ОРГАНИЗАТОРЫ

Ассоциация РусКрипто

АИС

25-Я МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РусКрипто’2023

21 - 24 МАРТА СОЛНЕЧНЫЙ HOTEL & SPA

ПРОГРАММА

БЛАГОДАРИМ СПОНСОРОВ И ПАРТНЕРОВ ЗА ОКАЗАННУЮ ПОДДЕРЖКУ!

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

КРИПТОПРО
ключевое слово в защите информации

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

infotecs

ЭКСКЛЮЗИВНЫЙ ГЕНЕРАЛЬНЫЙ ПАРТНЕР

ГАЗПРОМБАНК
Банк ГПБ (АО)

ОФИЦИАЛЬНЫЕ ПАРТНЕРЫ

КОМПАНИЯ АКТИВ

СПБ

СМАРТС КВАНТТЕЛЕКОМ

INTEGRA
PHOTONICS
DATATECH
BIOTECH
PROFTECH

ПАРТНЕР СЕССИИ

ЭЛВИС-ПЛЮС

НАУЧНЫЙ ПАРТНЕР

НЕОБИТ

КУЛЬТУРНЫЙ ПАРТНЕР

МУЗЕЙ КРИПТОГРАФИИ

ПАРТНЕРЫ ВЫСТАВКИ

с•терра

SPACE-BIT

АССОЦИАЦИЯ РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ

ПАРТНЕРЫ КОНФЕРЕНЦИИ

ANSWER pro

QApp

QRATE
QUANTUM SOLUTIONS

GIS ГАЗИНФОРМ СЕРВИС

QSpace Technologies

СТЦ
СПЕЦИАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР

АПКИТ

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

Связист

BIS JOURNAL

ВСЕ МЕРОПРИЯТИЯ ИТ НА ICT2GO

ICT ONLINE
ИНФОКОММУНИКАЦИИ ОНЛАЙН

АБИСС

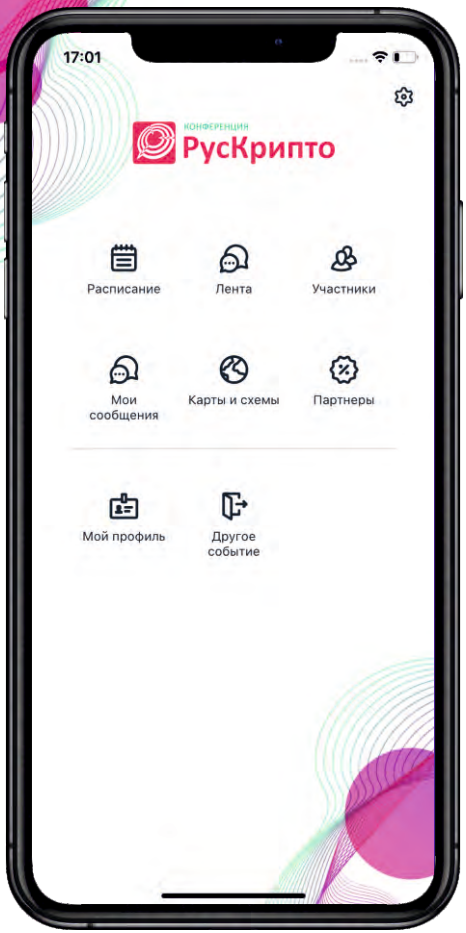
NBJ

CISOCLUB

CYBER MEDIA

БИТ

Системный администратор



Event.Rocks

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

В приложении введите ID события -

РУСКРИПТО2023

и далее, следуя инструкции, авторизируйтесь 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 Ивентницы

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»

22 марта в 08:00 утра трансфер **м. СТРОГИНО** - отель «Солнечный Park Hotel & SPA»

22 марта в 20:00 вечера трансфер отель «Солнечный Park Hotel & SPA» - **м. СТРОГИНО**

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

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

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

24 марта в 12:00 трансфер отель «Солнечный Park Hotel & SPA» - **м. СТРОГИНО**
Подача у ворот отеля.

Внимание! *Автобусы отправятся ровно в 12:00.*
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 - 21 марта с 16:00
Выезд - 24 марта до 12:00

22 и 23 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»

ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ

ОБЩАЯ ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ

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

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

- Получить закрывающие документы вы сможете на стойке регистрации 22-23 марта.

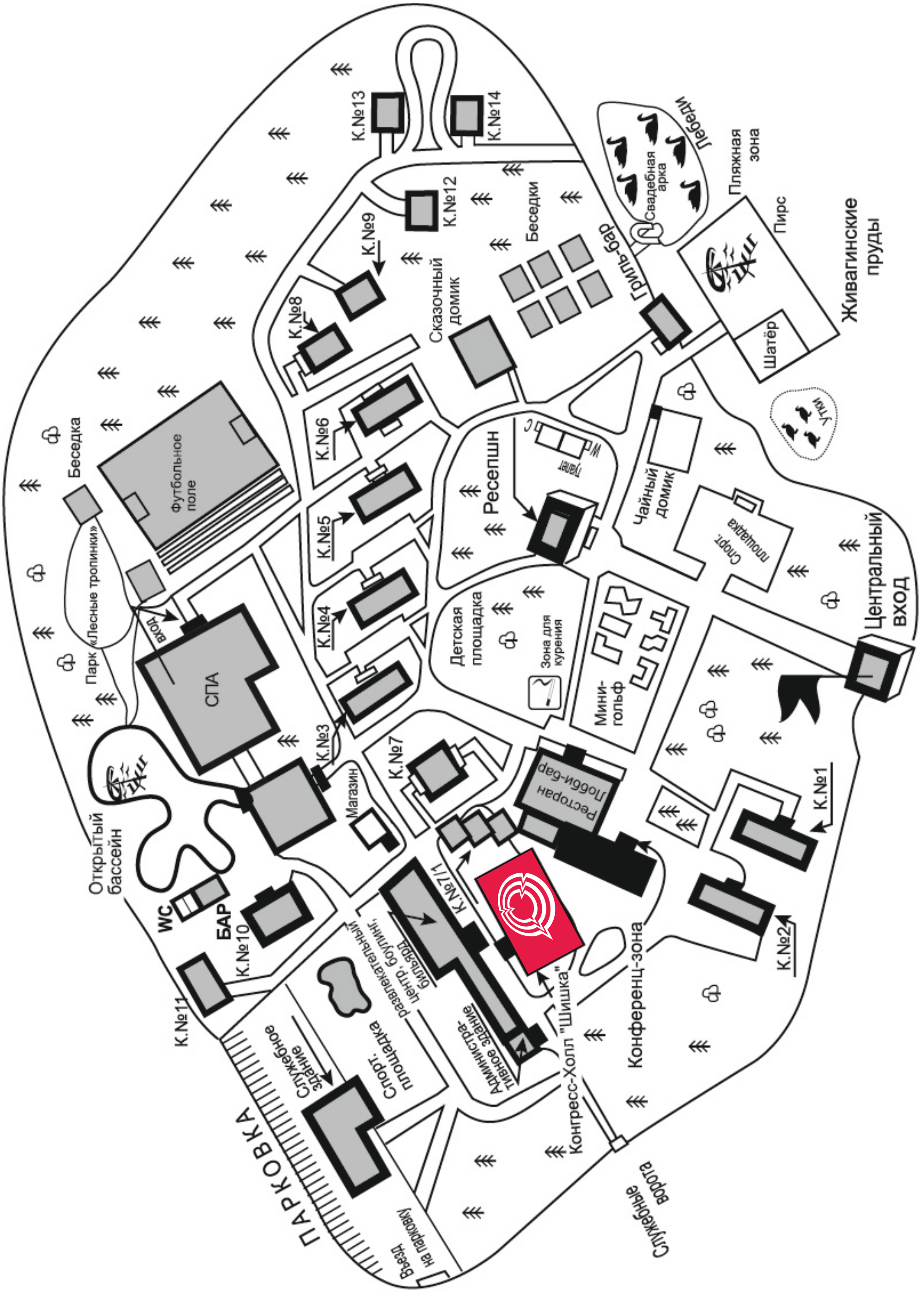
ОБСЛУЖИВАНИЕ В ОТЕЛЕ ПО СИСТЕМЕ «ВСЕ ВКЛЮЧЕНО»:

- расширенный шведский стол: завтрак (08:00-11:00), обед (13:00-16:00), ужин (19:00-23:00);
- в течение всего дня с 08:00 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.

22 и 23 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»



К.№13
К.№14
Лебеди
Свадебная арка
Пляжная зона
К.№12
К.№9
Беседки
Гриль-бар
Пирс
Живагинские пруды
Шатёр
К.№8
Сказочный домик
Утки
Беседка
Футбольное поле
К.№6
Ресепшн
Туалет
Чайный домик
Спорт. площадка
К.№5
Центральный вход
Парк «Лесные тропинки»
вход
К.№4
Детская площадка
Зона для курения
Мини-гольф
СПА
К.№3
К.№7
Ресторан Лобби-бар
К.№1
Открытый бассейн
Магазин
К.№711
WC
БАР
К.№10
Развлекательный центр, боулинг, бильярд
К.№2
К.№11
Конференц-зона
Служебное здание
Спорт. площадка
Административное здание
Конгресс-Холл "Шишка"
ПАРКОВКА
Въезд на парковку
Служебные ворота

22 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

09:00 – 10:00	Регистрация участников конференции		
10:00 – 12:00	**Официальное открытие конференции. Пленарное заседание** Зал «Шишка» *11 стр.*		
12:00 – 12:30	Кофе-брейк		
12:30 – 14:00	Зал «Шишка» Круглый стол **«Криптографические средства в государственных информационных системах»** Ведущие: · Маслов Ю.Г., КриптоПро · Романов К.О., ФТС России *11-12 стр.*	Кино-концертный зал Секция **«Исследование и защита цифровых технологий»** Ведущие: · Чиликов А.А., МГТУ им. Баумана · Комисаренко В.В., LWO *12-13 стр.*	Зал «Еловый» Экспертная панель **«Кадры завтрашнего дня. Популяризация криптографии и вовлечение в профессию»** Ведущая: Токарева Н.Н., лаборатория криптографии ММЦ НГУ *13 стр.*
14:00 – 15:00	Обед		
15:00 – 16:30	Зал «Еловый» Экспертная панель **«Практические вопросы применения технологий электронной цифровой подписи в РФ»** Ведущий: Горелов Д.Л., компания «Актив», Ассоциация «РусКрипто» *13-14 стр.*	Зал «Сосновый» Секция **«Решения, продукты и технологии ИБ»** Ведущий: Поташников А.В., АО «ИнфоТеКС» *14 стр.*	Кино-концертный зал **Научный лекторий** Ведущий: Коваленко А.П., Академия криптографии Российской Федерации *15 стр.*
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Зал «Сосновый» Секция **«Криптография и информационная безопасность в банковской сфере»** Ведущий: Елистратов А.А., Банк России *15-16 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», 1 часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *16-17 стр.*	Кино-концертный зал Секция **«Применение методов искусственного интеллекта в задачах кибербезопасности»** Ведущие: · Зегжда Д.П., ИКиЗИ СПбПУ · Овасапян Т.Д., ИКиЗИ СПбПУ *17-18 стр.*
19:00 – 23:00	**Гала-ужин юбилейной конференции РусКрипто’2023** Зал «Шишка»		

23 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 11:30	Зал «Шишка» Секция **«Российские криптографические средства защиты информации. Требования, разработка, внедрение и эксплуатация»** Ведущие: · Папаев И.С., ФСБ России · Хачатуров А.И., Ансер-Про *18-19 стр.*	Зал «Еловый» Секция **«Технологии цепной записи данных и распределенных реестров»** Ведущие: · Чубаров Р.Ю., ФНС России · Панасенко С.П., компания «Актив» *19-20 стр.*	Зал «Сосновый» Секция **«Квантовые коммуникации и квантовая криптография», 1 часть** Ведущий: Уривский А.В., ИнфоТеКС *20-21 стр.*
11:30 – 12:00	Кофе-брейк		
12:00 – 14:00	Зал «Шишка» Экспертная панель **«Электронный документооборот и электронная подпись»** Ведущий: Малинин Ю.В., Ассоциация РОСЭУ *22 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», 2 часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *22-24 стр.*	Зал «Сосновый» Секция **«Квантовые коммуникации и квантовая криптография», 2 часть** Ведущий: Уривский А.В., ИнфоТеКС *24 стр.*
14:00 – 15:00	Обед		
15:00 – 16:30	Зал «Сосновый» Секция **«Криптография в энергетической отрасли»** Ведущий: Щербаков А.В., ФСБ России *25 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», 3 часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *26-27 стр.*	Кино-концертный зал Секция **«Перспективные исследования в области кибербезопасности», 1 часть** Ведущий: Котенко И.В., СПб ФИЦ РАН *27-28 стр.*
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Зал «Еловый» Круглый стол **«Подготовка и трудоустройство специалистов в области ИБ»** Ведущий: Белов Е.Б., ФУМО СПО ИБ *28-29 стр.*	Кино-концертный зал Секция **«Перспективные исследования в области кибербезопасности», 2 часть** Ведущий: Котенко И.В., СПб ФИЦ РАН *29-30 стр.*	

КУЛЬТУРНО-РАЗВЛЕКАТЕЛЬНАЯ ПРОГРАММА

21 МАРТА, ВТОРНИК

15:00	Трансфер: метро «Строгино» – отель «Солнечный Park Hotel & SPA»	
16:00 – 22:00	Заезд и регистрация участников, проживающих в отеле	
19:00 – 20:00	Ужин	
20:00 – 22:00	Иммерсивный спектакль	Кино-концертный зал
20:00 – 22:00	Криптографический квиз «Игра в имитацию» с Алексеем Лукацким	Зал «Еловый»

22 МАРТА, СРЕДА

08:00 – 09:00	Завтрак	
08:00 – 09:00	Практика на Досках с гвоздями на РусКрипто’23	Зал «Стеклянный»
12:00 – 13:00	Мастер-классы «Шифр в кармане. Как шифровали в XX веке» и «Послание с секретом. Исследуем древние шифры» для детей и их родителей	Развлекательный комплекс
19:00 – 23:00	Гала-ужин юбилейной конференции РусКрипто’2023	Зал «Шишка»

23 МАРТА, ЧЕТВЕРГ

08:00 – 09:00	Завтрак	
08:00 – 09:00	Практика на Досках с гвоздями на РусКрипто’23	Зал «Стеклянный»
20:00 – 22:00	Вечернее шоу «Боксерский поединок»	Зал «Шишка»

24 МАРТА, ПЯТНИЦА

08:00 – 11:00	Завтрак	
08:00 – 09:00	Практика на Досках с гвоздями на РусКрипто’23	Зал «Стеклянный»
10:00 – 11:00	Банный релакс в спа-зоне	Спа-зона отеля
12:00	Трансфер из отеля до станции метро «Строгино»	

ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

(в программе возможны изменения)

10:00 – 12:00 Пленарное заседание

Зал «Шишка»

Официальное открытие конференции. Приветственные слова:

- ФСБ России
- Минцифры России
- Банк России
- АО «ИнфоТеКС»
- Компания КриптоПро

Дистанционное электронное голосование как источник инновационных криптографических задач
Матюхин Дмитрий Викторович, *к.ф.-м.н., ФСБ России*

О внедрении криптографии в информационные системы цифровой экономики
Шойтов Александр Михайлович, *д.ф.-м.н., заместитель министра цифрового развития, связи и массовых коммуникаций Российской Федерации*

Криптозащита в современных условиях обеспечения информационной безопасности
Баранов Александр Павлович, *д.ф-м.н., действительный член Академии криптографии Российской Федерации*

«Соединение защищено». Достижения и задачи в области защищенного доступа к веб-сайтам в России
Смышляев Станислав Витальевич, *д.ф.-м.н., заместитель генерального директора, КриптоПро*

Защита информационных систем на основе комбинации устройств квантового распределения ключей и постквантовых алгоритмов
Фёдоров Алексей Константинович, *руководитель научной группы «Квантовые информационные технологии» Российского квантового центра, основатель компании QApp*

12:30 – 14:00 Круглый стол «Криптографические средства в государственных информационных системах»

Зал «Шишка»

В круглом столе примут участие представители крупнейших государственных органов, использующих в своих информационных системах технологии электронной подписи и криптографические решения. Представители регулятора, разработчики криптосредств и руководители подразделений ИБ крупнейших ФОИВ-ов обсудят наболевшие вопросы, поделятся опытом и озвучат актуальные задачи, которые помогут развитию криптографической отрасли в интересах государства.

Ведущие:

- **Романов Кирилл Олегович,** начальник отдела информационной безопасности и технической защиты информации Службы информационной безопасности Главного управления информационных технологий ФТС России
- **Маслов Юрий Геннадиевич,** коммерческий директор компании КриптоПро, эксперт Ассоциации РОСЭУ

Эксперты:

- **Папаев Игорь Сергеевич,** ФСБ России
- **Бражко Вячеслав Сергеевич,** начальник Управления режима секретности и безопасности информации Федерального Казначейства
- **Данилов Сергей Николаевич,** начальник Управления информационной безопасности, Росреестр

К участию приглашены представители ФНС России, Минцифры, Банка России, СФР, ФССП.

12:30 – 14:00 Секция «Исследование и защита цифровых технологий»

Кино-концертный зал

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

Ведущие:

- **Чиликов Алексей Анатольевич,** к.ф.-м.н., доцент МГТУ им. Баумана
- **Комисаренко Владимир Владимирович,** заместитель директора по проектам в сфере защиты информации компании Light Well Organization (Республика Беларусь)

Технология автоматизированного подхода к реверс-инжинирингу обфускаторов-пакеров вредоносного кода

Раковский Станислав Александрович, *РТУ МИРЭА*

В ходе работы представлен подход к обратной разработке упакованного кода, в котором предположительно находится вредоносная активность, что накладывает дополнительные меры осторожности в процессе его анализа.

Особенности извлечения данных из Android устройств на китайских чипсетах

Карондеев Андрей Михайлович, *руководитель отдела исследований, МКО Системы*

Пользовательские данные на любом современном смартфоне хранятся в зашифрованном виде. ОС Android посредством TEE предполагает использование шифрования с защищенным на аппаратном уровне ключом. Тем не менее со стороны Android регламентирован интерфейс взаимодействия с TEE, а вот какая реализация TEE будет в конкретном устройстве во многом зависит от производителя устройства и модели чипсета. В докладе будут описаны некоторые детали реализации механизмов шифрования Android устройств на китайских чипсетах MediaTek, Unisoc и Kirin. Внимание будет уделено как крупным производителям типа Samsung, Xiaomi, Oppo, Huawei, так и некоторым заметно менее популярным, но с интересными особенностями реализации шифрования.

Автоматическая защита исполняемых модулей для ARM-архитектуры

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

Задача обфускации исполняемых модулей для ARM-архитектуры становится всё более востребованной, а хороших решений на рынке нет. В докладе рассматриваются существующие на текущий момент готовые протекторы и построенные на движке LLVM обфускаторы. Будет рассказано об одном из возможных решений связки протектора и обфускатора.

Как обезопасить от санкций ваш открытый проект на GitHub

Попов Александр Юрьевич, *главный исследователь безопасности открытых операционных систем, Positive Technologies*

На платформе GitHub зарегистрировано более 100 миллионов разработчиков. Это дает выход на огромную аудиторию, и поэтому многие open-source проекты разрабатываются там. С 2018 года компания Microsoft владеет платформой GitHub и в последнее время проводит на ней политику санкций и блокировок. В данном докладе будет рассказано о комплексе технических мер, которые позволяют снизить возможный ущерб от санкций для вашего открытого GitHub-проекта.

О снижении рисков атак, использующих программные закладки и уязвимости в проектах с открытым исходным кодом

Комисаренко Владимир Владимирович, *заместитель директора по проектам в сфере защиты информации компании Light Well Organization*

В настоящее время применение программного обеспечения с открытым исходным кодом приобретает особую актуальность. Перед владельцами информационных систем, применяющих такое ПО, остро встает проблема рисков, связанных с возможностью атак, использующих программные закладки и уязвимости в проектах с открытым исходным кодом. В докладе приводится обзор лучших мировых практик поиска и устранения уязвимостей, закладок. Предлагается классификация и соответствующе меры, направленные на снижение рисков. Выделяются особенности решения указанных задач для криптографического программного обеспечения.

12:30 – 14:00 Экспертная панель «Кадры завтрашнего дня. Популяризация криптографии и вовлечение в профессию»

Зал «Еловый»

Залог успешного будущего отечественной криптографии – в её крепком научном базисе, большом потенциале нашей талантливой молодёжи и широких возможностях для применения полученных знаний на практике. Участники дискуссии – академические учёные, музейные хранители традиций, представители сферы образования и специалисты-практики, расскажут о реализованных проектах, обменяются опытом вовлечения молодёжи в профессию и рассмотрят возможные пути популяризации криптографии и кибербезопасности.

Ведущая: Токарева Наталья Николаевна, руководитель Криптографического центра (Новосибирск), заведующая лабораторией криптографии Международного математического центра НГУ

Эксперты:

- **Лобанова Лидия Валерьевна,** директор научно-технологического Музея криптографии
- **Максименко Екатерина Павловна,** HR-директор АО «ИнфоТеКС»
- **Катышев Сергей Юрьевич,** эксперт ФУМО ИБ
- **Чижов Иван Владимирович,** заместитель руководителя лаборатории криптографии компании «Криптонит», к.ф.-м.н., доцент кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им М.В. Ломоносова
- **Селиванова Анна Юрьевна,** заместитель директора Института кибербезопасности и защиты информации СПбПУ по продвижению
- **Пудовкина Марина Александровна,** профессор НИЯУ МИФИ, заместитель заведующего кафедры «Криптография и безопасность компьютерных систем», руководитель образовательных программ бакалавриата и магистратуры кафедры Магистратура 10.04.01-«Информационная безопасность» название программы «Теоретическая и практическая криптография», директор Ассоциации «РусКрипто»

15:00 – 16:30 Экспертная панель «Практические вопросы применения технологий электронной цифровой подписи в Российской Федерации»

Зал «Еловый»

В рамках экспертной панели ведущие эксперты криптографической отрасли обсудят технологические аспекты российского рынка электронной подписи. Вопросы эксплуатации массовых средств электронной подписи, которые все шире используются гражданами и бизнесом. Вопросы совместимости криптосредств, встраивание электронной подписи в новые информационные системы. Использование асимметричной криптографии для идентификации и аутентификации субъектов и объектов информационных систем. Обзор текущего ландшафта использования ЭЦП и прогнозы на будущее.

Ведущий: Горелов Дмитрий Львович, управляющий партнер компании «Актив», директор Ассоциации «РусКрипто»

Эксперты:

- **Смышляев Станислав Витальевич,** д.ф.-м.н., заместитель генерального директора, КриптоПро
- **Гусев Дмитрий Михайлович,** заместитель генерального директора АО «ИнфоТеКС»
- **Мелузов Антон Сергеевич,** заместитель генерального директора РТЛабс
- **Сабанов Алексей Геннадьевич,** д.т.н., зам. генерального директора по науке АНО «НТЦ ЦК»

15:00 – 16:30 Секция «Решения, продукты и технологии ИБ»

Зал «Сосновый»

Секция, полностью посвящена российским разработчикам средств информационной безопасности. Презентации новых решений, перспективных технологий, продуктов. Обмен мнения и идеями, обсуждение профессиональной аудиторией.

Ведущий: Поташников Александр Викторович, заместитель директора центра разработки, АО «ИнфоТеКС»

Проблемы встраивания криптографии в прикладные системы. Что встраивать и как избежать ошибок?

Эм Арина Николаевна, *менеджер продуктов АО «ИнфоТеКС»*

В докладе будут рассмотрены новые подходы «ИнфоТеКС» к составу и архитектуре СКЗИ, предназначенных для встраивания в прикладные приложения. Обсудим сложности, с которыми сталкиваются наши заказчики при встраивании криптографии и пути их решения.

Практические аспекты применения стандартов по управлению компьютерными инцидентами

Сидак Алексей Александрович, *генеральный директор, ООО «ЦБИ»*

Разработаны и утверждены в конце 2022 года стандарты по управлению компьютерными инцидентами. С 1 февраля 2023 года стандарты введены в действие. В выступлении планируется доложить основные положения стандартов, взаимосвязь с иными национальными стандартами и практические вопросы реализации положений новых стандартов.

Использование протоколов технологии FIDO2 для выполнения электронной подписи данных отечественными криптоалгоритмами на смарт-картах

Сабиров Эдуард Радикович, *аналитик, компания «Актив»*

Мироненко Евгений Олегович, *руководитель отдела R&D, компания «Актив»*

Скоробогатова Марина Андреевна, *аналитик, компания «Актив»*

FIDO2 - технология беспарольной двухфакторной аутентификации, использующая международные криптографические алгоритмы. Данная технология имеет широкое распространение и поддерживается большинством браузеров без необходимости установки дополнительного программного обеспечения. В докладе представлен анализ возможности применения данной технологии в качестве основы для продуктов, реализующих электронную подпись документов в веб-приложениях с использованием смарт-карт с отечественными криптоалгоритмами.

Импортозамещение в экстренных условиях

Дударев Дмитрий Александрович, *исполнительный директор, ООО Фирма «АНКАД»*

Что делать, когда импортные комплектующие внезапно становятся недоступными? Как заменить в изделии ключевой компонент, сохранив при этом основные функциональные характеристики и, самое важное, сертификат соответствия? Отечественные разработчики СЗИ столкнулась с этими вопросами в начале 2022 года. Сейчас мы можем рассказать, как мы попытались решить некоторые из вышеперечисленных вопросов, как проходит срочная модернизация ПАК с переходом на новую элементную базу, и какие еще разработки пришлось делать в пожарном порядке.

15:00 – 16:30 Научный лекторий

Кино-концертный зал

Ведущий: Коваленко Андрей Петрович, вице-президент Академии криптографии Российской Федерации

17:00 – 19:00 Секция «Криптография и информационная безопасность в банковской сфере»

Зал «Сосновый»

В настоящее время в финансовой сфере появилось много новых, важных задач, связанных с обеспечением безопасности и устойчивости платежных систем и банковской деятельности. Финансовая система, являющаяся кровеносной системой экономики, как никакая другая сфера нуждается в цифровом суверенитете. Безопасность новых финансовых технологий, замещение критически важных компонентов информационной безопасности и совершенствование нормативной базы.

Ведущий: Елистратов Андрей Алексеевич, Банк России

О нормативных изменениях для финансовой отрасли, касающихся применения средств криптографической защиты информации и электронной подписи.

Зинюк Борис Фёдорович, *Академия криптографии Российской Федерации*

В связи с изменениями Положения Банка России № 683-П, вступившими в силу 1.10.2022, а также утверждением Положения Банка России № 757-П у финансовых организаций возникает ряд вопросов по трактовке формулировок. В первом докладе представители регулятора дадут разъяснения по применению подпункта 5.1 Положения №683-П и пункта 1.9 Положения № 757-П. Также в докладе будет изложено видение выполнения п. 12 Положения Банка России № 802-П.

Конфиденциальный скоринг с точки зрения криптографии

Кяжин Сергей Николаевич, *к.ф.-м.н., КриптоПро*

Митрофанов Александр Александрович, *к.т.н., ООО «Блуттех»*

Задачей скоринга в банковской сфере называется получение одним банком сумм некоторых метрик в других банках, характеризующих обслуживание их клиентов. Учитывая необходимость обеспечения банковской тайны, раскрытие информации в рамках данного процесса третьим лицам недопустимо. В докладе будут рассмотрены некоторые особенности построения модели угроз и модели нарушителя, присущие любому протоколу, решающему задачу конфиденциального скоринга.

Необходимость разработки и стандартизации ключевого контейнера TR31 с российскими криптографическими алгоритмами

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

Герасимова Алла Геннадьевна, *ООО «Системы практической безопасности»*

Габов Александр Александрович, *ООО «Системы практической безопасности»*

В настоящее время в финансовом секторе широко используется ключевой контейнер ACS X9 TR 31-2018, который применяется в индустрии платежных карт как основной и хорошо отражает платежную специфику за счет большого количества полей. При этом данный контейнер не допускает возможность хранения в нем ключей для российских криптографических стандартов. Создание TR 31 GOST и его поддержка в российских СКЗИ позволит кредитным и иным финансовым организациям шире использовать российские криптографические механизмы в привычных отрасли процессах.

Российский банкомат. Криптографическая защита

Евтушенко Владимир Олегович, *АО «СмартКард-Сервис»*

В докладе будут изложены принципы обеспечения защиты информации в банкоматах, являющиеся де-факто отраслевыми стандартами. Подходы и необходимые направления деятельности при реализации комплексного импортозамещения современных банкоматов.

Круглый стол: Аппаратные модули безопасности. Применение. Тенденции развития

Уже традиционно на секции поговорим в формате круглого стола о задачах и путях их решения, встающих в Российской Федерации в сфере информационной безопасности карточных платежных систем.

Эксперты:

- **Простов Владимир Михайлович,** КриптоПро
- **Мареева Елена Владимировна,** ООО «Системы практической безопасности»
- **Шибина Ольга Михайловна,** ГК Штрих-М
- **Горелов Дмитрий Львович,** компания «Актив»
- **Качалин Алексей Игоревич,** ПАО «Сбербанк»

17:00 – 19:00 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

О постквантовой стойкости на примере схемы подписи «Шиповник»

Царегородцев Кирилл Денисович, *старший специалист-исследователь лаборатории криптографии АО «НПК «Криптонит»*

На примере схемы подписи «Шиповник» будет обсуждено несколько «узких мест», которые возникают при изучении стойкости криптографических примитивов и протоколов в условиях нарушителя, имеющего доступ к квантовому компьютеру.

Схемы инкапсуляции ключа на основе кодов, исправляющих ошибки

Высоцкая Виктория Владимировна, *НПК «Криптонит», МГУ им. М.В. Ломоносова*

Чижов Иван Владимирович, *к.ф.-м.н., НПК «Криптонит», МГУ им. М.В. Ломоносова*

Описание существующих подходов к построению KEM на основе схем шифрования с открытым ключом. Сравнение оценок стойкости и параметров KEM, полученных различными способами. Вариант схемы KEM на кодах, исправляющих ошибки, для возможной дальнейшей стандартизации в РФ.

Гиперикум — проект квантово-устойчивой схемы цифровой подписи для стандартизации в России

Гребнев Сергей Владимирович, *руководитель направления прикладных исследований QApp*

В докладе будет рассмотрен разработанный в рамках деятельности рабочей группы 2.5 «Постквантовые криптографические механизмы» ТК 26 проект схемы цифровой подписи «Гиперикум», его синтезные принципы, основные свойства и характеристики.

О проблеме классификации AKE-протоколов

Алексеев Евгений Константинович, *к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро*

Бабуева Александра Алексеевна, *ведущий инженер-аналитик, КриптоПро*

Зазыкина Ольга Александровна, *магистрант, МТУСИ*

В настоящей работе предлагается подход к единообразному описанию протоколов аутентифицированной выработки общего ключа (AKE-протоколов), а также принципы классификации настоящих протоколов с точки зрения их конструктивных особенностей.

Гибридный пост-квантовый обмен ключами в интернет-протоколах

Смыслов Валерий Анатольевич, *архитектор системы отдела разработки ПО, АО «ЭЛВИС-ПЛЮС»*

Гибридный пост-квантовый обмен ключами позволяет снизить риски, связанные с недостаточной глубиной анализа, которому на сегодняшний день подвергались различные пост-квантовые механизмы. Однако его использование в интернет-протоколах вызывает определенные проблемы как криптографического, так и инженерного свойства. Как эти проблемы решаются на практике на примере реализации гибридного пост-квантового обмена ключами в протоколах IKEv2 и TLS 1.3.

Эффект плацебо в криптографии

Фомин Денис Бонифатович, *ТК 26*

В настоящее время сформировались различные подходы к оценке стойкости криптографических механизмов. При этом различные авторские коллективы и научные школы либо стараются придерживаться одного конкретного подхода, если он в достаточной степени прошел «проверку временем», либо предлагают свои «авторские» решения. В докладе рассмотрены два подхода, наиболее часто встречающиеся в отечественной литературе. Первый подход определяется средней трудоемкостью алгоритма нарушения свойств безопасности данных. Второй подход связан с так называемой «доказуемой стойкостью». Кратко описаны оба подхода, а также их положительные и отрицательные стороны. Сформулирован ряд открытых задач и выявлены скрытые угрозы, обусловленные использованием только подхода на основе доказуемой стойкости.

17:00 – 19:00 Секция «Применение методов искусственного интеллекта в задачах кибербезопасности»

Кино-концертный зал

Вследствие последних тенденций в области цифровизации идет неуклонный рост как объема, так и сложности данных, которые генерируются в информационном пространстве. Возможности искусственного интеллекта открывают новые перспективы для современных средств защиты информации, однако, цена ошибки в их применении очень высока. В рамках секции будут рассмотрены некоторые аспекты методов искусственного интеллекта в задачах обеспечения информационной безопасности и возникающие при этом сложности.

Ведущие:

- **Зегжда Дмитрий Петрович,** чл.-корр. РАН, директор Института кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого, Санкт-Петербург
- **Овасапян Тигран Джаникович,** к.т.н., доцент, Институт кибербезопасности и защиты информации СПбПУ, Санкт-Петербург

Анализ методов обнаружения искусственно синтезированного контента

Данилов Владислав Дмитриевич, *Институт кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого*

Доклад посвящен синтетическому контенту, сгенерированному с помощью методов глубокого обучения. В докладе анализируются актуальные подходы к обнаружению искусственных данных. Также приводится экспериментальная оценка эффективности различных методов с помощью разработанного макета автоматизированной системы обнаружения синтетического контента.

Выявление состязательных атак на системы обнаружения вторжений с помощью нейронных сетей

Югай Павел Эдуардович, *ООО «Лаборатория кибербезопасности»*

Современные системы обнаружения вторжений активно используют алгоритмы машинного обучения для выявления угроз. В связи с этим существует проблема безопасности данных средств защиты информации, заключающаяся в состязательных примерах для обучающих наборов данных обнаружения сетевых вторжений. В докладе рассматриваются примеры и способы реализации состязательных атак на алгоритмы машинного обучения в системах обнаружения вторжений, а также методы обнаружения данных атак с применением нейронных сетей.

Применение методов машинного обучения для автоматизированного развертывания honeypot-систем

Писков Александр Александрович, *Институт кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого*

Методы, используемые злоумышленниками для проведения атак, могут быть собраны с использованием нескольких подходов, одним из которых являются системы-приманки (honeypot). Эффективность этих систем для сбора информации об атаках в значительной степени зависит от их способности представлять реалистичную среду, которая может побудить злоумышленников раскрыть свои методы.
В докладе будут рассмотрены реализации адаптивных приманок, ориентированных на использование методов машинного обучения для достижения более реалистичного взаимодействия со злоумышленником. Также будут рассмотрены показатели производительности таких систем.

Защита узлов от распределенного сканирования из сети Интернет

Пахомов Максим Анатольевич, *Институт кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого*
Павленко Евгений Юрьевич, *Институт кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого*
В работе представлен метод защиты от распределенного сканирования узлов из сети Интернет. Метод основан на гибридном механизме обнаружения сканирования и механизме составления черных списков подсетей. Также представлен способ обнаружения подмены IP-адреса сканирующего узла. Приводятся результаты экспериментальной оценки описанного метода, демонстрирующие корректность и точность его работы. Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых – кандидатов наук МК-3861.2022.1.6.

Иммунизация объектов информационной системы для обеспечения ее кибербезопасности

Павленко Евгений Юрьевич, *Институт кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого*
В работе предложен механизм иммунизации сложных технических систем, заключающейся в наделении системы встроенными и дополнительными механизмами безопасности, взаимодействующими и способными к запоминанию сценариев атак и проведению аналогий за счет методов искусственного интеллекта. Разработанный подход в динамике описывает зависимость между зараженными и вылеченными объектами. Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых – кандидатов наук МК-3861.2022.1.6.

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

(в программе возможны изменения)

10:00 – 11:30 **Секция «Российские криптографические средства защиты информации. Требования, разработка, внедрение и эксплуатация»** Зал «Шишка»

Практические вопросы разработки и эксплуатации российских криптографических средств. Жизненный цикл программных и программно-аппаратных средств. Диалог представителей регулятора с экспертным сообществом.

Ведущий:
- **Папаев Игорь Сергеевич,** ФСБ России
- **Хачатуров Артур Иванович,** АНСЕР ПРО

СКЗИ. Разработка, внедрение и оценка влияния

Светушкин Владимир Владимирович, *ФСБ России*

Криптографические проблемы, возникающие при выполнении требований ПКЗ-2005

Тыщенко Никита Сергеевич, *ФСБ России*

Обзор текущего законодательства в сфере применения СКЗИ

Толстолуцкая Анастасия Васильевна, *ФСБ России*

Некоторые вопросы использования СКЗИ с применением средств контейнеризации

Пузырев Владимир Александрович, *зам. начальника отдела анализа криптосредств, КриптоПро*
Крапивенцев Дмитрий Михайлович, *инженер-аналитик 1 категории, КриптоПро*

Блок вопросов и ответов, диалог представителей регулятора с участниками секции.

10:00 – 11:30 Секция «Технологии цепной записи данных и распределенных реестров»

Зал «Еловый»

Технологии цепной записи данных и распределенных реестров (блокчейн-технологии) к настоящему времени применяются во множестве различных информационных систем в качестве базовых технологий хранения и обработки данных. Пережив бурный рост в 2010-х гг., блокчейн-технологии перешли в стадию спокойного развития. В рамках секции эксперты расскажут как о практических применениях данных технологий, так и о ряде их структурных особенностей, которые необходимо принимать в расчет при адаптации блокчейн-технологий для конкретных применений.

Ведущие:

- **Чубаров Роман Юрьевич,** начальник отдела методологии применения электронной подписи и хранения электронных документов хозяйствующими субъектами Управления электронного документооборота ФНС России
- **Панасенко Сергей Петрович,** директор по научной работе Компании «Актив»

Блокчейн-технологии VS традиционные технологии хранения данных: сложность и критерии выбора

Панасенко Сергей Петрович, *компания «Актив»*

Доклад посвящен критериям выбора базовых технологий хранения данных в информационных системах различного назначения. В докладе дается обзор применений блокчейн-технологий, рассматриваются их основные достоинства и недостатки как в целом, так и для некоторых частных применений. Рассматриваются различные попытки формализации вопросов выбора базовой технологии на основе характеристик и требований вышележащих информационных систем. В заключение даются рекомендации по выбору блокчейн-технологии в качестве базовой с точки зрения технической применимости и целесообразности на основе критериев и таблиц выбора, а также опыта предшествующих применений.

Методика анализа данных публичных блокчейн-систем

Ищукова Евгения Александровна, Романенко Кирилл Сергеевич, Салманов Вячеслав Дмитриевич, *Южный федеральный университет, Институт компьютерных технологий и информационной безопасности*

В докладе рассматриваются подходы к анализу открытых данных блокчейн-систем, в том числе с использованием готового инструментария, с целью расследования инцидентов различного характера. К таким инцидентам можно отнести кражу криптовалюты, использование адресов блокчейн-сети в мошеннических целях, подозрительные переводы и многое другое. Приведены конкретные примеры расследования атак на примере блокчейн-платформы Bitcoin с детализацией поиска и аналитики анонимизированных данных о переводах.

Практика применения технологии блокчейн в государственных организациях и частных компаниях

Калихов Артём Владимирович, *компания «Веб3 Технологии»*

Обзорный доклад по практике применения блокчейн-технологий. В докладе рассматриваются основные типы используемых блокчейн-платформ и отрасли, в которых наиболее целесообразно применение блокчейн-технологий. Приводится обзор крупных блокчейн-проектов в государственном секторе РФ, а также примеры реализованных и пилотных проектов в частных компаниях.

Особенности шифрования данных в смарт-контрактах на блокчейне InnoChain

Красненкова Анастасия Владимировна, *РТУ МИРЭА*

Отличительной чертой блокчейна InnoChain является использование формальной верификации на всех уровнях его функционирования: разработка смарт-контрактов, развертывание смарт-контрактов, разработка и функционирование ноды – узла, на котором разворачиваются смарт-контракты и где выполняются транзакции. Несмотря на достаточно высокую надежность смарт-контрактов на данном блокчейне, актуальной остается проблема шифрования чувствительных данных, таких как пин-коды карт, балансы клиентов, значения клиентских скидок и т. п. В докладе рассказывается об основных особенностях шифрования чувствительных данных в смарт-контрактах на блокчейне InnoChain.

Прокси-решифрование с децентрализованными идентификаторами в распределённых системах

Чеканов Михаил Николаевич, *АО «ПроКСи»*

Внедрение децентрализованной идентификации на базе W3C DID позволяет обеспечить контроль обработки конфиденциальных данных со стороны их владельца без их раскрытия оператору информационной системы. При этом DID может применяться для идентификации как пользователей, так и других сущностей в сети с возможностью цифровой, криптографически защищённой верификации (W3C Verifiable Credentials, VC). Для организации контролируемого раскрытия конфиденциальных данных заранее неизвестным контрагентам может применяться схема прокси ре-шифрования (proxy re-encryption, PRE). Комбинация этих подходов позволяет создавать принципиально новые сервисы для распределённых децентрализованных систем.

10:00 – 11:30 Секция «Квантовые коммуникации и квантовая криптография», 1 часть

Зал «Сосновый»

Секция посвящена вопросам доказательства теоретической и практической криптостойкости, научным и практическим вопросам внедрения и развития квантовых технологий для повышения безопасности государства и граждан.

Ведущий: Уривский Алексей Викторович, заместитель генерального директора по науке и инновациям, АО «ИнфоТеКС»

Передатчик для городской сети КРК с пассивным приготовлением состояний. Экономичность и безопасность

Павлов Игорь Денисович, *технический директор QRate*

Возможное развитие систем КРК – разработка упрощенного экономичного передатчика с дальностью работы до 25-30 км. Это создаст гибкость в построении городских сетей КРК и позволит не использовать в протоколе состояния-ловушки без потери уровня секретности. Дальнейшим упрощение – переход в передатчике к пассивному приготовлению состояний – сложение двух когерентных лазерных импульсов со случайной фазой и ортогональной поляризаций. Это удешевляет передатчик, оптическая система становится пассивной. Устойчивость к атакам становится выше.

Создание спутниковой системы квантового распределения ключей: российский опыт

Плохов Дмитрий Викторович, *менеджер проектов «КуСпэйс Технологии»*

Толстых Валентин Александрович, *руководитель проекта «КуСпэйс Технологии»*

Спутниковые системы квантового распределения ключей (СКРК) расширяют границы использования существующих волоконных систем КРК, обеспечивают развёртывание квантово-защищенных каналов на глобальном масштабе. СКРК также актуальна для объектов, для которых подключение через оптоволоконные сети невозможно или нерационально. В докладе обобщен опыт разработки элементов СКРК: наземных приёмных станций, передатчика КРК на базе спутника (CubeSat). Рассмотрены перспективы создания национальной масштабируемой спутниковой сети для квантового распределения ключей.

Классификация подходов квантовой аутентификации

Жиляев Андрей Евгеньевич, *исследователь, Центр исследований и перспективных разработок АО «ИнфоТеКС»*

Лихтенберг Анкель Мари, *системный аналитик, Центр разработки программных продуктов АО «ИнфоТеКС»*

Беззатеев Сергей Валентинович, *д.т.н., доцент, профессор, Университет ИТМО*

Работа посвящена перспективному направлению защиты информации с применением квантовых технологий — квантовой аутентификации. Авторы уточняют свойства безопасности, которые достигаются применением квантовой аутентификации и приводят классификацию существующих теоретических подходов к такой аутентификации. Также приводится уточнение применимости различных подходов в практических сценариях.

Квантовое распределение ключей для обеспечения сквозной безопасности в подвижных сетях радиосвязи

Емельянов Виктор Михайлович, *ООО «Системы практической безопасности»*
Герасимова Алла Геннадьевна, *ООО «Системы практической безопасности»*
Шкоркина Елена Николаевна, *ООО «Системы практической безопасности»*
Новичков Серафим Алексеевич, *АНО ОВО «Сколковский институт науки и технологий»*

Технология квантового распределения ключей (КРК) может быть применена в задачах обеспечения сквозной безопасности информации, передаваемой в сетях подвижной радиосвязи. Рассмотрена архитектура сетей КРК, требования к узлам, распределяющим целевые ключи (ЦК), используемые для защиты абонентской информации. Представлены результаты исследования принципов формирования, распределения и доведения ЦК, а также вопросы применения протокола ProtoQa и ключевой схемы ISTOQ-M в этих задачах.

Оценка эффективности мер защиты от атаки лазерного повреждения на компоненты волоконно-оптических систем квантового распределения ключей

Бугай Кирилл Евгеньевич, *специалист, ООО «СФБ Лаборатория»*
Зызыкин Артём Павлович, *специалист ООО «СФБ Лаборатория»*
Булавкин Даниил Сергеевич, *специалист ООО «СФБ Лаборатория»*
Богданов Сергей Александрович, *специалист ООО «СФБ Лаборатория»*
Сущев Иван Сергеевич, *специалист ООО «СФБ Лаборатория»*
Дворецкий Дмитрий Алексеевич, *ведущий специалист ООО «СФБ Лаборатория»*

Системы квантового распределения ключей (КРК) являются открытыми для нарушителя в том смысле, что помимо атаки на квантовые состояния, нарушитель может проводить атаку на оборудование. Такой атакой является атака с лазерным повреждением оптических компонентов (LDA), может позволить нарушителю уменьшить ослабление оптических элементов и привести к компрометации распределяемых ключей. В данной работе предложен критерий оценки мер защиты от атаки с лазерным повреждением компонентов, а также исследована устойчивость к LDA постоянных и переменных волоконно-оптических аттенюаторов, широко используемых в волоконно-оптических системах КРК.

Исследование атаки ослепления однофотонных детекторов модулированным ярким светом

Булавкин Даниил Сергеевич, *специалист ООО «СФБ Лаборатория»*
Сущев Иван Сергеевич, *специалист ООО «СФБ Лаборатория»*
Бугай Кирилл Евгеньевич, *специалист ООО «СФБ Лаборатория»*
Богданов Сергей Александрович, *специалист ООО «СФБ Лаборатория»*
Дворецкий Дмитрий Алексеевич, *ведущий специалист ООО «СФБ Лаборатория»*

В данном докладе мы представляем исследование атаки ослепления однофотонных лавинных фотодиодов (SPAD) на основе структуры InGaAs, которые используются в системах квантового распределения ключей, модулированным лазерным излучением. Модуляция позволяет установить различные параметры ослепляющих импульсов. Мы исследовали зависимости тока смещения детектора от энергии ослепляющего импульса при различной длительности световых импульсов, различных частот их следования, а также при различной форме импульсов.

12:00 – 14:00 Экспертная панель «Электронный документооборот и электронная подпись»

Зал «Шишка»

Эксперты обсудят нормативные, организационные и технологические аспекты российского юридически значимого электронного документооборота; вопросы использования квалифицированной электронной подписи государством, гражданами и бизнесом; переход на использование машиночитаемых доверенностей; вопросы трансграничного использования юридически значимого электронного документооборота и доверенной третьей стороны; расширение сфер применения электронного документооборота, повышение эффективности бизнес-процессов за счет разумной и последовательной цифровизации. К участию приглашены представители федеральных органов исполнительной власти, крупнейших разработчиков и операторов систем электронного документооборота и разработчиков средств электронной подписи. Экспертная панель будет состоять из блока вводных докладов и обсуждения в формате круглого стола.

Ведущий: Малинин Юрий Витальевич, Президент Ассоциации РОСЭУ, директор Академии Информационных Систем

Эксперты:

- **Новиков Федор Вадимович,** начальник управления электронного документооборота, ФНС России
- **Кузнецов Роман Валерьевич,** директор Правового департамента Минцифры России
- **Нагдаев Артем Юрьевич,** заместитель Начальника Управления режима секретности и безопасности информации, Федеральное казначейство
- **Парфенов Сергей Александрович,** начальник проектного управления по реализации мероприятий по развитию электронного взаимодействия органов государственной власти Департамента развития облачных сервисов, Минцифры России
- **Веселов Михаил Юрьевич,** директор Фонда «Центр инноваций и информационных технологий», Федеральная нотариальная палата
- **Кирюшкин Сергей Анатольевич,** советник генерального директора ООО «Газинформсервис», эксперт Ассоциации РОСЭУ

Российский юридически значимый электронный документооборот

Малинин Юрий Витальевич, *Президент Ассоциации РОСЭУ, директор Академии Информационных Систем*

Сводный аналитический отчет о текущем состоянии рынка ЭДО и использовании квалифицированной электронной подписи.

Практическое применение реформ 63 ФЗ в Банке ВТБ

Дементьева Светлана Александровна, *начальник управления «Государственные услуги и сервисы для бизнеса» Департамент корпоративного цифрового бизнеса, вице-президент, Банк ВТБ*

Опыт крупнейшего российского банка по выдаче сертификатов квалифицированной электронной подписи в качестве Доверенного Лица УЦ ФНС России и по внедрению сервиса машиночитаемых доверенностей для клиентов и сотрудников банка.

12:00 – 14:00 Секция «Криптография и криптоанализ», 2 часть

Зал «Еловый»

Ведущие:

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

О свойствах MDS-матриц XSL-блочных шифрсистем

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

Многие атаки на XSL-блочные шифрсистемы основаны на различных свойствах матрицы преобразования линейного слоя. В докладе описаны классы матриц линейного слоя XSL-шифрсистем, обладающие свойствами, которые потенциально могут привести к атакам. Предложены рекомендации для защиты от таких атак.

Применение разностного метода криптографического анализа к алгоритму шифрования КБ-256

Курочкин Алексей Вячеславович, *ООО «Код Безопасности», МФТИ*
Чухно Андрей Борисович, *ООО «Код Безопасности», НИУ ВШЭ*

С конца XX века широкое распространение получили блочные криптографические алгоритмы. Большинство из них построено по итеративному принципу, где каждая итерация представляет собой чередование линейных и нелинейных преобразований. После появления линейного и разностного методов криптографического анализа были сформулированы требования к выбору параметров нелинейных и линейных преобразований. Алгоритм КБ-256 – это открытый блочный алгоритм шифрования с длиной блока 256 бит, построенный по принципу обобщённой сети Фейстеля, в котором восемь ячеек. В данном алгоритме нелинейные преобразования – это сумма по модулю 2^n и восемь 4-х битных подстановок, аналогичных подстановкам из алгоритма шифрования «Магма». На каждой итерации изменению подвергаются 3 ячейки. В данной работе получена оценка на минимальное количество раундов, при которых алгоритм не устойчив к разностному методу анализа: построено разностное соотношение для 15 раундов алгоритма, и с помощью данного соотношения построена эффективная атака на 13 раундов алгоритма.

Разработка алгоритма поиска невозможных дифференциалов для блочного шифра КБ256-3

Астраханцев Роман Геннадьевич, *НИУ ВШЭ*
Дмух Андрей Александрович, *к.ф.-м.н., доцент кафедры «Компьютерная безопасность», НИУ ВШЭ*
Астраханцева Ирина Александровна, *доктор экономических наук, зав. каф. информационных технологий и цифровой экономики ФГБОУ ВО «Ивановский государственный химико-технологический университет»*

В работе для блочного шифра КБ256-3 (16 раундов, используются раундовые преобразования из ГОСТ Р 34.12-2015 «Магма») найдены невозможные дифференциалы длины от 8 до 18 раундов, что на 2 раунда больше, чем известные ранее. Полученные результаты свидетельствуют о необходимости увеличения количества раундов для КБ256-3 не менее чем на 6-10 раундов.

Подход к оценке стойкости блочных шифров к линейному криптоанализу с использованием квантовых алгоритмов

Щербаченко Андрей Александрович, *ООО «СФБ-Лаб»*

В докладе рассматриваются вопросы применения квантового алгоритма Бернштейна-Вазирани для оценки характеристик, определяющих стойкость алгоритмов блочного шифрования к линейному методу криптоанализа. Предложены подходы к оценке преобладания наилучшего линейного приближения при фиксированном значении ключа, а также математического ожидания преобладания при случайном выборе ключа.

О свойстве безопасности RUP для схем аутентифицированного шифрования

Бабуева Александра Алексеевна, *ведущий инженер-аналитик, КриптоПро*
Алексеев Евгений Константинович, *к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро*
Ахметзянова Лилия Руслановна, *к.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро*
Божко Андрей Алексеевич, *инженер-аналитик, КриптоПро*

Доклад посвящен свойству безопасности RUP (Release of Unverified Plaintext), которое характеризует стойкость схемы аутентифицированного шифрования относительно нарушителей, обладающих возможностью узнавать открытый текст, соответствующий некорректному шифртексту. Приводятся результаты исследований о соотношении данного свойства со свойством безопасности MRAE (Misuse-Resistance Authenticated Encryption), предлагается атака на механизм шифрования, использующийся в сообщении формата CMS, определенного в Рекомендациях по стандартизации Р 1323565.1.025-2019.

Характеристики режима работы блочных шифров, предлагаемого для защиты системных носителей информации с блочно-ориентированной структурой

Коренева Алиса Михайловна, *к.ф.-м.н., ООО «Код Безопасности», Финансовый университет при Правительстве РФ*

Фирсов Георгий Валентинович, *ООО «Код Безопасности», Национальный исследовательский ядерный университет «МИФИ»*

В 2022 году приняты рекомендации по стандартизации, определяющие режим работы блочных шифров DEC, используемый для защиты носителей информации с блочно-ориентированной структурой. Режим DEC имеет эксплуатационные особенности, усложняющие его использование для шифрования системных дисков, из-за чего востребован синтез альтернативных режимов для полнодискового шифрования. В большинстве существующего ПО для шифрования системных дисков используется режим XTS, но он имеет особенности, ухудшающие его криптографические качества. В докладе предлагается модификация режима XTS — режим XEH (Xor-Encrypt-Hash), для которого получена нижняя граница оценки уровня информационной безопасности и исследованы некоторые эксплуатационные характеристики.

12:00 – 14:00 Секция «Квантовые коммуникации и квантовая криптография», 2 часть

Зал «Сосновый»

Квантовое распределение ключей на практике

Смирнов Николай Валерьевич, *директор по продуктам АО «ИнфоТеКС»*

В докладе будет представлен опыт разработки комплексных решений, основанных на системах квантового распределения ключей. Будет представлен обзор разработанных продуктов и законченных решений квантового распределения ключей АО «ИнфоТеКС», результаты сертификации и опыт внедрения у заказчиков.

Динамика наблюдаемых в системах квантового распределения ключей с непрерывными переменными

Козубов Антон Владимирович, *начальник отдела перспективных исследований и разработок «СМАРТС-Квантателеком»*

Гайдаш Андрей Алексеевич, *ведущий научный сотрудник «СМАРТС-Квантателеком»*

В работе оценивается динамика наблюдаемых в квантовом канале для систем квантового распределения ключей с непрерывными переменными в терминах P-функции Глаубера-Сударшана. Получено вероятностное распределение разницы фотоотсчетов, среднее значение и дисперсия которого в явном виде зависят от параметров канала. Исследовано влияние анизотропии оптического волокна, а также поляризационных искажений и термализации на статистику фотоотсчетов и, как следствие, на производительность систем квантового распределения ключей с непрерывными переменными.

Система квантового распределения ключа на непрерывных переменных с гауссовской модуляцией

Самсонов Эдуард Олегович, *ведущий научный сотрудник «СМАРТС-Квантателеком»*

Гончаров Роман Константинович, *Университет ИТМО*

Квантовое распределение ключа (КРК) позволяет двум (и более) легитимным пользователям обмениваться криптографическими ключами. Для всех протоколов КРК различают протоколы на дискретных переменных (ДП) и на непрерывных переменных (НП). Последние реализуются с помощью балансных детекторов. Это означает, что за счет стандартизации оптического оборудования КРКНП может быть успешнее интегрирована в телекоммуникационную инфраструктуру. В рамках работы был создан первый в РФ комплекс КРКНП с обоснованной стойкостью против коллективных атак.

Совместное распространение квантового канала системы квантового распределения ключа и информационных каналов оптической транспортной сети

Киселёв Фёдор Дмитриевич, *старший научный сотрудник «СМАРТС-Квантателеком»*

Объединение квантового канала системы квантового распределения ключа и информационных каналов оптической транспортной сети является важным этапом развития технологии квантовых коммуникаций, так как позволяет решить экономическую проблему необходимости выделения темного волокна. В данной работе было исследовано влияние различных оптических шумов на работу систем и протоколов КРК, рассмотрены основные методы их компенсации, а также представлены наиболее эффективные схемы мультиплексирования квантового и информационных каналов.

15:00 – 16:30 Секция «Криптография в энергетической отрасли»

Зал «Сосновый»

Вопросы внедрения и эксплуатации криптосредств в энергетической сфере. Криптография в приборах учета электроэнергии. Адаптация и развитие текущих решений российских разработчиков под нужды энергетической отрасли. Стандарты, требования, ближайшие планы и перспективы. Секция состоит из блока докладов и обсуждения в формате круглого стола.

Ведущий: Щербаков Антон Владимирович, ФСБ России

Эксперты круглого стола:

- **Коротенко Александр Васильевич,** Минэнерго России
- **Иванов Михаил Николаевич,** генеральный директор, ООО «С-Терра СиЭсПи»
- **Сорокина Марина Викторовна,** руководитель направления, АО «ИнфоТеКС»
- **Васильев Дмитрий Николаевич,** директор департамента Информационной безопасности ПАО «Интер РАО»
- **Зарецкий Дмитрий Викторович,** генеральный директор НТЦ «Нартис»
- **Простов Владимир Михайлович,** советник, компания КриптоПро

Интеллектуальный учет

Рябко Сергей Дмитриевич, *президент, ООО «С-Терра СиЭсПи»*

Проблемы и решения по криптографической защите ПУ, УСПД и программного комплекса ИВК.

СКЗИ для Интеллектуальных систем учета электроэнергии. Реальный практический опыт

Сорокина Марина Викторовна, *руководитель направления, АО «ИнфоТеКС»*

В ходе презентации автор рассмотрит вопросы защиты информации интеллектуальных систем учета электроэнергии, расскажет о вызовах, с которыми сталкиваются разработчики СКЗИ и производители компонентов ИСУЭ при попытке обеспечить целостность и/или конфиденциальность передаваемой информации. На примере комплекса ViPNet SIES, покажет, как решаются такие задачи и почему стоит выбирать программно-аппаратные СКЗИ. В докладе будет представлен реальный практический опыт по встраиванию криптографических средств в УСПД и приборы учета разных вендоров, а также подсвечены открытые вопросы, которые необходимо решить на нормативно-организационном уровне.

Проблематика применения СКЗИ в ИСУ

Васильев Дмитрий Николаевич, *директор департамента Информационной безопасности ПАО «Интер РАО»*

В докладе будет отражены основные проблемы связанные с использованием СКЗИ в ИСУ и возможные пути их решения

Особенности интеграции СКЗИ в оборудование ИСУ

Зарецкий Дмитрий Викторович, *генеральный директор НТЦ «Нартис»*

В докладе будут отражены аспекты встраивания СКЗИ в УСПД/шлюзы ИСУЭ и интеллектуальные приборы учета со стороны производителя оборудования ИСУЭ. Докладчик поделится практическим опытом на основе проведенных работ по интеграции оборудования с СКЗИ различных производителей. Будет рассказано о проведенных работах в части конструктивных изменений оборудования, организационных изменениях, лицензировании и процесс сертификации и испытаний.

15:00 – 16:30 Секция «Криптография и криптоанализ», 3 часть

Зал «Еловый»

Ведущие:

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

Анализ подходов к построению протоколов RFID для защиты от атак пересылки

Чичаева Анастасия Александровна, *специалист-исследователь лаборатории криптографии АО «НПК «Криптонит»*

Бельский Владимир Сергеевич, *заместитель руководителя лаборатории криптографии АО «НПК «Криптонит»*

Царегородцев Кирилл Денисович, *старший специалист-исследователь лаборатории криптографии АО «НПК «Криптонит»*

Шишкин Василий Алексеевич, *руководитель лаборатории криптографии АО «НПК «Криптонит»*

В работе предложен протокол оценки расстояния DB-RFID, предназначенный для защиты от атак пересылки в технологии RFID. Протокол DB-RFID развивает идеи протокола «Швейцарский нож», который в соответствии с анализом является наиболее перспективным, так как защищает от большего числа атак. Также в работе рассматриваются варианты протокола с использованием отечественных криптографических механизмов.

Аутентификация устройств низкоресурсных киберфизических систем в граничной вычислительной архитектуре

Шкоркина Елена Николаевна, *Санкт-Петербургский политехнический университет Петра Великого*

Александрова Елена Борисовна, *Санкт-Петербургский политехнический университет Петра Великого*

Доклад посвящен разработанному протоколу аутентификации управляющего устройства на исполнительном с выработкой ключей защищенного управления, функционирующему в вычислительной архитектуре с граничным делегированием. Будут рассмотрены аспекты решения, благодаря которым обеспечивается стойкость к некоторым видам атак, а также возможность адаптации протокола к вычислительным возможностям устройств и противника.

Исследование эффективности применения нейросетевых алгоритмов для оценки минимальной энтропии последовательностей, вырабатываемых датчиками случайных чисел

Сергеев Андрей Михайлович, *ООО «СФБ Лаб»*

В докладе исследуются вопросы определения статистических свойств исходных последовательностей, вырабатываемых физической компонентой ФДСЧ (физического датчика случайных чисел), к которым не применимы известные статистические тесты NIST 800-22, Diehard и т.п. В 2018 году для оценки случайности исходных последовательностей предложен набор тестов NIST 800-90B, направленный на оценку минимальной символьной энтропии и включающий в себя тесты-предикторы, предсказывающие появление символов (бит, байт) последовательности. В настоящем докладе исследуется эффективность применения нейросетевых алгоритмов для построения предикторов в качестве тестов оценки мин-энтропии.

Обобщенный параметризованный алгоритм восстановления прообраза хеш-функции MD5 методом полного опробования

Коновалов Никита, *аспирант, НИЯУ МИФИ*

Работа посвящена продолжению исследований криптографических хеш-функций семейства MD и особенностей конструкций, позволяющих редуцировать функции для задачи восстановления прообраза по известному образу при некоторых известных характеристиках прообраза методом полного опробования. Был предложен обобщенный редуцированный параметризированный алгоритм для хеш-функции MD5, сокращающий количество алгоритмических и логических операций в задаче восстановления прообраза по известному образу методом полного опробования. Обобщенный алгоритм позволяет сократить количество шагов обновления состояния во внутреннем цикле алгоритма на 36% в лучшем случае.

Разработка способов поиска эквивалентных ключей в поточных шифрсистемах, основанных на алгоритме генерации случайных подстановок Фишера-Йетса

Киндеев Юрий Романович, *студент, НИЯУ МИФИ*

В работе проводится сравнительный анализ алгоритмов генерации начальной подстановки в поточной шифрсистеме RC4 и её модификациях RC4A, VMPC и RC4D, основанных на конструкции предложенной и описанной Р. А. Фишером и Ф. Ятсом, а также были рассмотрены методы получения пар эквивалентных ключей малой длины. В результате работы была найдена закономерность при формировании эквивалентных ключей, на ее основе был разработан алгоритм генерации пар эквивалентных ключей и опробован на поточной шифрсистеме RC4 и её модификациях RC4A, VMPC и RC4D.

15:00 – 16:30 Секция «Перспективные исследования в области кибербезопасности», 1 часть

Кино-концертный зал

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

Ключевые области внимания на стыке искусственного интеллекта и кибербезопасности

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

Искусственный интеллект (ИИ) стал жизнеспособным подходом к обработке огромных объемов разнородных данных и выполнению фундаментальных задач кибербезопасности, таких как обнаружение вторжений, управление уязвимостями и оценка безопасности, мониторинг безопасности, приоритизация активов, распределенный контроль доступа. В докладе представляется современное состояние использования ИИ в кибербезопасности (как со стороны защиты, так и атак). Анализируются следующие ключевые области внимания на стыке ИИ и кибербезопасности: повышение кибербезопасности с помощью ИИ, использование ИИ для кибератак, уязвимости систем ИИ к атакам, а также использование ИИ в вредоносных информационных операциях (фейки с использованием ИИ).

Анализ безопасности проекта национального стандарта «Нейросетевые алгоритмы в защищённом исполнении. Автоматическое обучение нейросетевых моделей на малых выборках в задачах классификации»

Маршалко Григорий Борисович, *ТК 26*

Романенков Роман Александрович, *ТК 26*

Труфанова Юлия Анатольевна, *ТК 26*

Исследуемый стандарт будет распространяться на системы и модели искусственного интеллекта, позволяющие решать задачи классификации образов, функционирующие на объектах критической информационной инфраструктуры и нуждающихся в обеспечении более высокого уровня защищенности. В докладе показывается, что параметры обученной в соответствии с проектом стандарта нейронной сети допускают утечку информации об обучающих примерах. В частности, предложен статистический критерий, позволяющий реализовать один из вариантов атак, направленных на извлечение знаний систем искусственного интеллекта — атаку проверки принадлежности обучающему множеству. Это, например, позволяет выделять биометрический образ, использовавшийся для обучения классификатора из некоторого набора образов.

Применение федеративного обучения для построения систем обнаружения вторжений

Новикова Евгения Сергеевна, *к.т.н., доцент, СПбГЭТУ «ЛЭТИ»*

Федорченко Елена Владимировна, *к.т.н., СПб ФИЦ РАН*

Применение федеративного обучения позволяет разрабатывать распределенные интеллектуальные системы, в которых обработка и анализ данных осуществляется на источниках генерации данных, что позволяет, с одной стороны, снизить требования к пропускной способности коммуникационной сети, а, с другой стороны, повысить уровень защищенности анализируемых данных. В докладе представлены результаты систематического исследования существующих решений по обнаружению вторжений и аномалий на основе федеративного обучения, формулируются преимущества его применения, а также указываются открытые проблемы, связанные с его применением на практике.

Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе фрактального анализа и машинного обучения

Крибель Александр Михайлович, *Военная академия связи им. С.М.Буденного*
Крибель Ксения Васильевна, *Военная академия связи им. С.М.Буденного*
Котенко Игорь Витальевич, *профессор, д.т.н., СПб ФИЦ РАН*

Рассматривается подход к выявлению аномалий и компьютерных атак в современных сетях передачи данных, который основывается на интеграции методов фрактального анализа и машинного обучения. Подход ориентирован на выполнение в реальном или близком к реальному масштабе времени, он включает несколько этапов, в том числе этап выявления аномалий в сетевом трафике, реализуемого с помощью методов фрактального анализа (оценки самоподобия сетевого трафика), этап идентификации в аномалиях компьютерных атак и этап их классификации, реализуемых с применением методов машинного обучения, использующих ячейки рекуррентных нейронных сетей с долгой краткосрочной памятью.

Интерпретируемые модели глубокого обучения для обнаружения аномалий в системах АСУТП

Чернышов Юрий Юрьевич, *к.ф.-м.н., руководитель исследовательского центра ИРИТ-РТФ УрФУ*

В докладе делается обзор перспективных методов обнаружения аномалий в сложных системах и предлагаются новые модели с использованием автокодировщиков и ограниченных машин Больцмана (Restricted Boltzmann Machine, RBM). Различные подходы опробованы на датасете SWAT (киберфизический макет водоочистного завода), проведено сравнение полученных метрик с результатами других исследовательских команд.

Уязвимости архитектуры Старлинк

Филимонов Дмитрий Викторович, *выпускник аспирантуры, Самарский университет*
Сагатов Евгений Собирович, *к.т.н., доцент, Самарский университет*
Сухов Андрей Михайлович, *д.т.н., в.н.с., Севастопольский государственный университет*
Ажмяков Вадим Викторович, *Dr. rer. nat. habil., профессор, Севастопольский государственный университет*

В докладе анализируется работа глобальной спутниковой системы Starlink, разворачиваемой компанией SpaceX. Рассматриваются недостатки архитектуры этой системы, используя которые можно было бы нарушить ее работу. Архитектура состоит из трех основных элементов: группировки спутников на низких орбитах, сети наземных станций, пользовательских терминалов. Спутниковая составляющая является наиболее устойчивой частью глобальной спутниковой системы Starlink. Поверхностный анализ угроз для Starlink показал, что наиболее уязвимая часть системы – это наземные, а не спутниковые компоненты системы. Это пользовательские терминалы и наземные станции, которые обеспечивают связь в ограниченном районе. Однако, площадь района без связи будет сильно различаться от того, какой элемент наземной инфраструктуры разрушен. В любом случае при выводе из строя такого элемента в соответствующем районе будут наблюдаться перебои со связью.

17:00 – 19:00 Круглый стол «Подготовка и трудоустройство специалистов в области ИБ»

Зал «Еловый»

Круглый стол, посвященный вопросам обучения и повышения квалификации в области информационной безопасности и взаимодействию с работодателями в формировании учебных программ.

Ведущий: 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

Эксперты:

- **Зегжда Дмитрий Петрович,** директор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого, член-корреспондент РАН
- **Лось Владимир Павлович,** директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности, Президент – Председатель правления МОО «Ассоциации Защиты Информации»

- **Гусев Дмитрий Михайлович,** заместитель Генерального директора АО «ИнфоТеКС»
- **Хорев Анатолий Анатольевич,** заведующий кафедрой информационной безопасности МИЭТ (по согласованию)
- **Хайров Игорь Евгеньевич,** заместитель директора Академии Информационных Систем

17:00 – 19:00 Секция «Перспективные исследования в области кибербезопасности», 2 часть

Кино-концертный зал

Механизмы создания системы доверия к социально значимым общественным информационным системам

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., доцент, заместитель заведующего кафедрой БИТ НИУ «МЭИ»*

В докладе модель доверия населения к социально значимым общественным (СЗО) ИТ-проектам рассматривается как многокомпонентная функция, конечные значения которой существенно зависят от концепции ИТ-проекта, способов и технологий его реализации, архитектуры системы безопасности и медийной части реализации этого проекта. Предлагаются механизмы построения моделей угроз вмешательства в СЗО на основе концепции ZTA («нулевого» доверия). На отдельных примерах представлены механизмы создания доверия к этим системам путем полного контроля всех процессов, в которых возможно постороннее вмешательство, обеспечение контроля всех подключений к их подсистемам и разработки системы доказательства доверия к СЗО.

Ленивая классификация сообщений злоумышленников на основе узорных структур (Lazy Classification of Underground Forums Messages Using Pattern Structures)

Газаль Абдулрахим, *аспирант Факультета компьютерных наук НИУ ВШЭ*
Кузнецов Сергей Олегович, *д.ф.-м.н., профессор ФКН НИУ ВШЭ*

На подпольных форумах хакеры сообщают о готовящихся атаках и средствах реализации атак на проекты, предприятия и организации. В докладе рассматриваются результаты экспериментов по оценке рисков, связанных с такими сообщениями, полученных на основе узорных структур, ленивой классификации (классификации по запросу), а также некоторых средств сокращения перебора и методов анализа естественного языка.

Перспективные направления применения аналитического моделирования атак для оценки защищенности компьютерных сетей

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

В настоящее время новые атаки появляются настолько часто, что крайне важной становится проактивная защита от них. Аналитическое моделирование — это подход, позволяющий строить модели защищаемой сети и на основе этой модели рассчитывать различные метрики характеризующие защищенность. В докладе рассматриваются подходы к применению моделирования атак для учета возможных уязвимостей нулевого дня, выявления слабых мест в защите сети, оценки возможного ущерба от появления инсайдеров и пр.

Анализ исходных кодов эксплойтов и признаков их выполнения для формирования объективных оценок защищенности информационных систем

Федорченко Елена Владимировна, *к.т.н., СПб ФИЦ РАН*
Новикова Евгения Сергеевна, *к.т.н., доцент, СПбГЭТУ «ЛЭТИ»*

Существующие показатели, применяемые для оценивания защищенности информационных систем, зачастую носят субъективный характер. Работа посвящена разработке объективных и обоснованных показателей, характеризующих вероятность реализации атаки, на основе модели выполнения исходных кодов эксплойтов и признаков их выполнения. Это необходимо для прогнозирования атакующих воздействий, а также автоматизации и обеспечения объяснимости применяемых решений по повышению защищенности. В докладе представлены результаты анализа возможных представлений выполнения исходных кодов эксплойтов, их признаков и возможных показателей, а также концепция оценивания защищенности информационных систем на их основе.

Генерация семантически корректного JavaScript-кода для фаззинг-тестирования движков браузеров

Козачок Александр Васильевич, *д.т.н., доцент, сотрудник Академии ФСО России*
Ерохина Наталья Сергеевна, *сотрудник Академии ФСО России*

Фаззинг-тестирование – это практичный, широко применяемый метод поиска ошибок в сложных реальных программах, например, таких как JavaScript-движки. Однако, существующие подходы к их фаззингу, не обеспечивают получения высококачественных корпусов начальных данных. Существующие фаззеры, как правило, не отслеживают семантику языка при генерации сложно структурированных данных. Для преодоления указанных недостатков и повышения покрытия кода предлагается моделировать семантически корректные кодовые конструкции на основе методов машинного обучения с учетом прироста покрытия кода в процессе работы фаззера.

О возможности проведения Makeup-атаки на биометрию по венозному рисунку

Мизинов Павел Владимирович, *аспирант кафедры «Информационная безопасность»,*
МГТУ им. Н. Э. Баумана.
Коннова Наталья Сергеевна, *к.т.н., доцент кафедры «Информационная безопасность»,*
МГТУ им. Н. Э. Баумана.

Биометрия по сосудистому рисунку является одной из самых популярных в настоящее время. В работе впервые представлен новый инструмент атаки на данные системы, изготовленный непосредственно на руке атакующего с применением отражающих/поглащающих веществ в ближнем инфракрасном излучении. Использование данной технологии изготовления инструмента атаки делает возможным реализацию нового типа атаки на биометрические системы рассматриваемого типа.

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 500 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 ФЗ-187, КИИ, Указ 250, Указ 166, ПДн, расследование компьютерных преступлений, аудит безопасности, управление рисками и др.;
- Программы повышения квалификации и профессиональной переподготовки, согласованные с ФСТЭК России, ФСБ России, ФУМО ВО ИБ, профильными ассоциациями по ИБ;
- 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, отечественными 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

Вечерняя программа

ИММЕРСИВНЫЙ СПЕКТАКЛЬ

21 МАРТА

НАЧАЛО В 20:00

КИНО-КОНЦЕРТНЫЙ ЗАЛ

Ждем вас на иммерсивном спектакле с полным погружением в сюжет.

Детективная ролевая игра, в которой вам нужно совместными усилиями вычислить грабителя.

ИГРА
В ИМИТАЦИЮ

21 МАРТА, 20:00

ЗАЛ «ЕЛОВЫЙ», 1 ЭТАЖ

ИНТЕЛЛЕКТУАЛЬНЫЙ КРИПТОГРАФИЧЕСКИЙ КВИЗ “ИГРА В ИМИТАЦИЮ”

С АЛЕКСЕЕМ ЛУКАЦКИМ

Практика на Досках с Гвоздями

22, 23, 24 МАРТА | 08:00-09:00
Зал “Стеклянный”

Быстро и качественно зарядиться энергией и позитивом перед деловой программой конференции поможет Практика на Досках с Гвоздями (Досках Садху)!

Музей Криптографии

конференция РусКрипто

Мастер-класс

Послание с секретом

Исследуем древние шифры

возраст:
7+

время:
22 марта 2023
12:00-13:00

место:
Детский развлекательный комплекс

Музей криптографии

конференция РусКрипто

Мастер-класс

Шифр в кармане

Как шифровали в XX веке

возраст:
12+

время:
22 марта 2023
12:00-13:00

место:
Детский развлекательный комплекс

Приглашаем на

Гала-ужин юбилейной конференции РусКрипто'2023

22 МАРТА • НАЧАЛО В 20:00 • ЗАЛ "ШИШКА", 2 ЭТАЖ

Стиль вечера - Black Tie

ВЫ МОЖЕТЕ ВЫИГРАТЬ! НЕТ НИЧЕГО ПРОЩЕ!

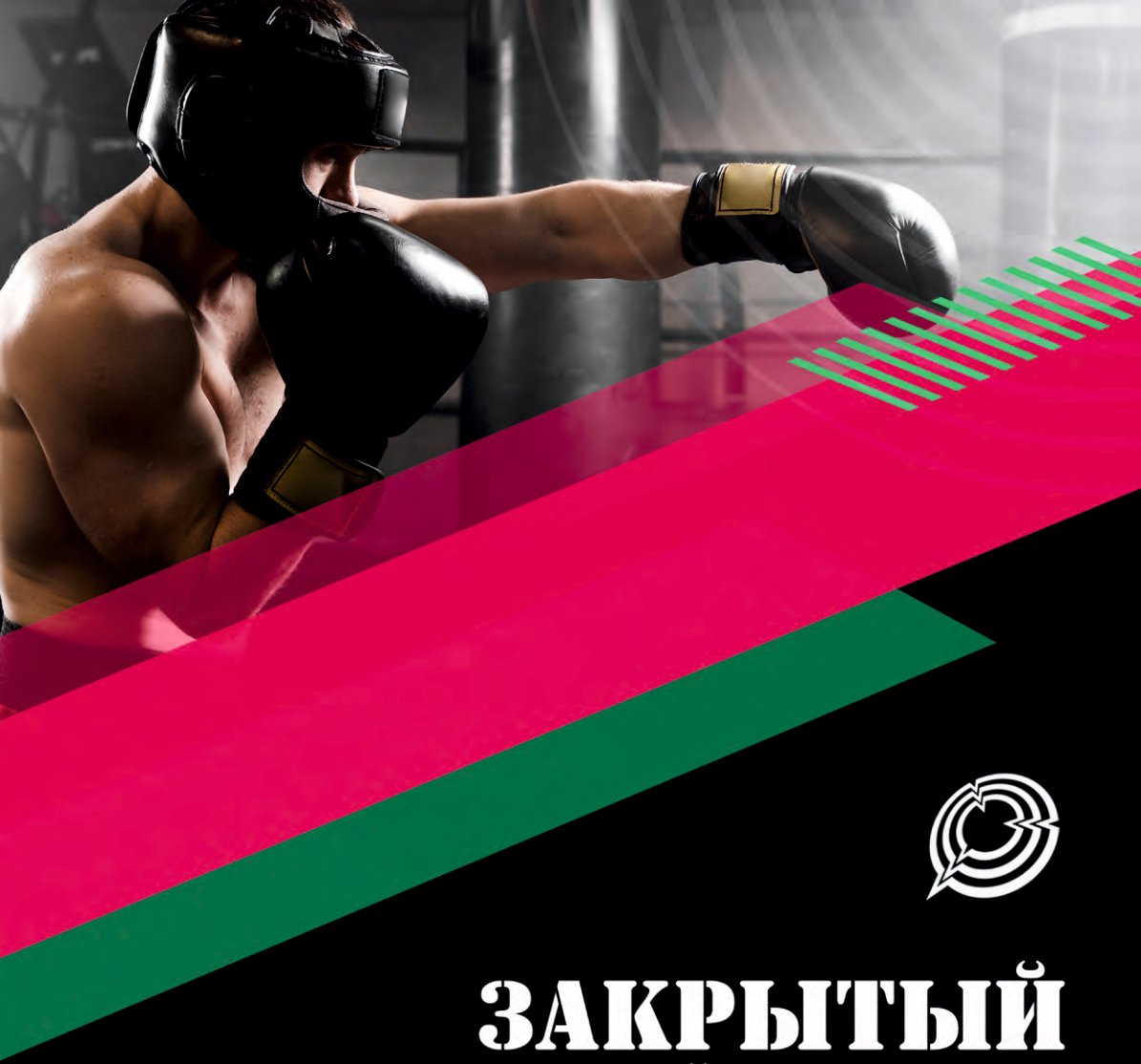
РОЗЫГРЫШ ПРИЗОВ СРЕДИ УЧАСТНИКОВ «РУСКРИПТО 2023» БУДЕТ ПРОВОДИТЬСЯ ВО ВРЕМЯ ГАЛА-УЖИНА

ГЛАВНЫЕ ПРИЗЫ

1 МЕСТО - УМНАЯ КОЛОНКА ЯНДЕКС СТАНЦИЯ МАКС

2 МЕСТО - УМНАЯ КОЛОНКА ЯНДЕКС СТАНЦИЯ ЛАЙТ

СКАЧИВАЙТЕ ПРИЛОЖЕНИЕ, БУДЬТЕ АКТИВНЫМ УЧАСТНИКОМ РУСКРИПТО 2023



ЗАКРЫТЫЙ БОКСЕРСКИЙ КЛУБ

23 МАРТА, НАЧАЛО В 20:00

ЗАЛ "ШИШКА", 2 ЭТАЖ

Вечер посвящен самому зрелищному виду спорта- боксу.
Опытные бойцы проведут три поединка по три раунда каждый.

КАЛЕНДАРЬ МЕРОПРИЯТИЙ АИС 2023

06 - 09 июня | Подмосковье

ФОРУМ ЭДО’2023. ЛЕТО

IV Всероссийский форум по электронному документообороту

22 - 23 июня | Санкт-Петербург

КРЭБ. БЕЛЫЕ НОЧИ

Образовательный интенсив «Практические аспекты корпоративной безопасности»

05 – 08 сентября | Сочи

ИНФОБЕРЕГ

XXII Всероссийский форум «Информационная безопасность. Регулирование. Технологии. Практика»

05 октября | Москва

МЕДИНФОБЕЗ

Всероссийская конференция «Информационная безопасность в сфере здравоохранения»

01 ноября | Москва

ФОРУМ ЭДО’2023. МОСКВА

V Всероссийский форум по электронному документообороту

04 - 05 декабря | Москва

КРЭБ'2023

Практическая конференция «Конкурентная разведка. OSINT & Экономическая безопасность»

06 декабря | Москва

АНТИФРОД РОССИЯ’2023

XIV Национальный форум «Борьба с мошенничеством в сфере высоких технологий»

Январь 2024 | Москва

ФОРУМ КВАНТ 2024

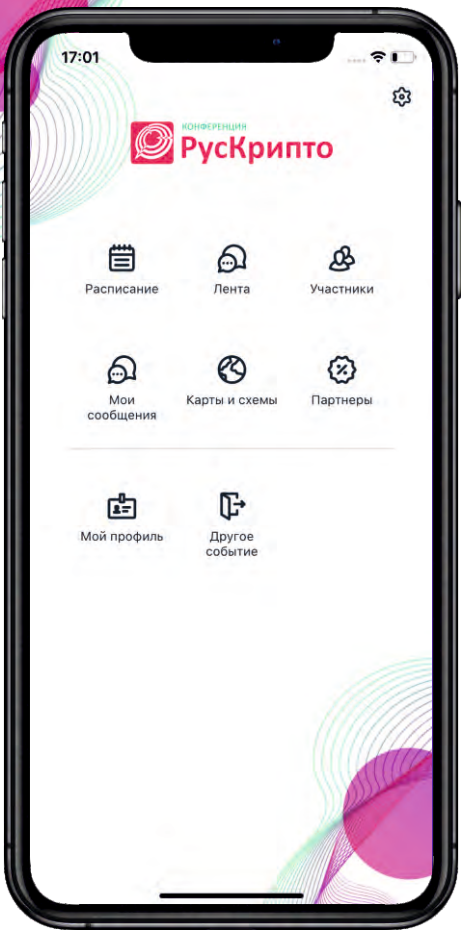
Всероссийский форум «Доверенные квантовые технологии и коммуникации»

+7 (495) 120-04-02 conf@infosystem.ru www.vipforum.ru

ДЛЯ ЗАМЕТОК

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 -

РУСКРИПТО2023

и далее, следуя инструкции, авторизируйтесь 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 Ивентницы

+7 (495) 120-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru