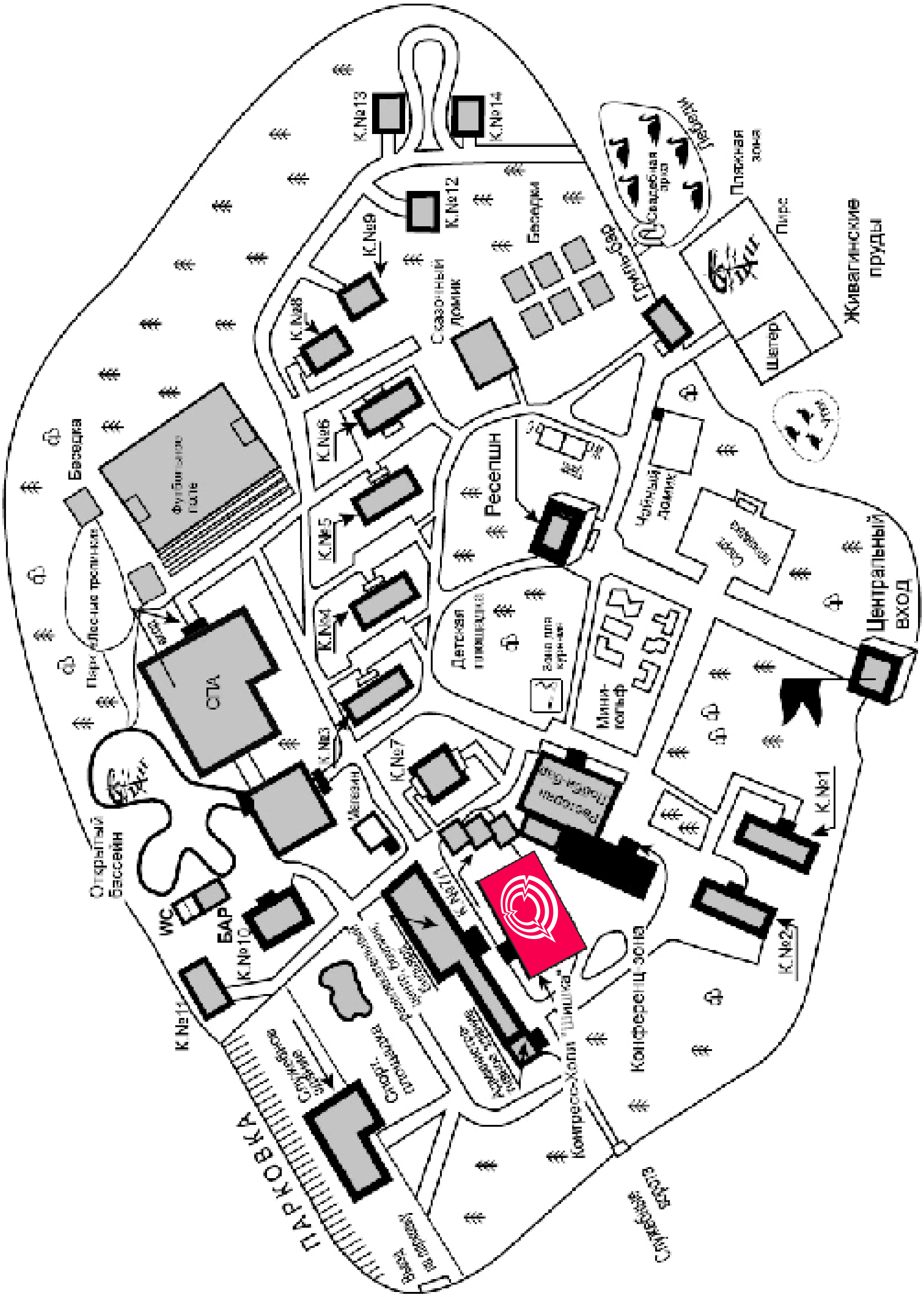
- расширенный шведский стол: завтрак (08:00-11:00), обед (13:00-16:00), ужин (19:00-23:00);
- в течение всего дня с 8-00 до 23-00 кофе, чай, выпечка, мороженое, соки, лимонады, разливное пиво, алкогольные напитки;
- бильярд, боулинг, пинг-понг;
- посещение термальной зоны SPA-комплекса (10 бассейнов 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»

КАРТА ОТЕЛЯ


К.№13
К.№14
К.№12
К.№9
К.№8
К.№6
К.№5
К.№4
К.№3
К.№7
К.№7/1
К.№1
К.№2
К.№10
К.№11
Беседки
Сказочный домик
Гриль-бар
Свадебная арка
Лебеди
Пляжная зона
Пирс
Живагинские пруды
Шатер
Ресепшн
Чайный домик
Центральный вход
Футбольное поле
Беседка
Парк «Лесные тропинки»
СПА
Открытый бассейн
WC
БАР
Магазин
Детская площадка
Зона для курения
Мини-гольф
Конференц-зона
Конгресс-Холл "Шишка"
Спорт. площадка
Служебное здание
ПАРКОВКА
Служебный въезд
Въезд на парковку

23 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

09:00 – 10:00	Регистрация участников	
10:00 – 11:30	**Официальное открытие конференции. Пленарное заседание** *Зал «Шишка», 2 этаж* *10 стр.*	
11:30 – 12:00	Кофе-брейк	
12:00 – 14:00	Круглый стол **«Квалифицированная электронная подпись в Российской Федерации»** Ведущие: · Малинин Ю.В., Ассоциациия РОСЭУ · Пауков А.А., Электронный экспресс *Зал «Шишка»* *10-11 стр.*	Секция **«Компьютерная криминалистика, реверсинг, исследование и защита цифровых технологий»** Ведущие: · Чиликов А.А., МГТУ им. Баумана · Скляров Д.В., Positive Technologies *Зал «Еловый»* *11-12 стр.*
14:00 – 15:00	Обед	
15:00 – 16:45	Секция **«Перспективные решения, продукты и технологии»** Ведущие: · Поташников А.В., АО «ИнфоТеКС» · Горелов Д.Л., компания «Актив» *Зал «Шишка»* *12-13 стр.*	Секция **«Криптографические средства защиты информации. Требования, разработка и эксплуатация»** Ведущий: Петров А.В., ФСБ России *Зал «Еловый»* *13 стр.*
16:45 – 17:00	Кофе-брейк	
17:00 – 19:30	Секция **«Криптография и информационная безопасность в банковской сфере»** Ведущий: Елистратов А.А., Банк России Секция **«Информационная безопасность в новой реальности»** Ведущий: Сычёв А.М., МГТУ им.Баумана *Зал «Сосновый»* *14 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»* *15-16 стр.*
19:30 – 20:00	Ужин	
20:00 – 22:00	**Торжественное открытие «РусКрипто'2022».** Зал «Шишка», 2 этаж	

24 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 10:00	Завтрак		
10:00 – 12:00	Секция **«Российская и международная стандартизация в области криптографии и информационной безопасности»** Ведущий: · Бондаренко А.И., ТК 26 · Смышляев С.В., КриптоПро *Зал «Шишка»* *17-18 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»* *18-20 стр.*	Круглый стол **«Построение доверенных информационных систем»** Ведущий: Аветисян А.И., ИСП РАН *Зал «Сосновый»* *20 стр.*
12:00 – 12:20	Кофе-брейк		
12:20 – 14:00	Круглый стол **«Протоколы дистанционного электронного голосования»** Ведущие: · Маршалко Г.Б., ФСБ России · Смышляев С.В., КриптоПро *Зал «Шишка»* *20 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»* *21 стр.*	Секция «**Методы машинного обучения в задачах обеспечения кибербезопасности»** Ведущие: · Зегжда Д.П., ИКиЗИ СПбПУ · Жуковский Е.В., ИКиЗИ СПбПУ *Зал «Сосновый»* *22-23 стр.*
14:00 – 15:00	Обед		
15:00 – 16:45	Секция **«Подходы к обезличиванию персональных данных: регулирование»** Ведущие: · Левова И.Ю., Ассоциация больших данных · Маршалко Г.Б., ФСБ России *Зал «Шишка»* *23 стр.*	Секция: **«Вопросы безопасности подвижной радио-телефонной связи»** Ведущий: Шишкин В.А., НПК «Криптонит» *Зал «Еловый»* *24-25 стр.*	Секция **«Квантовые технологии в сфере информационной безопасности». 1 часть** Ведущие: · Корольков А.В., Академия криптографии РФ · Уривский А.В., ИнфоТеКС *Зал «Сосновый»* *25 стр.*
16:45 – 17:00	Кофе-брейк		
17:00 – 19:00	Секция: «**Новые профессии и образовательные программы в области информационной безопасности**» Ведущие: · Белов Е.Б., ФУМО СПО ИБ · Лось В.П., ЦПК ИБ · Хайров И.Е., АИС *Зал «Стеклянный»* *25 стр.*	Секция **«Перспективные исследования в области кибербезопасности»** Ведущий: Котенко И.В., СПб ФИЦ РАН *Зал «Еловый»* *26-27 стр.*	Секция **«Квантовые технологии в сфере информационной безопасности». 2 часть** Ведущие: · Корольков А.В., Академия криптографии РФ · Уривский А.В., ИнфоТеКС *Зал «Сосновый»* *27-28 стр.*

19:00 – 20:00	Ужин
20:00 – 22:00	**Интеллектуальный криптографический квиз «Игра в имитацию».** Зал «Шишка», 2 этаж

25 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 – 11:30 Пленарное заседание

Зал «Шишка»

Официальное открытие конференции. Приветственные слова

Что подписано ключом, то не вырубишь... 10 лет действующим национальным стандартам электронной подписи и хэш-функции
Матюхин Дмитрий Викторович, *к.ф.-м.н., ФСБ России*

Перспективные информационные технологии и кибербезопасность
Шойтов Александр Михайлович*, д.ф-м.н., президент Академии криптографии Российской Федерации, заместитель министра цифрового развития, связи и массовых коммуникаций Российской Федерации*

Шифраторостроение в постПЛИСовую эпоху
Баранов Александр Павлович, *д.ф-м.н., НИИСИ РАН*
Массовая информационная безопасность может быть обеспечена только серийными специзделиями, включая серийную шифртехнику. Широкое распространение получили изделия с применением программируемыми логическими схемами(ПЛИС) в реализации ключевых, наиболее доверенных функций. В условиях санкций серийных поставок больших ПЛИС (более 5 тысяч ячеек) реализовать не удастся. Выход из проблемы в разработке и производстве собственных, доверенных микросхем и микропроцессоров

Перспективы развития российской криптографии для массового пользователя
Смышляев Станислав Витальевич*, д.ф.-м.н., заместитель генерального директора, КриптоПро*
Криптосредства стали доступны массовому пользователю, причем для применения как со стационарных компьютеров, так и с мобильных устройств. СКЗИ для мобильных устройств разработаны, сертифицированы и внедряются в рамках систем работы с электронной подписью, электронного голосования, защищенного доступа к веб-ресурсам, удаленной идентификации и аутентификации. Функционирование таких криптосредств осуществляется в условиях существенно ограниченного доверия к окружению и к квалификации пользователя, требуя корректировки парадигмы разработки программных криптосредств, решения новых научных и инженерно-технических задач. В докладе буден дан обзор и сравнение развиваемых в настоящее время подходов к архитектуре криптосредств массового применения, а также рассказ о задачах массовой криптографии: о решенных и о стоящих перед специалистами в настоящее время.

Международное сотрудничество РусКрипто
Жуков Алексей Евгеньевич, *к.ф.-м.н., Ассоциация «РусКрипто», МГТУ им. Баумана*

12:00 – 14:00 Круглый стол «Квалифицированная электронная подпись в Российской Федерации»

Зал «Шишка»

2022 год полон событиями, напрямую меняющими сценарии и правила работы с усиленной квалифицированной электронной подписью. В рамках круглого стола эксперты обсудят новые возможности и сложности, нюансы работы пользователей и операторов информационных систем в новых условиях. Планируется участие представителей Министерства цифрового развития, связи и массовых коммуникаций, ФСБ России, Федеральной налоговой службы, Федерального казначейства, Федеральной таможенной службы, Федеральной нотариальной палаты и др.

Ведущие:
- **Малинин Юрий Витальевич,** президент Ассоциации «РОСЭУ»
- **Пауков Алексей Анатольевич**, генеральный директор Оператора ЭДО «Электронный экспресс» (компания «Гарант»), член Совета 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
- **Маслов Юрий Геннадьевич**, коммерческий директор компании Крипто Про, член Совета Ассоциации «РОСЭУ»
- **Кирюшкин Сергей Анатольевич**, советник генерального директора – начальник удостоверяющего центра компании «Газинформсервис», эксперт Ассоциации «РОСЭУ»

12:00 – 14:00 Секция «Компьютерная криминалистика, реверсинг, исследование и защита цифровых технологий»

Зал «Еловый»

Доклады о инструментах цифровой криминалистики, реверсинге, о новых результатах исследователей вычислительных платформ, о технологиях и механизмах защиты. Эксперты поделятся практическим опытом, обсудят правовые, технические вопросы и ответят на вопросы профессиональной аудитории.

Ведущие:

- **Чиликов Алексей Анатольевич,** к.ф.-м.н., доцент**,** МГТУ им. Баумана
- **Скляров Дмитрий Витальевич ,** руководитель отдела анализа приложений, Positive Technologies

Chip Red Pill: Как нам удалось выполнить произвольный [микро]код внутри процессоров Intel Atom

***Горячий Максим Сергеевич**, независимый исследователь*

***Ермолов Марк Михайлович**, ведущий специалист, отдел исследований безопасности ОС и аппаратных решений, Positive Technologies*

***Скляров Дмитрий Витальевич**, руководитель отдела анализа приложений, Positive Technologies*

Внутри любого современного процессора Intel находится RISC-ядро. Оно реализует слой абстракции, который интерпретирует набор инструкций, видимый пользователю, в скрытые внутри аппаратного обеспечения RISC-инструкции. RISC-ядро обладает максимальными привилегиями и может напрямую манипулировать данными. Программа микрокода встроена в чип, но операционная система и UEFI могут устанавливать обновления для микрокода. К сожалению, сам микрокод зашифрован и о его работе крайне мало открытой информации. В связи с этим, публичных исследований о внутренней структуре микрокода процессора Intel на данный момент не существует. Мы нашли способ получить доступ к ядру на общедоступной платформе. В докладе мы расскажем о структуре микрокода для платформы Intel Atom, о том, как работает наш прототип и как перехватить видимые пользователям x86-инструкции. Также мы обсудим подход, используя который мы провели реверс-инжиниринг формата микрокода и внутренней структуры Intel Atom.

Особенности извлечения данных из мобильных устройств с пофайловым шифрованием

***Каронде ев Андрей Михайлович**, Оксижден Софтвер*

В последние годы в мобильных устройствах полнодисковое шифрование постепенно сменилось на пофайловое. Вместе с этим претерпели изменения и другие механизмы защиты пользовательских данных, что существенно затруднило реализацию атак типа подбор пароля. В докладе будут приведены особенности реализации пофайлового шифрования в современных смарфонах различных производителей таких как Samsung, Apple, Huawei, Xiaomi, Oppo, Realme, разобраны ситуации, в которых возможно извлечение данных, а также описан ряд особенностей, которые стоит учитывать при проведении компьютерно-технической экспертизы таких устройств.

Трояны и бэкдоры в кнопочных мобильных телефонах российской розницы

***ValdikSS,** независимый исследователь*

***Гарипов Артур Инилевич,** независимый исследователь*

Покупая простой кнопочный телефон, пользователь ожидает от него более высокий уровень безопасности в сравнении со смартфоном: веб-браузер отсутствует, приложения не установить, а значит и вредоносы не проникнут на устройство. К сожалению, многие «звонилки» производителей третьего эшелона, широко представленные в российских розничных сетях, содержат нежелательную функциональность в виде неотключаемого меню с платными подписками, смс- и интернет-маячков, передающих IMEI телефона и IMSI SIM-карты производителю, а в некоторых случаях — настоящие бэкдоры, управляемые с CnC через интернет. В докладе рассматриваются прошивки реальных устройств на чипах фирм Mediatek, RDA Microelectronics, Spreadtrum, методы их снятия, распаковки и анализа. Также приводятся результаты изучения интернет-трафика и СМС-сообщений.

Современные возможности криминалистического исследования компьютеризированных элементов автомобилей

Милешин Анатолий, *Следственный комитет Российской Федерации*
Бережной Игорь, *Следственный комитет Российской Федерации*
Пугачёв Илья Борисович, *технический директор, ООО «НТЦ «ИБ»*

Защита от копирования программной лицензии

Бакаляров Михаил Александрович, *руководитель департамента разработок и тестирования guardant, компания «Актив»*

Программная лицензия содержит данные, которые могут меняться в процессе работы программы. Ничто не мешает скопировать файлы лицензии, а затем вернуть их в исходное состояние. Мы расскажем один из способов защиты, который не требует прав администратора и установки драйверов. Файлы можно будет перемещать, но нельзя будет скопировать. Перехват функций операционной системы не потребуется, производительность не пострадает. Данный трюк использует возможности файловой системы и механизмы защиты от реверс-инжиниринга.

Положительный опыт криминалистического исследования мобильных устройств

Шавловский Андрей Борисович, *старший эксперт отдела компьютерно-технических исследований федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации»*

15:00 – 16:45 Секция «Перспективные решения, продукты и технологии»

Зал «Шишка»

Секция, целиком посвященная российским разработчикам криптографических решений и средств информационной безопасности. Презентации новых решений, перспективных технологий, продуктов. Дискуссии и ответы на сложные вопросы профессиональной аудитории РусКрипто.

Ведущий:

- **Поташников Александр Викторович**, заместитель директора центра разработки, АО «ИнфоТеКС»
- **Горелов Дмитрий Львович**, управляющий партнер компании «Актив», директор ассоциации «РусКрипто»

TLS ГОСТ для граждан и организаций

Еранов Сергей Валерьевич*, АО «ИнфоТеКС»*

В докладе рассказывается о продуктах компании АО «ИнфоТеКС» решающих задачи организации защищенных соединений по протоколу TLS с использованием российских криптографических алгоритмов. Будут представлены продукты как для конечных граждан, так и для организаций.

Перспективные технологии Рутокен для решения «необычных» задач

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

Рутокен – это не только устройства для хранения криптографических ключей и вычисления электронной подписи. Существует большое количество задач, не относящихся непосредственно к криптографическим. Компания «Актив» представляет технологические решения для нестандартных применений, которые уже используются и которые будут реализованы в скором будущем.

О реализации IPSec маршрутизатора на базе специализированной СБИС
Алешин Максим Сергеевич, *ведущий инженер службы 1 ЗИС, АО «НТЦ Атлас»*
В докладе рассказывается об архитектурных и технических решениях, примененных АО "НТЦ "Атлас" при разработке СБИС, предназначенной для построения IPSec шифраторов с производительностью до 10Гбит/с, а также вопросы построения API CS, решения по реализации базы данных соединений и защите информации в этой базе.

Преобразование интерфейса PKCS#11 в CryptoAPI
Агафьин Сергей Сергеевич, *начальник отдела разработки ФКН, КриптоПро*
PKCS#11 и CryptoAPI являются наиболее популярными интерфейсами для доступа к функциям криптографии ключевых носителей. Прикладные приложения, которые нацелены на обобщение пользовательского опыта работы с ключами, должны проводить независимую двойную работу по встраиванию обоих интерфейсов, что может быть затруднительно не только в разработке, но и в поддержке. В докладе предлагается решение данной проблемы путем сведения интерфейса PKCS#11 к интерфейсу CryptoAPI через промежуточный интерфейс ReaderAPI и приводятся результаты эксплуатации пользователями универсального криптопровайдера, который позволяет исключить потребность в двойном встраивании.

Постквантовая криптография и российские вычислительные системы: первый подход
Гугля Антон Павлович, *структурное подразделение «КуАпп» Российского квантового центра*
Гребнев Сергей Владимирович, *структурное подразделение «КуАпп» Российского квантового центра*
Кот Максим Антонович, *структурное подразделение «КуАпп» Российского квантового центра*
В докладе планируется представить разработанную «КуАпп» библиотеку постквантовых криптографических алгоритмов PQLR и возможности ее интеграции в программные продукты информационной безопасности, которые могут защитить данные бизнеса от кибератак с применением как классических, так и квантовых компьютеров.

Применение технологий искусственного интеллекта в информационной безопасности
Татевосян Айк Варданович, *ООО «Кросстех Солюшнс Групп»*
Сейчас никого не удивить технологиями искусственного интеллекта, так как каждый из нас сталкивался с ним: будь то звонок в службу поддержки, когда нам отвечает голосовой помощник, общение в чатах с роботом, одобрение заявки на кредит, таргетированная реклама продуктов и услуг, автоматическое считывание данных со сканов документов, верификация клиентов по средствам голоса и фотографий и многое другое. При таких тенденциях в области цифровизации остро встает вопрос о информационной безопасности и о защите собираемых данных о нас. В связи с этим многие компании, особенно крупные, столкнулись с тем, что традиционные технологии обеспечения информационной безопасности становятся малоэффективными либо вовсе неэффективными и убыточными. В докладе будет рассмотрены решения, позволяющие нивелировать риски, связанные с использованием традиционных технологий, использующие машинного обучения.

15:00 – 16:45 Секция «Криптографические средства защиты информации. Требования, разработка и эксплуатация»
Зал «Еловый»

Секция для разработчиков криптографических решений и организаций, занимающихся внедрением и эксплуатацией российских СКЗИ.

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

Обзор изменений законодательства в сфере применения СКЗИ
Толстолуцкая Анастасия Васильевна, *ФСБ России*

О возможности использования биометрической аутентификации в СКЗИ
Шейкин Всеволод Владимирович, *ФСБ России*

О подходах к обоснованию качеств биологических датчиков случайных чисел
Тыщенко Никита Сергеевич, *ФСБ России*

О порядке эксплуатации и сертификации средств криптографической защиты информации, использующих криптографические механизмы по ГОСТ 28147-89
Петров Алексей Владимирович, *ФСБ России*

17:00 – 18:00 Секция «Криптография и информационная безопасность в банковской сфере»

Зал «Сосновый»

Обеспечение безопасности банковской деятельности и финансовых операций. ИБ и криптография в платежных системах. Дорожные карты внедрения российской криптографии в кредитно-финансовой сфере. Стандарты и требования.

Ведущий: **Елистратов Андрей Алексеевич**, к.ф.-м.н., Департамент информационной безопасности, Банк России

О мероприятиях по импортозамещению в банковской сфере

Зинюк Борис Федорович, *Академия криптографии Российской Федерации*

Как известно п. 5.5. Положения Банка России от 04.06.2020 №719-П предписывает переход на отечественные средства криптографической защиты информации (СКЗИ) в значимых платежных системах. Для достижения данного результата в прошлом году был создан «Центр тестирования технических средств и программного обеспечения, реализующих СКЗИ значимых платежных систем», а в этом году созданы «Технологические карты осуществления переводов денежных средств, описывающие инфраструктурные процессы действующей системы проведения карточных платежей и эмиссии карт на территории Российской Федерации». Доклад будет посвящен сделанным и предстоящим шагам которые помогут российским вендорам в создании СКЗИ, способных заместить иностранное криптографическое оборудование в банковской сфере.

Об использовании аппаратных доверенных модулях (HSM) в национально значимых платежных системах

Простов Владимир Михайлович, *ТК26, КриптоПро*

Одной из задач импортозамещения в соответствии с п. 5.5. Положением Банка России от 04.06.2020 №719-П является создание российских HSM-модулей, которые способны обеспечить как функционал, так и безопасность в процессах обеспечения платежей значимых платежных систем Российской Федерации. Доклад будет посвящен проблемам создания таких средств и путям их решения.

Эволюция Мастерчейн: развитие технологии и создание Госчейн

Конкин Анатолий Юрьевич*, ООО «Системы распределенного реестра»*

В настоящее время в финансовой сфере расширяется применение технологии распределенных реестров. В частности, расширяется и применение ИС «Мастерчейн». В докладе будет рассказано о текущих сервисах Мастерчейн, о цифровой ипотеке на базе этой технологии и о Госчейн.

18:00 – 19:30 Секция «Информационная безопасность в новой реальности»

Зал «Сосновый»

Секция посвященная новым вызовам в области информационной безопасности возникшим в последние недели.

Ведущий: **Сычёв Артём Михайлович,** д.т.н., доцент МГТУ им.Баумана

Обеспечение устойчивого функционирования российского сегмента сети Интернет в условиях недружественной санкционной политики

Пьянченко Андрей Андреевич, *заместитель директора – директор программ, ФГАУ НИИ «Восход»*

Анализ трендов киберугроз последнего месяца глазами крупнейшего SOC России. Меры защиты. От WAF+AntiDDoS до NTA и EDR

Гончаров Павел Игоревич, *заместитель директора по развитию бизнеса Solar JSOC компании «Ростелеком-Солар»*

Дискуссия

17:00 – 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,** КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

Криптографический конкурс: разделение секрета или порча секрета (Cryptographic challenge – Secret Sharing or Secret Spoiling).

***Eric Filiol (Эрик Филиол)**, профессор, ENSIBS-France, НИУ ВШЭ*

Эрик Филиол предлагает участникам конференции принять участие в криптографическом конкурсе. Участникам конференции будет представлен код программы, реализующий протокол разделения секрета Шамира, и содержащий уязвимость (бэкдор) в системе безопасности. Цель конкурса – выявить недостаток и объяснить, как его можно использовать со значительной вероятностью успеха. Победителю будет вручен специальный приз от нашего уважаемого французского коллеги.

Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»

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

Двойное параллельное шифрование (TWIN-конструкция) – способ увеличения допустимой нагрузки на ключ для некоторых режимов, к примеру, CTR и GCM. С использованием теории доказуемой стойкости получены соответствующие оценки, выполнено сравнение с характеристиками стандартизированных режимов. Также показано, что использование в TWIN шифра «Магма» затрудняет применение известных методов определения секретного ключа.

О свойствах алгоритма S3G-128 при использовании усеченной хэш-функции Стрибог

***Кирюхин Виталий Александрович,** старший специалист, ООО «СФБ Лаб»*

Ключевой алгоритм S3G-128 построен на основе хэш-функции Стрибог, используется в аппаратных модулях устройств мобильной связи. Рассматриваются свойства S3G-128 при усечении Стрибога до одного вызова функции сжатия: получены оценки в рамках теории доказуемой стойкости; разработан метод определения секретного ключа для 6 (из 12) раундов.

О поиске разностных соотношений для подстановки ALZETTE с максимальным или близким к нему значением разностной характеристики

***Дмух Андрей Александрович**, Академия криптографии Российской Федерации*

***Пасько Дмитрий Олегович**, Академия криптографии Российской Федерации*

Предлагается подход для поиска разностных соотношений ARX-подстановки ALZETTE с переменным числом итераций, позволяющий получить соотношения с максимальными или близкими к максимальным разностными характеристиками.

Использование преобразований, задаваемых умножением на элемент кольца, в качестве линейных преобразований в XSL-схемах

***Давыдов Степан Андреевич,** специалист-исследователь, лаборатория криптографии НПК «Криптонит»*

***Шишкин Василий Алексеевич,** к.ф.-м.н., руководитель лаборатории криптографии НПК «Криптонит»*

Одной из основополагающих задач, стоящих перед разработчиками современных симметричных базовых криптографических систем является задача построения линейных преобразований с заданными криптографическими характеристиками. В работе рассматривается класс линейных преобразований, задаваемых умножением на элемент кольца. Такие преобразования могут быть эффективно реализованы с использованием современных инструкций процессора – CLMUL и XOR. Среди матриц указанного вида были найдены матрицы размера 8×8 с 8-битными блоками и показателем рассеивания 8, матрицы 16×16 с 4-битными блоками и показателем рассеивания 12.

О квази-адамаровых преобразованиях на конечных группах

***Пудовкина Марина Александровна**, д.ф-м.н., профессор НИЯУ МИФИ*

Для произвольной конченой группы введены обобщенные квази-адамаровы преобразования, частным случаем которых являются псевдо-адамаровы преобразования алгоритмов блочного шифрования семейства Safer, Twofish, а также квази-адамаровы преобразования, заданные на декартовом произведении Z^2_{2^m}. Доказан критерий биективности, а также выявлена связь биективности с принадлежностью к преобразованиям, которые можно считать обобщением ортоморфизмов и полных преобразований, применяемых в дискретной математике и криптографии.

Построение множества невозможных разностей алгоритмов шифрования Фейстеля с небиективной функцией усложнения для произвольного числа раундов

***Захаров Дмитрий,** НИЯУ МИФИ*

Доклад победителя конкурса студенческих докладов.

Задача скрытой подгруппы в методах квантового криптоанализа

***Поляков Михаил Вадимович**, МГТУ им. Н.Э.Баумана*

Задача скрытой подгруппы возникает как подзадача в квантовом алгоритме Шора, который эффективно решает задачу факторизации и дискретного логарифмирования. В тоже время, поиск скрытой подгруппы (или еще говорят, скрытого сдвига) является составной частью ряда методов криптоанализа симметричных шифрсистем. В данной работе рассматривается вопрос решения задачи скрытой подгруппы на квантовом компьютере для поиска линейных структур в симметричных криптоалгоритмах.

О реализации хэш-функции ГОСТ 34.11-2018 в виде квантовой схемы

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

***Рудской Владимир Игоревич**, ТК 26*

В докладе представлена реализация уменьшенной модели хэш-функции ГОСТ 34.11-2018 в виде квантовой схемы. Показано, что минимальное необходимое количество логических кубит зависит от длины хэшируемого сообщения. Представлены оценки минимального необходимого количества логических кубит для реализации ГОСТ 34.11-2018.

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 12:00 **Секция «Российская и международная стандартизация в области криптографии и информационной безопасности»**
Зал «Шишка»

Секция, полностью посвящённая стандартизации криптографических алгоритмов, протоколов, технологий информационной безопасности и цифровых технологий в целом.

Ведущие:

- **Бондаренко Александр Иванович,** заведующий лаборатории Академии криптографии Российской Федерации, соруководитель РГ СКАиП ТК 26
- **Смышляев Станислав Витальевич,** д.ф.-м.н., заместитель генерального директора КриптоПро, соруководитель РГ СКАиП ТК 26

Перспективные направления национальной стандартизации в области криптографии
Шишкин Василий Алексеевич, *к.ф.-м.н., руководитель лаборатории криптографии, НПК «Криптонит»*
В настоящее время в Российской Федерации существует развитая система национальных стандартов в области криптографии. Куда двигаться дальше? В докладе этот вопрос рассматривается в свете как международной стандартизации, так и внутренних вызовов

О перспективных для стандартизации схемах подписи вслепую
Алексеев Евгений Константинович, *КриптоПро*
Ахметзянова Лилия Руслановна, *КриптоПро*
Бабуева Александра Алексеевна, *КриптоПро*
В РГ СКАиП ТК26 в настоящее время ведутся работы по разработке Методических Рекомендаций «Протоколы формирования и проверки электронной подписи вслепую». В рамках этих работ было выбрано три перспективных для стандартизации схемы подписи вслепую: схема Abe, схема Шаума-Педерсена (Brands) и схема TeZhu. В докладе будут представлены данные схемы, а также проведен их сравнительный анализ с точки зрения обеспечиваемых ими свойств безопасности и эксплуатационных характеристик.

Об особенностях применения криптографических механизмов в системе маркировки товаров различных торговых групп
Гуселев Антон Михайлович*, Академия криптографии Российской Федерации*
В рамках реализации проекта «Внедрение автоматизированной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя для защиты населения от фальсифицированных лекарственных препаратов и оперативного выведения из оборота контрафактных и недоброкачественных препаратов прошел эксперимент по маркировке контрольными (идентификационными) знаками и мониторингу за оборотом отдельных видов лекарственных препаратов. Было установлено, что криптографические механизмы, определяемые документами национальной системы стандартизации, не в полной мере удовлетворяют потребностям разрабатываемой автоматизированной системы. Основное препятствие для безопасного применения указанных криптографических механизмов заключается в то, что значение кода проверки может быть записано в виде «44 символов (цифр, строчных и прописных букв латинского алфавита, а также специальных символов)», что составляет порядка 256 бит. В докладе рассмотрена схема цифровой подписи, подходящая для реализации в системе маркировки товаров различных товарных групп, в том числе лекарственных препаратов для медицинского применения.

Использование российских криптографических алгоритмов в протоколах OpenID Connect
Грунтович Михаил Михайлович, *АО «ИнфоТеКС»*
OpenID Connect – семейство протоколов, являющихся усовершенствованием протоколов OAuth 2.0, позволяющих улучшить их функционал путем более точного описания процесса аутентификации клиента, использования криптографических алгоритмов и возможности клиенту получить информацию о конечном пользователе. Разрабатываемые технические спецификации ТК26 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколах OpenID Connect» описывают сценарии с кодом авторизации (а также гибридный сценарий) протокола OpenID Connect с использованием криптографических алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, Р 1323565.1.026 2019. Обсуждаются вопросы разработки данного документа и его применение для аутентификации клиентов прикладных протоколов.

Возможности применения российских криптографических алгоритмов в стандарте FIDO2
Мироненко Евгений Олегович, *руководитель отдела R&D Рутокен, компания «Актив»*
FIDO2 – набор спецификаций, описывающих схему беспарольной двухфакторной аутентификации, поддерживаемую большинством современных браузеров и мобильных операционных систем. В докладе будут представлены результаты анализа возможности использования отечественных криптоалгоритмов в данной схеме.

Состояние гармонизации системы ГОСТ Р с международными стандартами в области идентификации и аутентификации
Сабанов Алексей Геннадьевич, *заместитель генерального директора, Аладдин Р.Д.*
Будут обсуждаться вопросы соотношения количества международных и российских стандартов в области идентификации и аутентификации, вопросы определения приоритетов, состава и качества стандартов в данной области. Будет затронута тема задач гармонизации стандартов и пути решения этих задач. Кроме того, будут рассмотрены смежные проблемы, касающиеся стандартов по управлению доступом и защите персональных данных.

Стандартизация цифровых технологий: или несколько рано, или уже безнадежно поздно
Уткин Никита Александрович, *руководитель технического комитета по стандартизации «Кибер физические системы» (ТК 194)*
Развитие цифровых технологий требует одновременно как максимально широкого взгляда на возможные технологические альтернативы, так и ускоренного формирования отраслевого консенсуса по целому набору вопросов. Поиск единого знаменателя, качественный диалог, концентрация экспертизы - возможны только при открытой совместной работе над стандартами в предметной области.Однако систематически встает вопрос своевременности и системности данной работы.В докладе будет представлено комплексное видение развития ключевых направлений стандартизации цифровых технологий, даны оценки степени их актуальности и определен уровень их взаимосвязанности.

Стандарты - инструмент обеспечения безопасности биометрических технологий
Николаев Данила Евгеньевич, *председатель технического комитета по стандартизации «Биометрия» (ТК 98)*
В докладе будут затронуты вопросы, связанные с проблематикой обеспечения безопасности биометрических технологий и корректного применения национальных стандартов в области биометрических технологий. А также рассмотрены конкретные примеры, в результате которых понижается безопасность государственных и коммерческих биометрических систем.

10:00 – 12:00 Секция «Криптография и криптоанализ», 2 часть
Зал «Еловый»

О статистических свойствах последовательностей, формируемых физически неклонируемыми функциями для использования в механизмах идентификации и аутентификации
Романенков Роман Александрович, *ТК26*
Уривский Алексей Викторович, *АО «Инфотекс»*

Щербакова Анна Олеговна, *АО «Инфотекс»*
Бондаренко Александр Иванович, *Академия криптографии Российской Федерации*
Маршалко Григорий Борисович, *ФСБ России*
Работа посвящена исследованию характеристик двоичных последовательностей, вырабатываемых с использованием физически неклонируемых функций (ФНФ). Предложен набор статистических экспериментов, позволяющий сделать вывод о свойствах ФНФ на основе анализа характеристик вырабатываемых ими двоичных последовательностей. Приведены результаты экспериментальных исследований ФНФ, основанных на использовании статической памяти с произвольным доступом (ФНФ типа SRAM).

Псевдослучайные функции «с забыванием» в механизмах защиты на основе паролей

Никифорова Лидия Олеговна, *инженер-аналитик, КриптоПро*
Ахметзянова Лилия Руслановна, *зам. начальника отдела криптографических исследований, КриптоПро*
В работе рассматриваются псевдослучайные функции «с забыванием» (oblivious PRF, OPRF). Данный механизм позволяет клиенту получать результат вычисления псевдослучайной функции, использующей в качестве ключа секрет сервера, от своих данных. Вычисление выполняется с помощью интерактивного протокола таким образом, что клиент не узнает секрет сервера, а сервер не получает никакой информации о данных клиента и результате вычисления. Основное внимание в работе уделено рассмотрению OPRF в качестве составной части механизмов защиты на основе малоэнтропийных секретов (паролей). Рассмотрены механизм распределенного хранения секрета с доступом по паролю, менеджер паролей. Для рассмотренных механизмов обозначены свойства безопасности, которые ими обеспечиваются, описаны принципы построения.

Высокопроизводительная псевдослучайная функция pCollapserARX256-32x2

Поликарпов Сергей Витальевич*, Южный федеральный университет*
Румянцев Константин Евгеньевич*, Южный федеральный университет*
Прудников Вадим Александрович*, Южный федеральный университет*
Определяется возможность использования ARX-функций в качестве основного элемента псевдо-динамической подстановки. Осуществляется интегрирование псевдо-динамических подстановок на основе ARX-функций в структуру псевдо-случайной функции pCollapser. Создаётся и оценивается производительность последовательной и параллельной программной реализации.

Об одном классе алгоритмов контроля целостности больших блоков данных

Бобровский Дмитрий Александрович, *Финансовый университет при Правительстве РФ, ООО «Код Безопасности»*
Фомичёв Владимир Михайлович, *д.ф.-м.н., профессор, Финансовый университет при Правительстве РФ, ООО «Код Безопасности», ФИЦ ИУ РАН*
Задорожный Дмитрий Игоревич*, ООО «Код Безопасности»*
Коренева Алиса Михайловна*, к.ф.-м.н., ООО «Код Безопасности»*
Курочкин Алексей Вячеславович*, ООО «Код Безопасности», МФТИ*
В докладе представлен класс алгоритмов контроля целостности больших блоков данных. Алгоритмы класса превосходят по производительности до 73 раз известные алгоритмы, что показывает высокий потенциал данного класса в части приложений. Вместе с тем, для некоторых алгоритмов из класса показана недостаточность уровня защиты от коллизий, что инициирует задачу тщательного выбора в заданном классе параметров алгоритмов.

Атака на шифры гаммирования, использующие q-слабые ключи.

Бабаш Александр Владимирович*, д.ф.-м.н., профессор, НИУ ВШЭ, РЭУ им. Г.В. Плеханова*
Под информацией о «читаемом» тексте понимается собственное подмножество всех читаемых текстов содержащее текст. Дешифрование шифра по шифрованному тексту трактуется как определение информации о зашифрованном читаемом тексте. Для шифртекста шифра гаммирования вводится понятие q-слабого ключа, учитывающее корреляцию между зашифрованным текстом и используемым ключом. Указываются методы дешифрования шифров гаммирования на основе q-слабых ключей с расчетом параметров их сложности.

О возможностях противника при атаках на некоторый класс протоколов аутентифицированной выработки общего ключа

Алексеев Евгений Константинович, *начальник отдела криптографических исследований, КриптоПро*
Ахметзянова Лилия Руслановна, *зам. начальника отдела криптографических исследований, КриптоПро*
Куценок Кирилл Олегович, *инженер-аналитик, КриптоПро*
Кяжин Сергей Николаевич, *ведущий инженер-аналитик, КриптоПро*

В настоящей работе приводится систематизированный обзор качественных возможностей противника, атакующего протоколы аутентифицированной выработки общего ключа (AKE-протоколы, Authenticated Key Exchange), которые рассматриваются в современных криптографических исследованиях по данному направлению. Внимание в работе концентрируется на наиболее базовом типе таких протоколов, который предполагает взаимодействие двух участников (в частности, не рассматриваются протоколы с участием третьей доверенной стороны). Для каждой из возможностей, перечисленных в настоящей работе, приводится мотивация ее рассмотрения. Также приводятся примеры их применения при построении атак на известные протоколы.

10:00 – 12:00 Круглый стол «Построение доверенных информационных систем»

Зал «Сосновый»

В рамках круглого стола будут обсуждены инструменты, методики и практики создания доверенных систем, в т.ч. технологии жизненного цикла безопасной разработки программного обеспечения. Эксперты расскажут об опыте внедрения в практике и об оценках ресурсозатратности/эффективности, обсудят планы отрасли на ближайшее время.

Ведущий: **Аветисян Арутюн Ишханович,** академик РАН, профессор РАН, доктор физико-математических наук, директор ИСП РАН

Эксперты круглого стола:

- **Пономарёв Дмитрий Юрьевич,** технический директор НТЦ «Фобос-НТ»
- **Гусев Дмитрий Михайлович,** заместитель генерального директора АО «ИнфоТеКС»
- **Задорожный Дмитрий Игоревич**, руководитель службы по сертификации, ИБ и криптографии, ООО «Код Безопасности»
- **Падарян Вартан Андроникович,** руководитель направления обратной инженерии бинарного кода ИСП РАН

12:20 – 14:00 Круглый стол «Протоколы дистанционного электронного голосования»

Зал «Шишка»

Обсуждение вопросов безопасности криптографических протоколов дистанционного электронного голосования. Технологические и криптографические аспекты.

Ведущие:

- **Маршалко Григорий Борисович,** ФСБ России
- **Смышляев Станислав Витальевич,** д.ф.-м.н., заместитель генерального директора, КриптоПро

Эксперты круглого стола:

- **Сатиров Юрий Константинович,** заместитель генерального директора, РТЛабс
- **Калихов Артем Владимирович,** генеральный директор Waves Enterprise
- **Сазонов Александр Валентинович,** руководитель проекта Polys, лаборатория Касперского
- **Алексеев Евгений Константинович,** начальник отдела криптографических исследований, КриптоПро
- **Шишкин Василий Алексеевич,** руководитель лаборатории криптографии, НПК «Криптонит»
- **Науменко Антон Павлович**, руководитель направления, СФБ Лаб
- **Шишмарев Владислав Борисович,** заместитель руководителя ДИТ Москвы

12:20 – 14:00 Секция «Криптография и криптоанализ», 3 часть

Зал «Еловый»

Новый механизм матричного гибридного асимметричного шифрования (A new matrix hybrid asymmetric ciphering mechanism)

Франсуа Дюпон (François Dupont), *CNRS*

Предлагается новый гибридный механизм асимметричного шифрования, использующий трехпроходный протокол с ключами шифрования, которые являются коммутирующими матрицами. Такой трехпроходный протокол также позволяет проводить аутентификацию участников.

Еще раз о важности построения модели противника на примере протокола аутентификации 5G-AKA

Царегородцев Кирилл Денисович, *специалист-исследователь, НПК «Криптонит»*

Грибоедова Екатерина Сергеевна, *руководитель направления стандартизации, НПК «Криптонит»*

Довольно часто вопросы "доказуемой стойкости" вызывают дискуссии; так, многими ставится под сомнение сама необходимость подобного подхода, а ошибки в доказательствах и моделях стали "притчей во языцех".В докладе на примере угрозы нарушения приватности пользователей для протокола 5G-AKA будут затронуты некоторые аспекты моделирования и теоретико-сложностных сведений: зачем нужна формализация/модель и можно ли обойтись без этого этапа? каковы гарантии, если сведение всё-таки удалось построить? и наконец: отличается ли кардинально ситуация с моделями внутри криптографии от других наук?

Использование атрибутной подписи в двухуровневой распределенной информационной системе с динамической структурой

Беззатеев Сергей Валентинович, *Санкт-Петербургский университет аэрокосмического приборостроения*

Жиданов Константин Александрович, *Санкт-Петербургский университет аэрокосмического приборостроения*

Афанасьева Александра Валентиновна, *Санкт-Петербургский 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.

Методика автоматизированного тестирования реализаций криптографических протоколов

Прокопьев Сергей Евгеньевич, *Институт системного программирования им. В.П. Иванникова РАН, НПК «Криптонит»*

В докладе представляется подход к тестированию реализаций криптопротоколов, основанный на использовании выразительных формальных моделей. Рассматриваются преимущества предлагаемого подхода в части измерения качества тестирования, применимости тестового инструментария для разных криптопротоколов и др.

Сеанс черной магии с разоблачениями

Eric Filiol (Эрик Филиол), *профессор, ENSIBS-France, НИУ ВШЭ*

Подробное объяснение механизма работы лазейки из первого доклада в секции и вручение приза от Эрика Филиола победителю.

12:20 – 14:00 Секция «Методы машинного обучения в задачах обеспечения кибербезопасности»

Зал «Сосновый»

Научная секция, посвященная вопросам применения машинного обучения для решения частных задач в области обеспечения кибербезопасности, в т.ч. поиска уязвимостей, обнаружения вредоносного программного обеспечения, аудита безопасности информационных систем и других. В рамках секции также будут обсуждаться вопросы безопасности применения машинного обучения.

Ведущие:

- **Зегжда Дмитрий Петрович**, д.т.н., профессор РАН, директор Института кибербезопасности и защиты информации СПбПУ
- **Жуковский Евгений Владимирович,** к.т.н., доцент, Институт кибербезопасности и защиты информации СПбПУ

Анализ защищенности интеллектуальных информационных систем с учетом классификации состязательных угроз MITRE

Жуковский Евгений Владимирович, *доцент, ИКиЗИ СПбПУ*

Существующие методики выявления уязвимостей и недекларированных возможностей в программном обеспечении не учитывают особенности анализа безопасности на наличие уязвимостей, связанных с применением машинного обучения в программных системах. В докладе рассмотрены основные аспекты проведения анализа защищенности информационных систем, использующих машинное обучение с учетом известных видов атак на них. Также предложены методические рекомендации при проведении анализа защищенности информационных систем, использующих машинное обучение.

Методы генерации состязательных примеров для нейросетевых моделей

Аверьянова Полина Александровна, *старший аналитик. ООО «Лаборатория кибербезопасности»*

В докладе рассматриваются методы создания состязательных примеров для проведения атаки на нейронные сети. Состязательный пример представляет собой специальным образом искусственно созданный объект данных, который используется для обмана нейронных сетей. Рассмотрены тип состязательных атак на нейронные сети. Производится описание математической основы алгоритмов создания состязательных примеров.

Сокращение пространства признаков путём предварительной кластеризации трасс выполнения вредоносного программного обеспечения

Огнев Роман Андреевич, *ассистент, ИКиЗИ СПбПУ*

В докладе будет рассмотрен предложенный подход к выявлению вредоносного программного обеспечения, основанный на применении статико-динамического анализа и методов машинного обучения. Предлагаемый метод построения трассы вызовов, включает помимо WinAPI-функций, также информацию об использовании собственных функций, идентифицированных при помощи алгоритма fuzzy-хэширования. Также применена техника оптимизации количества параметров поведения исполняемых файлов при помощи предварительной кластеризации незначимых признаков.

Поиск уязвимостей на основе применения методов машинного обучения к графовому представлению кода

Кубрин Георгий Сергеевич, *инженер-программист, ИКиЗИ СПбПУ*

С целью автоматизации поиска сложных логических уязвимостей, вызванных наличием двух и более ошибок в программном коде, предлагается подход на основе применения методов машинного обучения и экспертных систем к графовому представлению кода. В докладе на базе формализации задачи поиска сложных логических уязвимостей рассматриваются ограничения применения методов машинного обучения к подзадачам выявления сигнатур программных ошибок и определения зависимости по данным и по управлению между компонентами сложных уязвимостей.

Использование машинного обучения для создания цифровых двойников критических информационных систем

Зубков Евгений Альбертович, *ассистент, ИКиЗИ СПбПУ*

Обеспечение функциональной устойчивости любой системы является трудоемкой и комплексной задачей, так как необходим учет множества факторов и характеристик целевой системы. Однако для устранения сложностей обеспечения устойчивости возможно использовать концепцию цифровых двойников. В докладе будет рассмотрен предложенный подход к созданию цифрового двойника с использованием машинного обучения, что позволяет более гибко реализовывать определенные функциональные показатели системы с целью дальнейшей оценки их безопасности.

Применение технологий машинного обучения в задачах искусственной иммунизации, направленной на обеспечение информационной безопасности сложных систем*

Павленко Евгений Юрьевич, *доцент, ИКиЗИ СПбПУ*

Целью научного исследования является создание нейросетевого механизма иммунизации сложных систем, обеспечивающего противодействие киберугрозам. Такой нейросетевой механизм должен обеспечивать киберустойчивость сложных систем, реализуя упреждающую, динамическую и адаптивную защиту от кибеугроз.

* Исследование выполнено в рамках грантов Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук МК-3861.2022.1.6

15:00 – 16:45 Секция «Подходы к обезличиванию персональных данных: регулирование и технологии»

Зал «Шишка»

В секции примут участие эксперты в области защиты информации и криптографии, операторы, обрабатывающие большие массивы персональных данных, представители регуляторов. Тематика обезличивания стала одним из основных трендов при обсуждении вопросов оборота и защиты персональных данных. Участники круглого стола постараются ответить на вопросы: как обезличивание помогает защитить персональные данные пользователей, каковы перспективы использования этой технологии, какие существуют требования и подходы к обезличиванию и др.

Ведущие:

- **Левова Ирина Юрьевна**, Директор по стратегическим проектам Ассоциации больших данных
- **Маршалко Григорий Борисович**, ФСБ России

О подходах к обезличиванию персональных данных. Модели применения

Дали Фархад Алишерович, *Академия Криптографии Российской Федерации*

Доклад посвящен исследованиям современных подходов к обеспечению безопасной обработки персональных данных, а также моделям их применения в информационных системах персональных данных, включающих широкий спектр математических методов обезличивания персональных данных таких, как k-анонимность, l-разнообразие, статистическое обезличивание и др., для которых при определенных условиях могут быть получены численные оценки безопасности обезличивания персональных данных.

Риск-ориентированный подход к оценке рисков при обезличивании персональных данных и тестирование моделей оценки

Нейман Алексей Владимирович, *Исполнительный директор Ассоциации больших данных*

Доклад описывает риск-ориентированный подход к обработке обезличенных данных, в том числе методологию оценки контекстных рисков, рисков данных. А также мероприятий АБД по тестированию данного подхода на бизнес-кейсах участников АБД

Правовые аспекты обезличивания данный: проблемы и перспективы

Иванова Екатерина Пенчева, *Директор по правовым вопросам oneFactor*

В докладе будут отражены основные подходы к регулированию обезличенных данных, существующие в России подходы к формированию правовой модели, проблемы терминологического и концептуального характера и возможные подходы к решениям.

Дискуссия

15:00 – 16:45 Секция: «Вопросы безопасности подвижной радио-телефонной связи»

Зал «Еловый»

В рамках секции будут обсуждаться вопросы безопасности технологий, применяемых в подвижной радио-телефонной связи. Основное внимание будет уделено технологиям 5G и eSIM и сосредоточено на таких вопросах, как внедрение отечественных криптографических механизмов, национальная и международная стандартизация, безопасность реализации.

Ведущий: **Шишкин Василий Алексеевич,** к.ф.-м.н., руководитель лаборатории криптографии, НПК «Криптонит»

Об участии российских специалистов в развитии криптографических протоколов сетей связи 5G в 3GPP

Давыдов Степан Андреевич, *специалист-исследователь, НПК «Криптонит»*

Грибоедова Екатерина Сергеевна, *руководитель направления стандартизации, НПК «Криптонит»*

Для безопасного функционирования сетей 5G на территории России необходимо не только разработать российские аналоги криптографических алгоритмов, но и стандартизировать их как в России (в рамках ТК 26 и Росстандарта), так и за рубежом (в 3GPP). В докладе будет рассказано об итогах взаимодействия с 3GPP в 2021 году, а также дальнейших планах по участию в разработке безопасных криптографических протоколов в сетях связи нового поколения как в рамках 3GPP, так и в рамках недавно сформированной рабочей группы ТК 26.

Технология eSIM. Проблемы внедрения российских криптографические механизмов в стандарты GSMA: задачи, перспективы

Грибоедова Екатерина Сергеевна, *руководитель направления стандартизации, НПК «Криптонит»*

Давыдов Степан Андреевич, *специалист-исследователь, НПК «Криптонит»*

Самохвалов Ромах Игоревич, *специалист-исследователь в области телекоммуникаций, НПК «Криптонит»*

В докладе будут освещены базовые аспекты функционирования технологии ESIM с точки зрения обеспечения криптографической безопасности, рассмотрены основные криптографические протоколы и их уязвимости, а также рассказано о проблемах внедрения решений на базе отечественной криптографии и предполагаемый порядок действий по замене криптографических механизмов на отечественные. Отдельное внимание будет уделено обзору первых результатов анализа процессов внутри GSMA.

О дополнительных требованиях к отечественным криптографическим механизмам доверенных элементов безопасности, внедряемых в технологию ESIM

Дрелихов Владимир Олегович*, к.ф.-м.н., заместитель начальника центра, АО «ИТМиВТ»*

В докладе будут рассмотрены некоторые требования к безопасности криптографических механизмов, связанные с реализацией отдельных функций доверенных элементов безопасности, внедряемых в технологию eSIM.

Повышение защиты процессов формирования электронной подписи с помощью доверенных SIM-карт

Белова Светлана Вячеславовна, *генеральный директор, ООО «Системы управления идентификацией» (IDX)*

Смирнов Павел Владимирович*, к.т.н., директор по развитию, КриптоПро*

Рассматриваются подходы, позволяющие обеспечивать повышенный уровень информационной безопасности процедур формирования электронной подписи с применением мобильных устройств пользователей при использовании SIM-карт с доверенными элементами безопасности.

Особенности построения инфраструктуры PKI GSMA и оценка возможности создания российского аналога инфраструктуры PKI GSMA для его применения в российских экосистемах eSIM

Александров Сергей Викторович*, технический директор, ООО «СПБ»*

Герасимова Алла Геннадьевна*, руководитель отдела системных исследований, ООО «СПБ»*

В докладе будет рассмотрена возможность создания российского аналога инфраструктуры PKI GSMA для его применения в российских экосистемах eSIM с использованием российских криптоалгоритмов.

Система доверенной аутентификации абонентов сети подвижной радиосвязи
***Емельянов Виктор Михайлович**, к.ф.-м.н., руководитель направления, ООО «СПБ»*
***Александров Сергей Викторович**, технический директор, ООО «СПБ»*
В докладе будет рассмотрены принципы создания системы доверенной аутентификации абонентов в качестве одного из базовых элементов обеспечения безопасности в сети подвижной радиосвязи.

15:00 – 16:45 Секция «Квантовые технологии в сфере информационной безопасности» 1 часть

Зал «Сосновый»

Секция посвященная квантовым вычисления, концептуальным вопросам создания систем квантового распределения ключей и вопросам практической реализации систем квантового распределения криптографических ключей.

Ведущие:

- **Корольков Андрей Вячеславович,** Академия криптографии РФ
- **Уривский Алексей Викторович,** заместитель генерального директора по науке и инновациям, АО «ИнфоТеКС»

Анализ модели недекларированных возможностей оптических компонентов систем квантового распределения ключей. Методы противодействия.
***Дуплякин Евгений Владимирович,** ООО «КуРэйт»*

Квантовое распределение ключей на непрерывных переменных
***Самсонов Эдуард Олегович,** ООО «СМАРТС-Квантителеком», Университет ИТМО*
***Гончаров Роман Константинович,** ООО «СМАРТС-Квантителеком», Университет ИТМО*

Подходы к моделированию атаки на упрощённый алгоритм AES при помощи квантового алгоритма Гровера
***Моисеевский Алексей Денисович,** Центр Научных Исследований и Перспективных Разработок, АО «ИнфоТеКС»*
***Елисеев Владимир Леонидович,** Центр Научных Исследований и Перспективных Разработок, АО «ИнфоТеКС»*

17:00 – 19:00 Секция: «Новые профессии и образовательные программы в области информационной безопасности»

Зал «Стеклянный»

Секция, посвящённая вопросам обучения и повышения квалификации в области информационной безопасности.

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,** Центр исследования проблем кадрового обеспечения отрасли информационной безопасности (ЦПК ИБ), председатель правления Ассоциации Защиты Информации
- **Хайров Игорь Евгеньевич,** заместитель директора Академии Информационных Систем

17:00 – 19:00 Секция «Перспективные исследования в области кибербезопасности»

Зал «Еловый»

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

Ведущий: **Котенко Игорь Витальевич,** д.т.н., профессор, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН

Интеллектуальные методы корреляции событий кибербезопасности

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

Гайфулина Диана Альбертовна, *СПб ФИЦ РАН*

Анализируются интеллектуальные методы корреляции событий применительно к задачам кибербезопасности. В области кибербезопасности эти методы необходимы для обнаружения и прогнозирования угроз с пошаговым характером, таких как многоэтапные или целевые атаки и другие причинно-связанные последовательности аномальных событий. В докладе технологии корреляции событий систематизируются по применяемым интеллектуальным методам корреляции на три основные класса: на основе сходства, пошаговые и смешанные. Методы корреляции на основе сходства сравнивают несколько событий на основе атрибутов или временных меток, а также на основе фильтров. Пошаговые методы основаны на составлении цепочек событий и анализируют связи между несколькими событиями. Смешанные методы используют комбинированные алгоритмы. В докладе представляется систематический анализ современного состояния исследований в области корреляции событий кибербезопасности.

Безопасность персональных данных: новый взгляд на старую проблему

Минзов Анатолий Степанович, *д.т.н., профессор кафедры БИТ НИУ «МЭИ»*

Невский Александр Юрьевич, *к.т.н., заведующий кафедрой БИТ НИУ «МЭИ»*

Баронов Олег Рюрикович, *к.т.н., заместитель заведующего кафедрой БИТ НИУ «МЭИ»*

Появление в Европе новой концепции защиты персональных данных (ПДН) в 2018 году, к сожалению, не нашло широкого отражения в отечественной печати, хотя взгляд на систему защиты ПДН в этой концепции несколько изменился в сторону расширения как самого понятия «персональные данные», так и в сторону создания более жестких механизмов обеспечения безопасности, контроля и ответственности операторов. В докладе рассматриваются новые подходы к моделированию угроз информации с позиций субъекта персональных данных, классификации этой информации и представления ПДН в форме единой модели, объединяющей различные прямые и косвенные, измеряемые, вычисляемые и наблюдаемые параметры модели персональных данных человека. Предложенная модель может быть использована в качестве методологической основы для нового подхода к решению задач по безопасной обработке, хранению, передачи и ответственности операторов персональных данных.

Зависимость пороговых значений для обнаружения источников сетевых атак от разрешения выборки

Терехов Александр Игоревич, *НИУ ВШЭ*

Сагатов Евгений Собирович, *к.т.н., доцент, НИУ ВШЭ*

Сухов Андрей Михайлович, *д.т.н., профессор, ДКИ МИЭМ, НИУ ВШЭ*

Рассматриваются результаты исследования метода пороговых значений для обнаружения источников сетевых атак по неполным данным. Основной вывод состоит в том, что произведение порогового значения на разрешение выборки остается постоянным. На основании собранных данных было проведено тестирование предложенной гипотезы. С учетом ошибки эксперимента эта гипотеза подтверждается. Публикация подготовлена в ходе проведения исследования по проекту № 21-04-033 в рамках Программы «Научный фонд Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ)» в 2021 году.

Автоматизация оценки защищенности компьютерных сетей

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

Одним из эффективных подходов к обнаружению проблем с защитой компьютерных сетей является подход, основанный на моделировании атак. При этом, точность результата сильно зависит от точности входных данных, которые, в свою очередь, часто основаны на знаниях оператора. Таким образом, на всех этапах от сбора информации до принятия решений высокую роль имеют знания, выбор и когнитивные способности оператора, что может не лучшим образом повлиять на качество решений по повышению защищенности компьютерной сети. В докладе предлагается комплексный подход, позволяющий автоматизировать основные шаги оценки защищенности. За счет автоматизации и используемых методов снижения неполноты и неточности данных, данный подход позволяет повысить точность результатов и свести к минимуму потенциальные ошибки.

Оценка способности человека к обнаружению ботов в социальных сетях

Коломеец Максим Вадимович, *PhD, СПб ФИЦ РАН*

Большинство систем обнаружения ботов в социальных сетях основаны на методах обучения с учителем и наборах данных, размеченных людьми. В докладе оценивается качество разметки таких наборов данных и его теоретическое влияние на эффективность систем обнаружения ботов. Приведены результаты экспериментов, показывающие что ни люди ни обученные на их метках системы обнаружения не могут обнаружить некоторые виды ботов.

Методика раннего обнаружения кибератак на компьютерные сети

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

Крибель Ксения Васильевна, *Военная академия связи им. С.М.Буденного*

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

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

Обнаружение аномалий в сетевом трафике компьютерных сетей является сложной задачей. В докладе рассматривается подход к обнаружению аномалий на основе анализа свойств самоподобия нестационарного трафика и методов машинного обучения. В качестве инструментов при реализации данного подхода были использованы фрактальный анализ, математическая статистика и нейронные сети с долгой краткосрочной памятью. Рассмотрены вопросы программной реализации предлагаемой системы и формирования набора данных, содержащего сетевые пакеты. Экспериментальные результаты, полученные с использованием сгенерированного набора данных, продемонстрировали и подтвердили высокую эффективность предлагаемой методики раннего обнаружения кибератак, в реальном или близком к реальному масштабе времени, прогнозировании факта воздействия кибератак и выработке эффективных мероприятий противодействия.

Подход к обнаружению аномалий и атак в Linux-системах на основе логов, полученных с использованием зонда eBPF

Виткова Лидия Андреевна, *к.т.н, СПбГУТ*

В современных исследованиях чаще всего зонд Extended Berkeley Packet Filter (Ebpf) используется как балансировщик нагрузки или как инструмент управления сетевыми потоками. Однако такое применение для данной технологии является ограниченным, так как по сути, Ebpf – это подсистема ядра Linux, дающая возможность писать небольшие программы, которые будут запущены ядром в ответ на событие. В докладе рассматривается комплексный подход обнаружения аномалий и атак, позволяющий формировать белые и черные списки системных вызовов, создавать профили поведения контейнеров на основе данных, полученных при помощи зонда Ebpf. Предложенный подход расширяет горизонт контроля событий информационной безопасности в ОС Linux.

17:00 – 19:00 Секция «Квантовые технологии в сфере информационной безопасности» 2 часть

Зал «Сосновый»

Ведущие:

- **Корольков Андрей Вячеславович,** Академия криптографии РФ
- **Уривский Алексей Викторович,** заместитель генерального директора по науке и инновациям, АО «ИнфоТеКС»

Об оценке эффективности защиты от оптических атак на волоконные квантовые криптографические системы выработки и распределения ключей
***Дворецкий Дмитрий Алексеевич**, ООО «СФБ Лаб»*
***Зызыкин Артем Павлович**, ООО «СФБ Лаб»*
***Сущев Иван Сергеевич**, ООО «СФБ Лаб»*
***Бугай Кирилл Евгеньевич**, ООО «СФБ Лаб»*
***Богданов Сергей Александрович**, ООО «СФБ Лаб»*
***Булавкин Даниил Сергеевич**, ООО «СФБ Лаб»*

Влияние плотности соединений на безопасность квантовой сети
***Гайдаш Андрей Алексеевич**, ООО «СМАРТС-Кванттелеком», Университет ИТМО*
***Мирошниченко Георгий Петрович**, ООО «СМАРТС-Кванттелеком», Университет ИТМО*
***Козубов Антон Владимирович**, ООО «СМАРТС-Кванттелеком», Университет ИТМО*

Ассоциация «РусКрипто»

Российская Криптологическая Ассоциация (Ассоциация «РусКрипто») – это общественная организация, объединяющая разработчиков и потребителей информационных технологий, которые заинтересованы в развитии открытой криптографии в России, а также в интеграции России в мировое информационное сообщество.

Членами Ассоциации являются ведущие российские специалисты в области криптографии и информационной безопасности. Ассоциация «РусКрипто» ежегодно проводит одноименную конференцию.

Конференция «РусКрипто» представляет собой базовую площадку для общения и обмена опытом специалистов в области криптографии и защиты информации. В ней участвуют разработчики и заказчики ИБ-решений, представители науки и образования, регуляторы и государственные чиновники.

«РусКрипто» позволяет участникам не только ознакомиться с передовыми технологиями и получить актуальную информацию о состоянии рынка средств криптозащиты, но и обсудить в неформальной обстановке задачи, которые ставят перед собой специалисты в области информационной безопасности. Аудитория конференции более 400 специалистов. География участников из года в год расширяется, охватывая как новые города России, так и страны СНГ и дальнего зарубежья.

Контактная информация:
www.ruscrypto.ru

Академия Информационных Систем

Академия Информационных Систем (АИС) создана в 1996 году. Более 25 лет АИС предоставляет образовательные услуги по информационной безопасности, информационным технологиям, конкурентной разведке и экономической безопасности. Обучение своих кадров нам доверяют Пенсионный фонд РФ, ФСС РФ, ФСКН России, ФСО России, ФССП России, ФСБ России, «Сбербанк», «Газпромбанк», «Альфа банк», «Северсталь», МТС, «Ростелеком» и многие другие.

Академия Информационных Систем сегодня это:

- Всестороннее обучение ГОСТ, СТО БР, НПС, Стандарт PCI DSS, защита ДБО, расследование компьютерных преступлений, аудит безопасности, управление рисками и др.;
- Программы повышения квалификации и профессиональной переподготовки, согласованные с ФСТЭК России, ФСБ России, Банком России, в том числе, с выдачей диплома МГТУ им. Н.Э. Баумана;
- Подготовка к международным сертификациям CISA, CISM, CGATE и т.п.;
- Единственный учебный центр, который проводит разноплановое обучение по направлению «Конкурентная разведка»;
- Обучение по защите АСУ ТП, управлению электронным документооборотом, экономической безопасности и пр.;
- Высококвалифицированные тренеры, обладающие большим практическим опытом и международными сертификациями;
- Технологии дистанционного обучения, вебинары и онлайн-тестирования.

25 лет АИС выступает организатором ежегодных конференций, бизнес-форумов и других мероприятий.

Контактная информация:
www.infosystems.ru; www.vipforum.ru

КРИПТОПРО

ключевое слово в защите информации

Компания КриптоПро занимает лидирующее положение в сфере разработки средств криптографической защиты информации (СКЗИ) и развития PKI на территории России.

Специалистами КриптоПро созданы:

- первое в РФ сертифицированное СКЗИ, интегрированное с ОС Microsoft Windows – КриптоПро CSP;
- первое в РФ сертифицированное средство обеспечения деятельности удостоверяющих центров – КриптоПро УЦ;
- первые в РФ сертифицированные службы актуальных статусов сертификатов и штампов времени – КриптоПро OCSP и КриптоПро TSP;
- первые в РФ сертифицированные аппаратные криптографические модули – Атликс HSM и КриптоПро HSM;
- первые в истории сообщества Интернет стандарты, описывающие применение российских криптоалгоритмов – RFC 4357, RFC 4490, RFC 4491, RFC 7836, RFC 8133, RFC 8645;
- первые стандартизированные параметры эллиптических кривых для российских алгоритмов ЭП, а также сопутствующие криптографические алгоритмы (HMAC, KDF, PRF, VKO, ACPKM) для российских стандартов хэширования и шифрования;
- первый в РФ стандартизированный протокол для защиты взаимодействия с ключевыми носителями (SESPAKE) и реализующие его СКЗИ, предоставляющие исключительные свойства безопасности при работе с неизвлекаемыми ключами;
- первые утвержденные методические рекомендации по применению российских криптографических алгоритмов в протоколах TLS, IPsec, CMS;
- первое в РФ сертифицированное СКЗИ, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture) – КриптоПро JCP.

КРИПТОПРО NGate TLS-VPN

КриптоПро NGate — это универсальный высокопроизводительный TLS-VPN сервер и VPN, позволяющий быстро и безопасно реализовать защищённый доступ к веб-сайтам и корпоративным ресурсам через незащищённые каналы связи, в том числе сети общего пользования.

ГОСТ TLS

NGate обеспечивает одновременную поддержку TLS с ГОСТ и зарубежными криптоалгоритмами. Это позволяет реализовать плавный перевод защиты доступа к веб-сайтам на ГОСТ.

Компоненты **NGate** сертифицированы ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать **NGate** в том числе для защиты ПДн (152-ФЗ) при передаче по незащищенным каналам связи, в том числе из-за пределов РФ.

БЕЗОПАСНЫЙ ДОСТУП

Многофакторная аутентификация (по сертификату, LDAP / AD, Radius) и гибкое разграничение прав доступа к ресурсам.
Поддержка аппаратных ключевых носителей: Рутокен, eToken, JaCarta, ESMART и др.

ОБЛАСТЬ ПРИМЕНЕНИЯ

Субъекты КИИ, государственные органы, операторы ПДн, финансовые и иные организации, которым необходимо обеспечить защиту передаваемой информации и удаленного доступа.

НАГРУЗКА

Один узел шлюза **NGate** держит до **45 000 соединений** с обработкой информационных потоков до **20 Гбит/с** в режиме TLS-сервера. До **32 узлов** в кластере.

КриптоПро NGate

- @CryptoProAssistantBot
- info@cryptopro.ru
- +7 (495) 995-48-20
- https://cryptopro.ru

РЕЖИМЫ РАБОТЫ NGate

→ **Режим TLS-сервера** используется для безопасного подключения к веб-сайтам и снятия нагрузки по обработке TLS-соединений с веб-серверов. В данном режиме NGate может использоваться для обеспечения доступа к госпорталам, сайтам организаций и ДБО и др., предоставляющих доступ пользователей через веб-браузер. При этом доступ к веб-ресурсам возможен как напрямую без аутентификации, так и с аутентификацией через централизованной веб-портал, входящий в состав продукта.

→ **Режим VPN-сервера** используется для безопасного подключения с помощью VPN-клиента, поддерживающего все популярные ОС (в том числе мобильные), к произвольным корпоративным ресурсам.

Компания «ИнфоТеКС» (АО «Информационные Технологии и Коммуникационные Системы») — ведущий отечественный разработчик и производитель высокотехнологичных программных и программно-аппаратных средств защиты информации. Входит в ТОП-5 крупнейших вендоров в сфере защиты информации.

В портфеле ИнфоТеКС более 50 продуктов для защиты информации. Флагманская разработка — технология ViPNet, гибкое VPN-решение для безопасной передачи данных в защищенной сети. Более 10 млн рабочих станций защищены продуктами ViPNet.

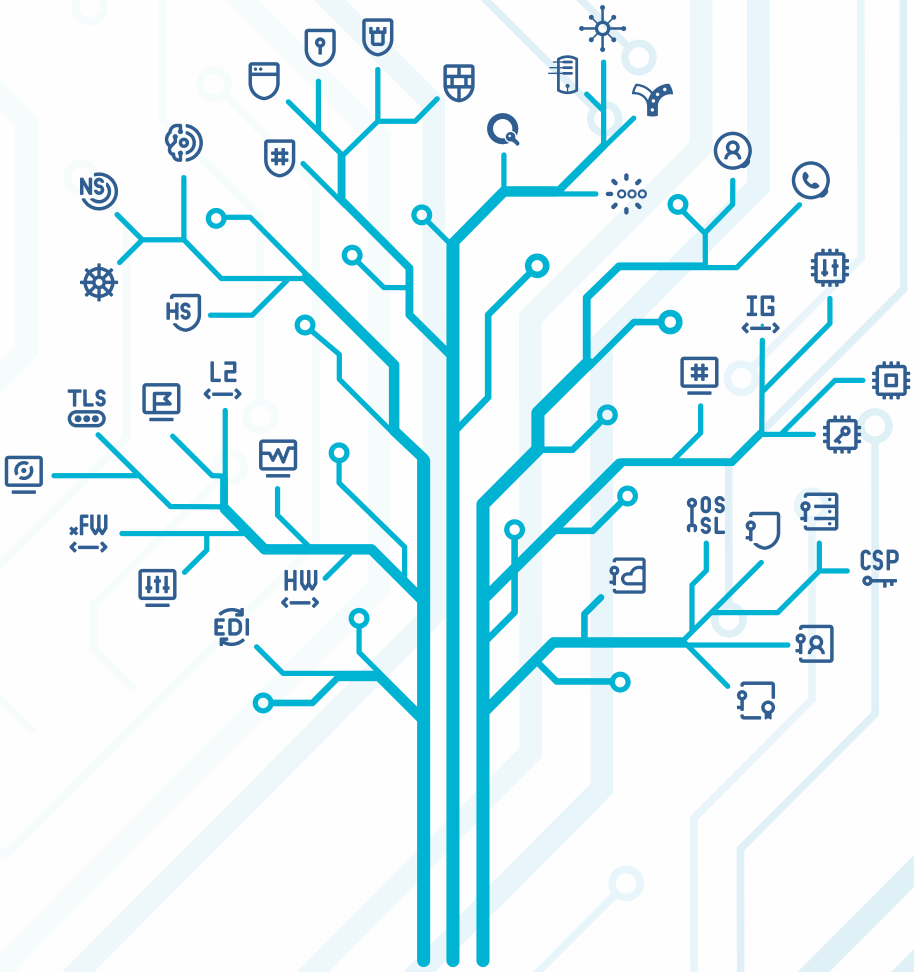
В штате компании более 1600 сотрудников, офисы открыты в 9 городах России, партнерская сеть включает в себя более 300 компаний.

Специалистами компании ведется активная работа в области нормотворчества. ИнфоТеКС выполняет роль секретарской компании в техническом комитете по стандартизации ТК № 26 «Криптографическая защита информации». Кроме этого, эксперты компании принимают активное участие в работе технических комитетов и экспертных советов, в том числе международной организации по стандартизации ИСО (ISO).

В группу компаний «ИнфоТеКС» входит 7 компаний, занимающихся исследованиями, разработкой и производством продуктов и решений в области информационной безопасности.

‹Мы защищаем информацию,
которую вы цените/›

>60
продуктов для защиты информации



>10 млн
рабочих станций защищенных продуктами ViPNet

infotecs
www.infotecs.ru

Компания «Актив» — российский разработчик средств информационной безопасности, крупнейший в России производитель электронных идентификаторов, электронных ключей и решений для защиты программного обеспечения. Компания была основана в 1994 году и сегодня объединяет бренды Рутокен и Guardant.

Продуктовый портфель компании содержит эффективные решения, направленные на повышение уровня информационной безопасности предприятий. У «Актива» накоплен обширный опыт реализации значимых проектов в ИКТ, корпоративном, финансовом и государственном секторах. Для этого у компании есть все необходимые лицензии ФСБ и ФСТЭК России на разработку и производство средств защиты информации.

Рутокен — первая в России полностью отечественная линейка аппаратных продуктов и решений для аутентификации и создания электронной подписи. Ключевые носители Рутокен используются везде, где требуется безопасное хранение и использование паролей, цифровых сертификатов, ключей шифрования и ключей электронной подписи. Электронные идентификаторы Рутокен представлены в различных форм-факторах: от стандартного USB-токена или смарт-карты до Bluetooth-устройств.

Линейка Guardant — это стандарт де-факто на российском рынке защиты и лицензирования ПО. Более 20 лет компания последовательно развивает собственное производство, которое не имеет аналогов в стране. Программный код всех устройств полностью создан разработчиками «Актива». Решения Рутокен и Guardant включены в единый реестр отечественного ПО.

КОМПАНИЯ АКТИВ

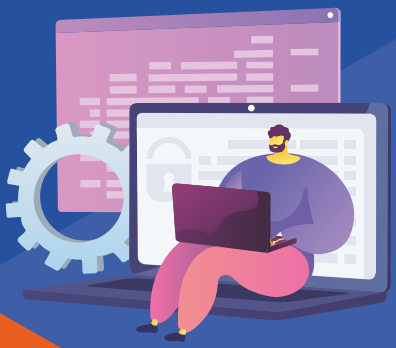
Российский производитель
и разработчик программно-
аппаратных средств
защиты информации

РУТОКЕН

Аутентификация и электронная подпись

Guardant

Защита и контроль
распространения программных
продуктов



AKTIV. CONSULTING

Консалтинг и аудит информационной
безопасности

www.aktiv-company.ru

«С-ТерраСиЭсПи» – российский разработчик и производитель средств сетевой безопасности на основе технологии IPsec VPN.

Продукты С-Терра используют современные криптоалгоритмы ГОСТ, сертифицированы ФСТЭК России, ФСБ России и Минкомсвязи России, включены в Единый реестр российского ПО и в реестр Минпромторга.

Высокопроизводительные криптошлюзы линейки DP шифруют со скоростью до 50 Гбит/с и поддерживают технологию квантового распределения ключей (КРК).

Решения С-Терра обеспечивают защиту каналов связи между ЦОД, при межсетевом взаимодействии и при удалённом доступе, применяются для защиты ИСобъектов КИИ.

Продукция компании применяется в государственных учреждениях различных уровней, крупнейших финансовых организациях, производственных предприятиях.

s•terra®

Ваш ориентир в мире безопасности

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ

- канал ЦОД-ЦОД
- виртуальные сети
- удалённый доступ
- распределённые сети
- обнаружение сетевых атак
- доступ с мобильных устройств
- IP-видеокамеры, банкоматы, ВКС

СДЕЛАНО В РОССИИ!

Москва · Зеленоград
Тел.: +7 (499) 940 9061 · www.s-terra.ru

QRATE
QUANTUM SOLUTIONS

QRate разрабатывает и поставляет комплексные аппаратно-программные решения для обеспечения информационной безопасности с помощью квантовых технологий. Компания обладает технологиями и оборудованием для организации передачи симметричных ключевых документов в шифраторы заказчика.

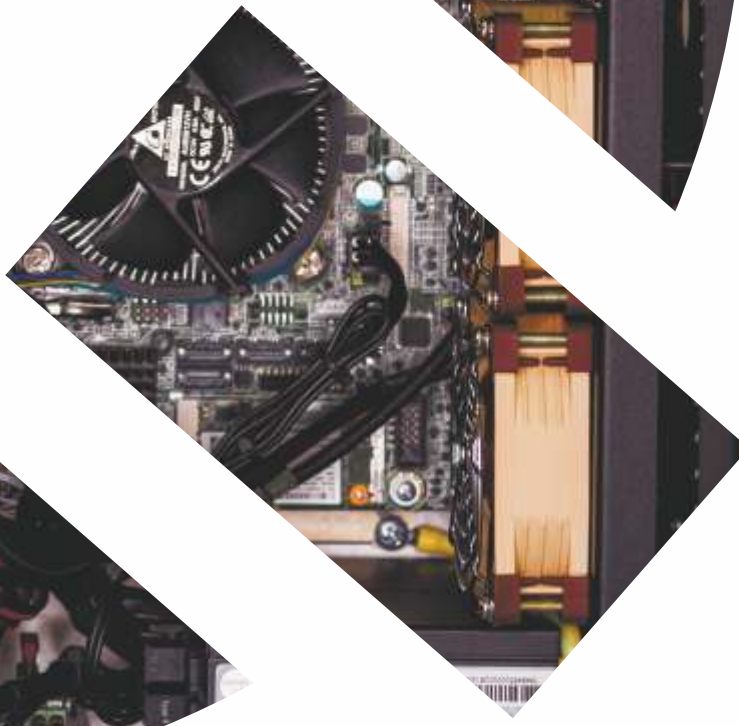
Реализуемые продукты и проекты:

- QRate QKD312 – технология высокоскоростного квантового распределения ключей на расстояние до 120 км;
- QRate QKD312 mini – технология квантового распределения ключей для разворачивания сетей в топологии звезда;
- QRate Chaos – квантовый генератор случайных чисел;
- QRate Lab – учебная квантовая лаборатория для образовательных и научных проектов.

Qrate является членом консорциума НТИ «Квантовые коммуникации» и стратегическим партнером НИТУ «МИСиС», реализует профстандарты и методические программы подготовки в учебных заведениях. Исследования осуществляются при грантовой поддержке Фонда «Сколково».

QRATE

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ГАРАНТИРОВАННАЯ ФУНДАМЕНТАЛЬНЫМИ ЗАКОНАМИ ФИЗИКИ



goqrate.com
+7(495) 114-55-17
mail@goqrate.com

КРИПТОНИТ

«Криптонит» — технологическая и научно-исследовательская компания, ведущая разработки в области криптографии, машинного обучения и других перспективных сферах ИТ, а также создающая современные платформенные решения на базе искусственного интеллекта. Входит в структуру «ИКС Холдинга», российской многопрофильной ИТ-группы, в основные задачи которой входят управление и консолидация на рынке телеком-медиа и технологий.

В числе приоритетных направлений работы: криптография, телекоммуникации, технологии и решения в области хранения, обработки и управления большими данными, машинное обучение и нейросети, информационная безопасность.

КРИПТОНИТ

«КРИПТОНИТ» — технологическая и научно-исследовательская компания

РАЗРАБАТЫВАЕМ

создаем продукты, которые решают актуальные задачи в области больших данных, телекоммуникаций, криптографии и информационной безопасности.

ПОДДЕРЖИВАЕМ НАУКУ

занимаемся научными исследованиями и опытными разработками.

ПРОСВЕЩАЕМ

открыли первый в России научно-технологический музей, посвященный криптографии.

kryptonite.ru

Telegram-канал

СМАРТС
КВАНТТЕЛЕКОМ

Компания ООО «СМАРТС-Кванттелеком» является ведущим российским разработчиком и производителем квантовых криптографических систем выработки и распределения ключей (ККС ВРК).

Компания выполняет научно-исследовательские и опытно-конструкторские работы в области систем квантовой коммуникации, квантовых генераторов случайных чисел, волоконно-оптической связи и фотоники, участвует в проектировании и строительстве квантово-защищенных сетей.

Для повышения уровня защищенности данных в качестве источника ключей мы применяем системы квантового распределения ключей на боковых частотах (КРКБЧ).
Эта оригинальная технология позволяет создавать экономически эффективные инфраструктуры сетевой безопасности нового поколения на квантовых принципах.

Разрабатываемые на их основе решения обеспечивают защиту информации с использованием классических и квантовых подходов (обновление ключей устройств криптографической защиты информации (СКЗИ) с помощью квантовых криптографических систем выработки и распределения ключей (ККС ВРК)).

На текущий момент пилотные зоны защищенной сети организованы в Санкт-Петербурге, Казани и Самаре.

Основу нашей команды составляют доктора и кандидаты наук Университета ИТМО, опытные разработчики аппаратных и программных средств защиты информации.
Мы ведем непрерывные теоретические и прикладные исследования в области квантовых коммуникаций, наши сотрудники принимают участие в ведущих всероссийских и международных конференциях, результаты исследований публикуются в ведущих мировых журналах.

О компании

Компания ООО "Кванттелеком"
является ведущим российским разработчиком
и производителем систем квантовой рассылки ключей

СМАРТС
КВАНТТЕЛЕКОМ

- Разработка и производство квантового оборудования
- Проектирование квантово-защищенных сетей
- Консалтинг и обучение специалистов по направлению «Квантовые коммуникации»

Квантовые криптографические системы выработки и распределения ключей

Детектор одиночных фотонов

Контакты

199178, Санкт-Петербург, В.О.,
6 линия д.59, корп. 1, лит. Б

+7 (812) 244-29-23

info@quanttelecom.ru

quanttelecom.ru

Модуляторы для оптических, радиофотонных и квантовых систем

Sk Технопарк

НЕОБИТ

Компания «НеоБИТ» создана командой ведущих специалистов в области информационной безопасности для продвижения на российский и мировой рынок решений и передовых технологий, разрабатываемых российскими учеными, отечественных продуктов и решений, направленных на обеспечение защиты информационных систем.

В компании работают доктора и кандидаты технических наук, ведущие специалисты высшей квалификации в области защиты информации, создания телекоммуникационных систем и систем связи. Профессионализм наших сотрудников подтвержден опытом реализации проектов различного масштаба, многочисленными дипломами и сертификатами.

Профиль компании – проектирование и разработка продуктов и решений, обеспечивающих безопасность информации, создание защищенных информационных систем.

НЕОБИТ

NEOBIT

НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Офис: 195220, Санкт-Петербург, ул. Гжатская, д. 21, литера “Г”
Тел. / факс: 8 812 535-28-06 / 8 812 535-88-67

www.neobit.ru

#УЧИСЬВАИС

АИС

НАМ 25 ЛЕТ!

АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

Академия Информационных Систем (АИС) – это учебный центр дополнительного профессионального образования в сфере информационных технологий, информационной безопасности, конкурентной разведки и экономической безопасности.

АИС – комфортное обучение онлайн и офлайн

- учебные курсы, согласованные с регуляторами (ФСБ, ФУМО, ФСТЭК, Банк России)
- единственный учебный центр с лицензией на обучение по направлению «Конкурентная разведка»
- подготовка к сдаче на международные сертификаты CISA, CISM, CGEIT, CISSP, CEH, CCNA, CCIE

+7 (495) 120-04-02 info@infosystem.ru www.nfosystems.ru | www.vipforum.ru

КАЛЕНДАРЬ МЕРОПРИЯТИЙ АИС 2022

21 АПРЕЛЯ 2022
МОСКВА

Весенняя сессия
AntiFraud Spring Russia

Обсуждение актуальных проблем правоприменения федеральных законов и нормативно-правовых актов в области противодействия фроду, обмен практическим опытом, улучшение взаимодействия банков и операторов связи, e-commerce при выявлении и предотвращении кибермошенничества.

7 - 9 ИЮНЯ 2022
СОЧИ

Всероссийский форум
по электронному документообороту
Форум ЭДО-2022

Конференция посвящена вопросам развития цифровых услуг при взаимодействии государства, бизнеса и граждан. На конференции обсуждаются проблемы развития и внедрения Электронного документооборота, электронных подписей и связанных с ними сервисов применительно ко всем отраслям экономики.

СЕНТЯБРЬ 2022
ЯЛТА

Всероссийский Форум
Информационная безопасность. Регулирование. Технологии. Практика. Инфоберег

Главная тема: Нормативное правовое регулирование в области ИБ, перспективы развития, практический опыт, решение проблемных вопросов в ИБ.
Проводится в рамках Летней Академии АИС.

ДЕКАБРЬ 2022
МОСКВА

Неделя безопасности АИС.
X Практическая конференция
Конкурентная разведка & Экономическая безопасность

Самые актуальные и интересные доклады в области экономической безопасности, конкурентной разведки, информационного противоборства и аналитики. Лучшие практики и готовые решения по защите бизнеса.

ДЕКАБРЬ 2022
МОСКВА

Неделя безопасности АИС.
XIII Международный форум
Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia

Организационные, юридические и технологические аспекты борьбы с мошенничеством. Управление рисками, практика расследования инцидентов и привлечение к ответственности злоумышленников.

МАРТ 2023
ПОДМОСКОВЬЕ

XXV Международная
научно-практическая конференция
РусКрипто'2023

Главная тема: использование криптографических средств и методов защиты информации, юридическое оформление электронного документооборота, обзоры основных достижений криптологии, криптографии.

конференция
РусКрипто

РАСПИСАНИЕ

СПОРТИВНЫХ ТУРНИРОВ

22 МАРТА
17:00 - 19:00
РАЗВЛЕКАТЕЛЬНЫЙ КОМПЛЕКС

- ТУРНИР ПО БИЛЬЯРДУ
- НАСТОЛЬНЫЙ ТЕННИС
- БОУЛИНГ

ВЫИГРЫВАЙТЕ КРИПТО РУБЛИ И ОБМЕНИВАЙТЕ ИХ НА ЦЕННЫЕ ПРИЗЫ

конференция
РусКрипто

СОРЕВНОВАНИЯ

В СПА-КОМПЛЕКСЕ

22 МАРТА
17:00 - 18:30

- Плавание
- Сквош
- Армрестлинг

ВЫИГРЫВАЙТЕ КРИПТО РУБЛИ
И ОБМЕНИВАЙТЕ ИХ НА ЦЕННЫЕ ПРИЗЫ

ГАЛА УЖИН

Торжественное открытие XXIV международной научно-практической конференции

23.03.22 | **НАЧАЛО В 20:00**
ЗАЛ «ШИШКА», 2 ЭТАЖ

РОЗЫГРЫШ ПРИЗОВ ПРОЙДЕТ С ПОМОЩЬЮ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЦИФР, КОТОРЫЕ БУДУТ УКАЗАНЫ НА ВАШИХ КРИПТО РУБЛЯХ

ИНТЕЛЛЕКТУАЛЬНЫЙ
КРИПТОГРАФИЧЕСКИЙ КВИЗ

ИГРА
В ИМИТАЦИЮ

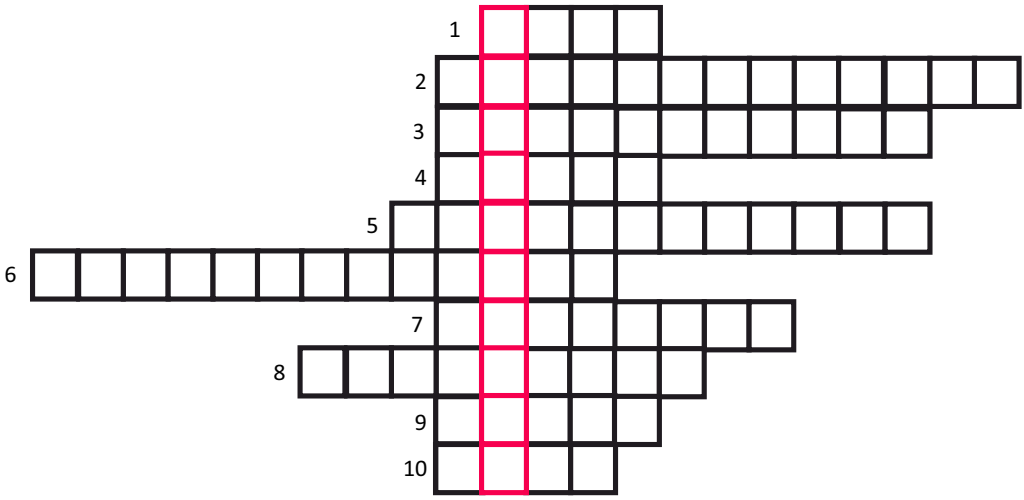
24 МАРТА, 20:00

ЗАЛ «ШИШКА», 2 ЭТАЖ

РусКрипто

ИНТЕЛЛЕКТУАЛЬНЫЙ
КРИПТОГРАФИЧЕСКИЙ КВИЗ
«ИГРА В ИМИТАЦИЮ»
С АЛЕКСЕЕМ ЛУКАЦКИМ

КРИПТО КРОССВОРД



1. Общедоступный параметр криптографического механизма, обеспечивающий невозможность использования в ходе атаки результатов повторного применения данного механизма к одному и тому же набору входных данных
2. Технология, обеспечивающая возможность восстановления криптографического ключа при участии заранее определенных центров доверия
3. Синоним термина “шифрование”, используемый дилетантами, наряду с “шифрация” и “шифрированием”.
4. Процедура аннулирования сертификата в случае его компрометации
5. Битовая строка, добавляемая к сообщению и являющаяся результатом применения к нему криптографической хеш-функции, зависящей от ключа, с целью обнаружения подмены и защиты от навязывания.
6. Способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения)
7. Специальное разрешение на право осуществления выполнения работ или оказания услуг в области шифрования.
8. Свойство криптосистемы или отдельного криптографического механизма характеризующее их способность противостоять атакам на криптосистему
9. Псевдослучайная последовательность элементов данных, вырабатываемая по заданному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных путем комбинирования с ними с использованием обратимой бинарной операции.
10. Браузер, в который встроен корневой сертификат Минцифры.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Event.Rocks

Отсканируйте QR-код
или введите название
приложения Event.Rocks
в App Store и Google Play.

В приложении введите
ID события —

РУСКРИПТО2022

и далее, следуя инструкции,
авторизуйтесь в вашем профиле

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

При поддержке Ивентищее

+7 (495) 120-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru