ОРГАНИЗАТОРЫ

Ассоциация РусКрипто

АИС

ВИПФОРУМ
Организация деловых событий

26-Я НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РусКрипто’2024

ПРОГРАММА

19 - 22 МАРТА | СОЛНЕЧНЫЙ PARK HOTEL & SPA

БЛАГОДАРИМ СПОНСОРОВ И ПАРТНЕРОВ ЗА ОКАЗАННУЮ ПОДДЕРЖКУ!

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

КРИПТОПРО
ключевое слово в защите информации

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

infotecs

ГЛАВНЫЙ ТЕХНОЛОГИЧЕСКИЙ ПАРТНЕР

ГАЗПРОМБАНК
Банк ГПБ (АО)

СТРАТЕГИЧЕСКИЙ ДЕЛОВОЙ ПАРТНЕР

КОМПАНИЯ АКТИВ

СТРАТЕГИЧЕСКИЙ НАУЧНЫЙ ПАРТНЕР

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

ОФИЦИАЛЬНЫЙ ПАРТНЕР

СПБ

ОФИЦИАЛЬНЫЙ ПАРТНЕР

КОД безопасности

ПАРТНЕР СЕССИИ

positive technologies

СМАРТС КВАНТТЕЛЕКОМ

АССОЦИАЦИЯ РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ

GREEN LIGHT TECHNOLOGY

ПАРТНЕРЫ ВЫСТАВКИ

SPACE-BIT

с•терра

альфа

НИИМЭ

ЛАН АТМ сервис
ГРУППА КОМПАНИЙ ЛАНИТ

НАУЧНЫЙ ПАРТНЕР

КРИПТОНИТ

ПАРТНЕРЫ КОНФЕРЕНЦИИ

QApp

QRATE
QUANTUM SOLUTIONS

АПКИТ

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

CISOCLUB

CYBER MEDIA

ВСЕ МЕРОПРИЯТИЯ ИТ НА ICTGO

ICTONLINE
ИНФОКОММУНИКАЦИИ ОНЛАЙН

NBJ

Единый портал Электронной подписи

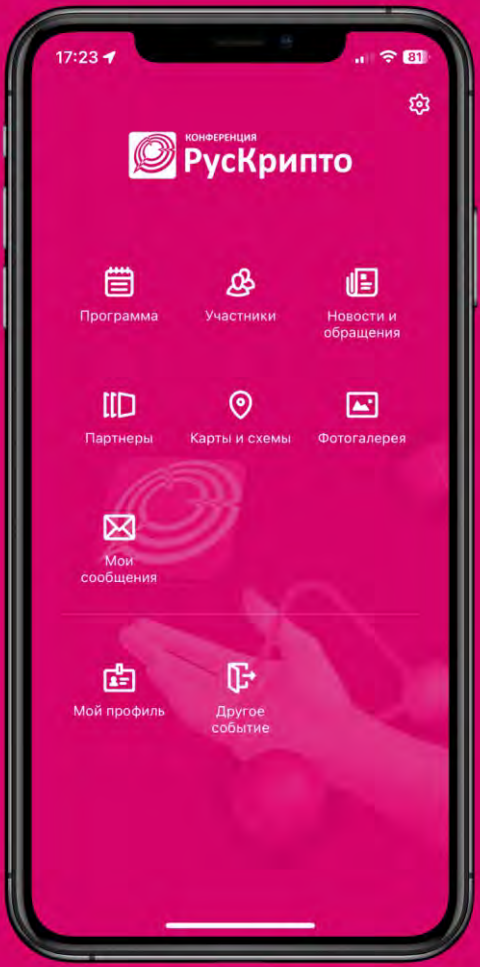
BIS JOURNAL

УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ ГАРАНТ
ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

CIS
Современные Информационные Системы

BANKIROS

Основание
Удостоверяющий центр



Event.Rocks

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

В приложении введите
ID события —

РусКрипто

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

Скачать из Google Play

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»

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

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

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

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

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

22 марта в 12:00 трансфер отель «Солнечный Park Hotel & SPA» - **м. ХОВРИНО**
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 - 19 марта с 16:00
Выезд - 22 марта до 12:00

20 и 21 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.

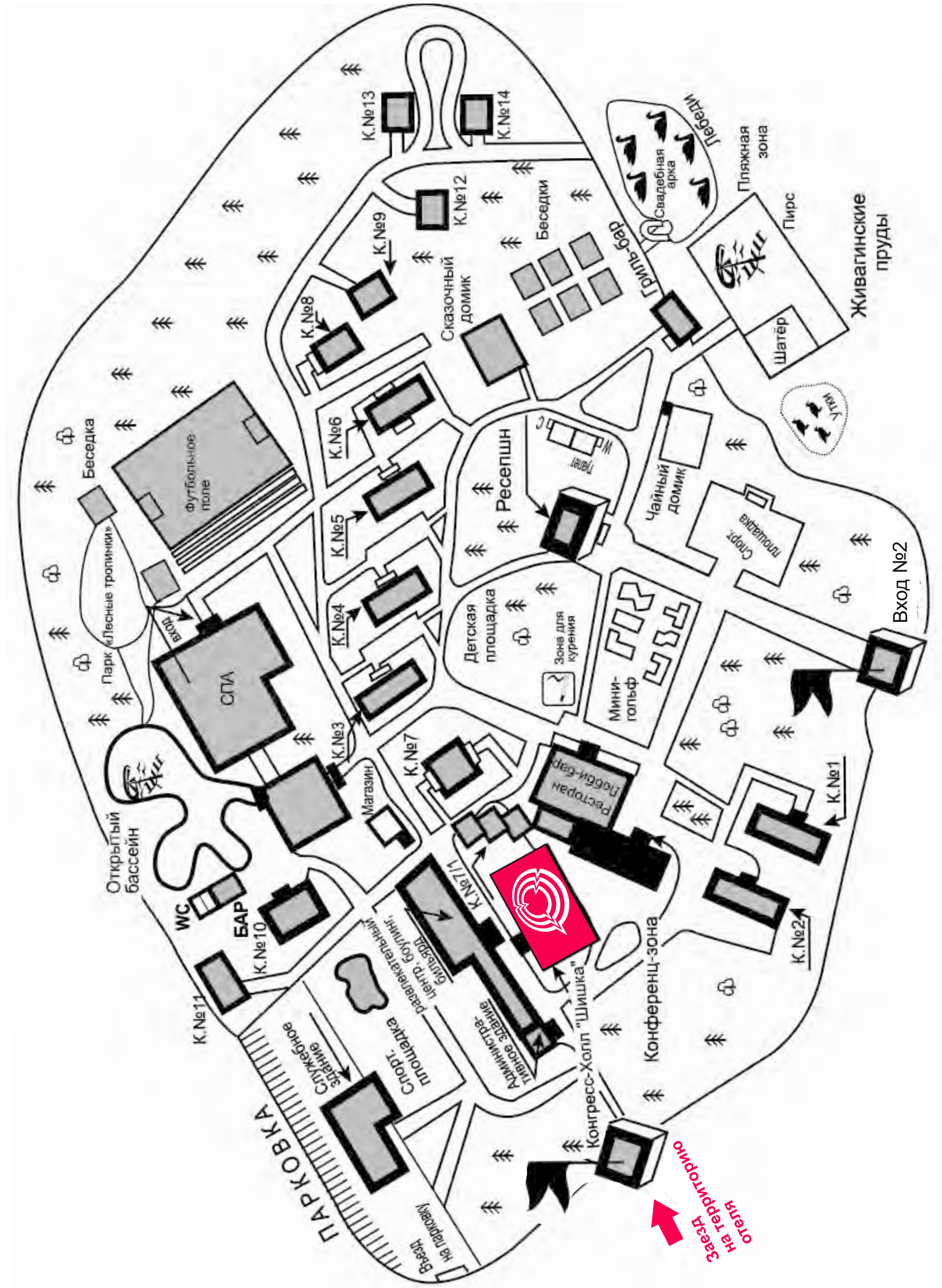
- Официальный хэштег конференции **#РусКрипто**
  Мы будем рады, если вы будете упоминать наше мероприятие с этим хэштегом.

- Получить закрывающие документы вы сможете на стойке регистрации 21-22 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,
- 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.

20 и 21 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»


К.№13
К.№14
Лебеди
Пляжная зона
Свадебная арка
К.№12
Беседки
Пирс
Живагинские пруды
К.№9
Гриль-бар
К.№8
Сказочный домик
Шатёр
Утки
К.№6
Беседка
Футбольное поле
Ресепшн
Чайный домик
Спорт. площадка
К.№5
Вход №2
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
WC
БАР
К.№10
К.№7/1
К.№2
К.№11
Центр. боулинг, бильярд, развлекательный
Конференц-зона
Служебное здание
Спорт. площадка
Административное здание
Конгресс-Холл "Шишка"
ПАРКОВКА
Въезд на парковку
Заезд на территорию отеля

20 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ 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 **«Российский рынок ИБ сегодня и завтра»** Ведущий: Качалин И.Ф., АНО «НТЦ ЦК» *11 стр.*	Зал «Еловый» Секция **«Исследование и защита цифровых технологий»** Ведущий: Сычев А.М., Positive Technologies *11-12 стр.*	
14:00 – 15:00	Обед		
15:00 – 16:30	Зал «Шишка» Секция **«Решения, продукты и технологии»** Ведущий: Поташников А.В., АО «ИнфоТеКС» *12-13 стр.*	Зал «Еловый» Секция **«Развитие массовых криптосредств»** Ведущие: · Петров А.В., ФСБ России · Смышляев С.В., КриптоПро *13-14 стр.*	Зал «Сосновый» Дискуссия **«HR в ИБ: Поиск, мотивация, адаптация и развитие специалистов. Кадровые практики»** Ведущие: · Хайров И.Е., АИС · Селиванова А., НеоБИТ *14 стр.*
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Кино-концертный зал Дискуссия **«Доверенный Интернет вещей: от «умных домов» до «умных городов»** Ведущие: · Уткин Н.А., АНО «Умный МКД» *14-15 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», I часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *15-16 стр.*	Зал «Сосновый» Секция «**Искусственный интеллект в задачах кибербезопасности: за и против**» Ведущий: Лаврова Д.С., ИКиЗИ СПбПУ *16-18 стр.*
20:00 – 23:00	**Гала-вечер в стиле КИБЕР-РОК** Зал «Шишка»		

21 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 11:30	Зал «Шишка» Круглый стол **«Электронный документооборот и электронная подпись»** Ведущий: Малинин Ю.В., Ассоциация «РОСЭУ» *18 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», II часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *18-19стр.*	Зал «Сосновый» Секция **«Криптографические механизмы в подвижной радиотелефонной связи»** Ведущие: · Шишкин В.А., АО «НПК «Криптонит» · Мареева Е. В., ООО «СПБ» *20-21 стр.*
11:30 – 12:00	Кофе-брейк		
12:00 – 14:00	Зал «Шишка» Круглый стол **«Импортоопережение в банковской сфере»** Ведущие: · Елистратов А.А., Банк России · Горелов Д.Л., Компания «Актив», Ассоциация «РусКрипто» *21 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», III часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *21-23 стр.*	Зал «Сосновый» Секция **«Квантовые коммуникации и квантовая криптография»** Ведущий: Корольков А.В., Академия криптографии РФ *23-24 стр.*
14:00 – 15:00	Обед		
15:00 – 16:30	Зал «Шишка» Секция **«Новые информационные технологии и криптография в финансах»** Ведущий: · Папаев И.С. · Елистратов А.А., Банк России *24-25 стр.*	Зал «Еловый» Секция **«Криптография и криптоанализ», IV часть** Ведущие: · Матюхин Д.В., ФСБ России · Алексеев Е.К., КриптоПро · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *25-26 стр.*	Зал «Сосновый» Секция **«Перспективные исследования в области кибербезопасности», I часть** Ведущий: Котенко И.В., СПб ФИЦ РАН *26-27 стр.*
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Кино-концертный зал Секция **«Подготовка кадров в области ИБ. Облик специалиста по защите информации 2030»** Ведущий: Белов Е.Б., ФУМО СПО ИБ *27-28 стр.*	Зал «Еловый» Круглый стол **«Настоящее и будущее криптографии в информационных системах»** Ведущий: Качалин А.И., Сбербанк *28 стр.*	Зал «Сосновый» Секция **«Перспективные исследования в области кибербезопасности», II часть** Ведущий: Котенко И.В., СПб ФИЦ РАН *28-31 стр.*

КУЛЬТУРНО-РАЗВЛЕКАТЕЛЬНАЯ ПРОГРАММА

20 МАРТА, СРЕДА

08:00 – 09:00	Завтрак	
08:00 – 09:00	Практика на Досках с гвоздями на РусКрипто’24	Зал «Стеклянный»
20:00 – 23:00	Гала-вечер в стиле КИБЕР-РОК	Зал «Шишка»

21 МАРТА, ЧЕТВЕРГ

08:00 – 09:00	Завтрак	
08:00 – 09:00	Практика на Досках с гвоздями на РусКрипто’24	Зал «Стеклянный»
20:00 – 22:00	Игра в имитацию. Интеллектуальный криптографический квиз с Алексеем Лукацким	Зал «Шишка»

22 МАРТА, ПЯТНИЦА

08:00 – 11:00	Завтрак	
10:00 – 11:00	Банный релакс в спа-зоне	Спа-зона отеля
12:00	Трансфер из отеля до станции метро «Ховрино»	

ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

(в программе возможны изменения)

10:00 – 12:00 Пленарное заседание

Зал «Шишка»

Официальное открытие конференции. Приветственные слова

Страх и ненависть в постквантовой криптографии
***Маршалко Григорий Борисович**, ФСБ России, Академия криптографии Российской Федерации*

Массовая постквантовая криптография: задачи и перспективы
***Смышляев Станислав Витальевич**, д.ф.-м.н., заместитель генерального директора, КриптоПро*

Импортозамещение в криптографической защите массового сегмента пользователей
***Баранов Александр Павлович,** д.ф-м.н., действительный член Академии криптографии Российской Федерации*

12:30 – 14:00 Круглый стол «Российский рынок информационной безопасности сегодня и завтра»

Зал «Шишка»

Круглый стол, посвящённый главным событиям и вызовам российского рынка информационной безопасности, взаимодействию игроков рынка, повышению общей защищённости информационных систем, безопасности государства, бизнеса и граждан.

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

Участники:

- **Шойтов Александр Михайлович,** заместитель министра Минцифры России
- **Лютиков Виталий Сергеевич,** заместитель директора ФСТЭК России
- **Матюхин Дмитрий Викторович**, ФСБ России
- **Гусев Дмитрий Михайлович,** заместитель генерального директора АО «ИнфоТеКС»
- **Смышляев Станислав Витальевич,** заместитель генерального директора компании КриптоПро

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

Зал «Еловый»

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

Ведущий: Сычев Артем Михайлович, советник генерального директора, Positive Technologies

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения
***Наумова Ксения Денисовна**, специалист отдела обнаружения вредоносного ПО экспертного центра безопасности, Positive Technologies*

Большинство вредоносного ПО используют взаимодействие по сети: для скачивания вредоносных файлов, взаимодействия с управляющим сервером. Для сокрытия трафика хакеры используют различные методы шифрования и обфускации - это нужно для того, чтобы специалистам ИБ, изучающим сетевые пакеты, было сложнее определить вредоносность. Будут показаны современные подходы злоумышленников к сокрытию ВПО в сети, а также будут предложены актуальные способы его исследования, детектирования и дальнейшего обнаружения.

Как бы я взломал Рунет

***Первушин Игорь Александрович**, руководитель направления создания базы знаний, СайберОК*

Будет представлена статистика и выводы по результатам продолжающегося более года проекта по анализу защищенности периметра Рунет. Крупные инциденты и опасные уязвимости и реакция на них как на техническом, так и на организационном уровне. Также будут обозначены технические нюансы подобных масштабных проектов, применение LLM, CNN и других трюков для автоматизации рутины.

Обзор атак на протоколы технологии FIDO2

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

***Сабиров Эдуард Радикович**, инженер-программист, Компания «Актив»*

***Мироненко Евгений Олегович**, руководитель отдела исследований, Компания «Актив»*

Технология беспарольной строгой аутентификации FIDO2 постепенно обосновывается в российском сегменте Интернет. Распространение технологии делает ее интересной для злоумышленников с точки зрения эксплуатации уязвимостей. В докладе представлен обзор известных на текущий момент уязвимостей FIDO2, выходящих за рамки модели безопасности технологии.

Микропрограммное обеспечение аппаратных средств – напоминание об угрозах

***Аксененко Юрий Иванович**, к.т.н., председатель совета директоров, ООО «Центр безопасности информации»*

Насколько сложно нарушителю воспользоваться потенциально опасными функциональными возможностями аппаратных средств? Каковы могут быть последствия от использования потенциально опасных функциональных возможностей аппаратных средств? Если все окажется «печально», что мы можем и должны предпринять? Ответы на эти и другие связанные вопросы будут даны в выступлении.

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

Зал «Шишка»

Секция, посвященная актуальным российским разработкам в области криптографии и информационной безопасности. Презентации новых решений, перспективных технологий, продуктов. Обмен мнениями и идеями, обсуждение.

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

Управление уязвимостями: процессы и инструменты

***Дорофеев Александр Владимирович,** генеральный директор АО «Эшелон Технологии»*

Рассмотрены подходы к выявлению известных уязвимостей в информационных системах и проведен их сравнительный анализ. Подробно разобран процесс управления уязвимостями в контексте СМИБ, а также актуальные проблемы, возникающие в ходе внедрения.

Безопасная разработка в жизненном цикле ПО. Балансируем характеристики: функционально, безопасно, быстро и дешево

***Калугина Анастасия Валентиновна,** руководитель направления безопасной разработки и инфраструктуры, АО «ИнфоТеКС»*

Безопасная разработка, какая она? Быстро, качественно, дешево? А если добавляем безопасность? Совместить несовместимое или минимизация трудозатрат в безопасной разработке.

Перспективные подходы к аппаратному ускорению постквантовой криптографии

***Турченко Олег Юрьевич**, к.т.н., исследователь, QApp*

Проводится обзор перспективных подходов к аппаратному ускорению постквантовых алгоритмов. В алгоритмах выделяются наиболее узкие места и предлагаются способы ускорения на основе известных научных результатов.

Национальный удостоверяющий центр - безопасность в Интернете

***Хасин Евгений Владимирович,** врио Директора Департамента обеспечения кибербезопасности, Минцифры России*

Текущая работа НУЦ, ближайшие и долгосрочные планы развития. Перспективы нормативно-правового обеспечения в области выпуска и использования ssl-сертификатов.

О некоторых результатах разработки специализированных комплексов для исследования телекоммуникационных линий связи и межмашинных каналов управления на физическом уровне

***Тараканов Аркадий Борисович,** старший специалист по проектам ИБ, АНО «Национальный технологический центр цифровой криптографии»*

Доклад о результатах создания и испытаний экспериментального образца на базе российской перспективной АЦП и отечественного специализированного ПО, предназначенного для исследования физических трактов низкоскоростных и высокоскоростных каналов и интерфейсов обмена данными, используемых для криптографически и инженерно-криптографически значимых элементов аппаратно-программных средств, комплексов и систем обеспечения информационной безопасности.

15:00 – 16:30 Секция «Развитие массовых криптосредств»

Зал «Еловый»

Секция, состоящая из блока экспертных докладов и дискуссии в формате круглого стола. Посвящена вопросам развития криптографических решений для массового применения бизнесом и гражданами.

Ведущие:

- **Петров Алексей Владимирович,** ФСБ России
- **Смышляев Станислав Витальевич**, КриптоПро

Некоторые примеры уточнения требований к СКЗИ для отдельных информационных систем

***Петров Алексей Владимирович,** ФСБ России*

Сценарии, в которых (не) требуются дополнительные исследования при встраивании СКЗИ

***Багин Дмитрий Валерьевич,** КриптоПро*
***Хачатуров Артур Иванович,** АНСЕР-ПРО*

Внедрение российской криптографии в пользовательские продукты на примере клиентского программного модуля ЕБС

***Приезжая Алина Николаевна,** «Центр биометрических технологий»*

Разработка и эксплуатация программного обеспечения со встроенными криптографическими модулями

***Зинюк Борис Федорович,** Академия криптографии Российской Федерации*

Круглый стол
Эксперты круглого стола:

- **Елистратов Андрей Алексеевич**, Банк России
- **Зинюк Борис Федорович**, Академия криптографии Российской Федерации

- **Качалин Алексей Игоревич**, Сбербанк
- **Багин Дмитрий Валерьевич**, КриптоПро
- **Хачатуров Артур Иванович**, АНСЕР-ПРО
- **Приезжая Алина Николаевна**, «Центр биометрических технологий»

15:00 – 16:30 Дискуссия «HR в ИБ: Поиск, мотивация, адаптация и развитие специалистов. Кадровые практики»

Зал «Сосновый»

Обмен опытом и кейсами по управлению человеческим ресурсами в компаниях отрасли ИТ и информационной безопасности.

Ведущие:
- **Хайров Игорь Евгеньевич,** заместитель директора, Академия Информационных Систем
- **Селиванова Анна Юрьевна,** руководитель по развитию персонала и корпоративной культуры, директор по связям с общественностью, ООО «НеоБИТ»

Участники:
- **Пилипенко Галина,** директор по безопасности, МТС Диджитал
- **Старостина Екатерина Вячеславовна,** директор по развитию, компания Вебмониторэкс
- **Прабарщук Анна Сергеевна,** директор по персоналу, компания «Газинформсервис»
- **Свешников Виктор Алексеевич,** ведущий менеджер по персоналу, АО «ИнфоТеКС»

Вопросы к обсуждению:
- Охота за талантами.
- Хочу, могу, не буду - или все про финансовые ожидания и реальность
- Карьерная лестница: прозрачная/не прозрачная, работающий ли это инструмент для удержания
- Наставник, бадди, тимлид - практики реализации адаптации
- Из технарей в менеджмент и наоборот. И что делать с «переростками» (оверквалификация)
- «Выгорание»: как обнаружить и предотвратить
- Развитие своих или перекупать чужих? В каких ситуациях, что выгоднее и разумнее?
- Корпоративные ценности и культурный код. Оценка влияния на команды.
- Назад в будущее - ушедшие и вернувшиеся.
- Кодекс этики HR в ИБ.

17:00 – 19:00 Дискуссия «Доверенный Интернет вещей: от «умных домов» до «умных городов»

Киноконцертный зал

Участники дискуссии рассмотрят роль криптографии в системах «умный дом», «умный город» и интернет вещей, обсудят принципы и опыт применения передовых решений на примере существующих экосистем и проектов-лидеров, обменяются мнениями по преимуществам и недостаткам использования криптографии в различных сферах применения. Обсуждение поможет экспертам найти консенсус между интересами центров развития градостроительства и задачами обеспечения комплексной безопасности граждан и инфраструктуры. Участники дискуссии (стейкхолдеры знаковых градостроительных проектов – с одной стороны и эксперты в области информационной безопасности и криптографии – с другой) последовательно обменяются мнениями по ключевым вопросам:
- Проектирование и обеспечение информационной безопасности «Умного города» – от концепции до реализации.
- Особенности применения криптографии для экосистем и платформ.
- Криптография в обеспечении безопасности различных секторах экономики – связь, ЖКХ, здравоохранение, промышленность, транспорт.

- Криптография интернета вещей.
- Потребность в современных разработках, решениях, элементной базе.
- Нормативно-правовая база и стандартизация.
- Тиражирование умных сервисов.

Ведущие:

- **Уткин Никита Александрович,** директор АНО «Умный МКД», председатель ТК 194 «Кибер-физические системы»

Эксперты:

- **Заренин Андрей Александрович,** заместитель министра цифрового развития, связи и массовых коммуникаций Российской Федерации
- **Семенихин Игорь Викторович,** директор Центра исследования интернета вещей ФГБУ НИИ Радио
- **Петров Алексей Владимирович,** ФСБ России
- **Горбут Андрей Александрович**, начальник отдела криптографической защиты информации ГКУ Инфогород, Департамент информационных технологий города Москвы
- **Минаков Сергей Сергеевич**, заместитель генерального директора, «НТЦ ЦК», с.н.с. Академии криптографии Российской Федерации
- **Зайдуллин Булат Салаватович,** директор по развитию блока Новостройки ЭР-Телеком
- **Рудина Екатерина Александровна,** руководитель группы аналитиков по информационной безопасности, Лаборатория Касперского

17:00 – 19:00 Секция «Криптография и криптоанализ», I 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

Аддитивно связанные ключи подписи: взломать нельзя использовать

Бабуева Александра Алексеевна, *ведущий инженер-аналитик, КриптоПро*
Кяжин Сергей Николаевич, *к.ф.-м.н., ведущий инженер-аналитик, КриптоПро*

Для некоторых практических приложений представляет интерес использование схемы подписи со связанными ключами. В докладе будут представлены результаты аналитического обзора моделей угроз и нарушителя для анализа схем подписи в случае использования связанных ключей, а также результаты анализа схем подписи ГОСТ, ECDSA, SM2 и Шнорра в указанных моделях безопасности в случае использования аддитивно связанных ключей.

О методах построения схем динамической групповой подписи и атаках на одну схему

Утехина Мария Павловна*, Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики*

Динамические групповые подписи — это механизм, позволяющий не только аутентифицировать подписанное сообщение, но и обеспечивать частичную анонимность подписывающего — анонимность среди участников группы. Динамические групповые подписи также позволяют добавлять новых пользователей на протяжении всего времени работы схемы, не только в момент инициализации схемы. В работе рассматриваются два метода построения схем динамической групповой подписи: метод, использующий рандомизируемые подписи (схемы подписи, в которых по одному значению подписи возможно построить без знания секретного ключа множество других подписей, корректных для того же сообщения), и метод, использующий схему шифрования с открытым ключом. Далее в работе описывается схема динамической групповой подписи, основывающаяся на задаче дискретного логарифмирования, и атаки на свойство анонимности данной подписи.

Encrypt-then-Sign или Sign-then-Encrypt, вот в чем вопрос

Ахметзянова Лилия Руслановна, *к.ф.-м.н., зам. начальника отдела криптографических исследований, КриптоПро*

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

Стандартно для одновременного обеспечения аутентичности и конфиденциальности сообщений в системах, где может быть несколько отправителей или несколько получателей, используются комбинации схемы подписи и схемы шифрования с открытым ключом, а именно либо комбинация Sign-then-Encrypt (шифруется сообщение и подпись), либо комбинация Encrypt-then-Sign (подписывается шифртекст сообщения). В настоящем докладе будут представлены результаты анализа указанных двух подходов к комбинированию с точки зрения обеспечения безопасности в многопользовательских системах.

Показуемая стойкость в задаче обфускации криптографических исследований

Маршалко Григорий Борисович*, Академия криптографии Российской Федерации, МИЭМ НИУ ВШЭ*

Фомин Денис Бониславович*, к.ф.-м.н., Академия криптографии Российской Федерации, МИЭМ НИУ ВШЭ*

Основной задачей, решаемой в ходе проведения криптографических исследований, является получение обоснованных оценок стойкости криптографического механизма. В настоящее время особое распространение получил теоретико-информационный подход, сводящийся к обоснованию неотличимости результатов проведённых изысканий от возможных результатов всесторонних криптографических исследований. В этом смысле основная задача исследователя – построить релевантную модель проведения криптографических исследований такую, что потенциальный рецензент не сможет в рамках взаимодействия с моделью сделать обоснованный вывод видит ли он результаты полных (исчерпывающих) криптографических исследований или нет. В докладе на основе изучения ряда примеров и гипотетических ситуаций рассматриваются вопросы отличия используемого в современной криптографической практике теоретико-информационного подхода от проведения реальных криптографических исследований.

RC4OK. Модифицированная версия RC4

Ховайко Олег Игоревич, *компания «Эмеркоин»*

Щелкунов Дмитрий Анатольевич, *к.т.н., компания «Рекрипт»*

Описывается модифицированная версия поточного шифра RC4. Модификации позволяют реализовать легковесный криптографически стойкий высокоскоростной генератор случайных чисел, подходящий для использования как в IoT, так и в качестве соответствующего компонента ОС. Высокая скорость и низкая ресурсоёмкость генератора достигаются, в том числе, за счёт оригинального механизма добавления энтропии из внешних источников

О сложности алгоритмов последовательного опробования (АПО)

Фомичев Владимир Михайлович, *д.ф.-м.н., профессор, научный консультант ООО «Код Безопасности», ведущий научный сотрудник ФИЦ ИУ РАН*

Общая задача решения системы булевых уравнений имеет высокую сложность. В докладе показано, что перестановкой уравнений системы, часть которых зависит не от всех переменных, достигается приближение к треугольной системе уравнений, что снижает среднюю сложность алгоритмов последовательного опробования (АПО) в естественной вероятностной модели вычислений. Предложен алгоритм поиска подходящей перестановки уравнений с учетом структуры множеств существенных переменных уравнений, дана оценка сложности АПО. Приведен пример.

17:00 – 19:00 Секция «Искусственный интеллект в задачах кибербезопасности: за и против»

Зал «Сосновый»

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.

Ведущий: Лаврова Дарья Сергеевна, д.т.н., профессор Высшей школы кибербезопасности Санкт-Петербургского политехнического университета Петра Великого

Противодействие стегоанализу с использованием генеративно-состязательных сетей

***Сергадеева Анастасия Игоревна**, Высшая школа кибербезопасности Санкт-Петербургского политехнического университета Петра Великого*

Доклад содержит исследование методов противодействия стегоанализу, особенное внимание уделяется подходам на основе искусственного интеллекта. Предлагаемый подход ориентирован на изображения, он базируется на использовании генеративно-состязательных сетей с учетом значимости пикселей.

Обнаружение искусственно синтезированных аудиофайлов с использованием графовых нейронных сетей и алгоритмических методов анализа текста

***Изотова Оксана Александровна**, ООО «Лаборатория кибербезопасности»*

Доклад посвящен исследованию подходов к решению проблемы обнаружения искусственно синтезированных медиаданных на примере аудиоданных. Предлагается сочетать единовременный анализ характеристик аудиофайла и его смысловой составляющей , представленной в виде текста. В основе подхода лежат графовые нейронные сети и алгоритмические подходы на основе анализа ключевых слов и тональности текста.

Обфускация модели искусственной нейронной сети с применением афинных преобразований

***Гололобов Никита Вячеславович**, Высшая школа кибербезопасности Санкт-Петербургского политехнического университета Петра Великого*

В докладе поднимается вопрос обеспечения безопасности модели искусственной нейронной сети посредством изменения ее структуры и весов. Работоспособность модели ИНС при этом сохраняется, однако в условиях отсутствия обратных преобразований, ее функциональные характеристики становятся непригодными для использования. Предложенный метод позволяет защитить ИНС от несанкционированного запуска в случае ее утечки ввиду отсутствия у нарушителя знаний о выполненных в отношении ИНС преобразований.

Защита программно-определяемых сетей с использованием квантовых нейронных сетей

***Соболев Николай Владиславович**, Высшая школа кибербезопасности Санкт-Петербургского политехнического университета Петра Великого*

Доклад посвящен исследованию подходов к защите программно-определяемых сетей (Software-Defined Networking, SDN) от кибератак. Предоставляя гибкий и эффективный способ управления сетевыми ресурсами, программно-определяемые сети, тем не менее, уязвимы к ряду специфичных атак. Предложен подход, базирующийся на использовании квантовых нейронных сетей как инструмента повышения безопасности программно-определяемых сетей.

Реализованные в решение методики обезличивания и создания синтетических наборов для обеспечения защиты персональных данных, в том числе для их безопасного использования в системах искусственного интеллекта.

***Ганелин Петр Владимирович,** советник по стратегии, АНО «НТЦ ЦК»*

В рамках доклада представляется описание создания макета технического решения с программными библиотеками обезличивания и производства синтетических наборов данных, а также функционалом, позволяющим обеспечивать оценки статистических свойств массивов.

О статическом анализе исполняемых файлов на содержание вредоносного кода

***Щелкунова Надежда Владимировна ,** компания «Вычислительные решения»*

***Щелкунов Дмитрий Анатольевич ,** к.т.н., компания «Рекрипт»*

В работе описывается статический анализ исполняемых файлов с помощью моделей на основе машинного и глубокого обучения.

Синтез сетевой инфраструктуры самоорганизующихся киберфизических систем с использованием искусственного интеллекта

Павленко Евгений Юрьевич, *Высшая школа кибербезопасности Санкт-Петербургского политехнического университета Петра Великого*

Доклад посвящен исследованию проблемы синтеза сетевой инфраструктуры киберфизических систем, обладающих способностью к самоорганизации, таким образом, чтобы обеспечить ее устойчивость к кибератакам. Сформулированы и математически описаны критерии синтеза, определены графовые метрики и инварианты, которые будут использоваться при синтезе. Рассмотрены алгоритмы машинного обучения и архитектуры нейронных сетей, подходящие для решения поставленной задачи.

*Исследование выполнено при финансовой поддержке Минцифры России в рамках конкурса «Грант ИБ МТУСИ» (соглашение № 40469-04/23-Д от 01.08.2023).

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

(в программе возможны изменения)

10:00 – 11:30 Круглый стол «Электронный документооборот и электронная подпись»

Зал «Шишка»

Ведущие эксперты отрасли и регуляторы обсудят нормативные, организационные и технологические аспекты российского юридически значимого электронного документооборота, вопросы использования квалифицированной электронной подписи государством, гражданами и бизнесом.

Ведущий: Малинин Юрий Витальевич, президент Ассоциации «РОСЭУ»

Участники:

- **Кузнецов Роман Валерьевич**, директор Правового департамента Минцифры России
- **Бондарь Денис Игоревич**, ФСБ России
- **Новиков Федор Вадимович,** начальник управления электронного документооборота, ФНС России
- **Маслов Юрий Геннадьевич**, коммерческий директор компании КриптоПро, эксперт Ассоциации «РОСЭУ»
- **Ярунин Александр Андреевич**, начальник управления криптографии X5 Group, эксперт Ассоциации «РОСЭУ»
- **Кирюшкин Сергей Анатольевич**, советник – начальник удостоверяющего центра «Газинформсервис», эксперт РОСЭУ

10:00 – 11:40 Секция «Криптография и криптоанализ», II часть

Зал «Еловый»

Ведущие:

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

О стойкости алгоритма блочного шифрования КБ-256 к атакам с использованием квантовых алгоритмов

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

Поляков Михаил Вадимович, *ООО «Код Безопасности», МГТУ им. Н.Э. Баумана*

КБ-256 – открытый алгоритм блочного шифрования, рекомендованный для защиты больших объемов данных, который имеет состоятельные оценки «классической» стойкости. В рамках доклада рассматривается вопрос криптографической стойкости КБ-256 в модели атакующего, имеющего доступ к квантовому компьютеру. В частности, оценивается трудоемкость применения алгоритма Гровера, а также его комбинации с алгоритмом Саймона.

Усиление квантовой угрозы на примере оптимизированной атаки Гровера для S-AES

***Моисеевский Алексей Денисович**, Центр научных исследований и перспективных разработок ИнфоТеКС, Центр квантовых технологий МГУ имени М. В. Ломоносова*

***Манько Софья Дмитриевна**, Центр научных исследований и перспективных разработок ИнфоТеКС*

В докладе представлены оптимизированные подходы к построению квантовой атаки с помощью алгоритма Гровера на блочный шифр S-AES. Известные ранее способы построения подобной атаки требовали 32 и более кубитов. На предыдущих этапах работы были найдены альтернативные схемы атак с более низкими требованиями по числу кубитов, а также способные работать с частичной утечкой ключа. В данной работе рассматривается схема прямой атаки Гровера с обработкой однобайтовой утечки, требующая 24 кубита, а также схема атаки разделением, требующая 23 – 4 * n кубитов при утечке n полубайтов ключа. Такое снижение ресурсных требований позволило произвести моделирование предложенных атак на квантовом эмуляторе, а также анализ устойчивости полученных квантовых схем к элементарным шумам, что является оригинальным результатом работы. Это, в свою очередь, позволило провести анализ некоторых статистических свойств ключей, таких как средне количество коллизий, с помощью квантового алгоритма.

Об оценке трудоёмкости перебора ключей алгоритмом Гровера с неравновзвешенным состоянием на входе

***Щербаченко Андрей Александрович**, специалист, ООО «СФБ Лаб», НИУ ВШЭ*

Рассматривается модификация алгоритма Гровера, в которой на вход алгоритма подается неравновзвешенное квантовое состояние ключей, характеризующееся заданным следовым расстоянием до равновзвешенного. В таких условиях установлена нижняя оценка средней трудоемкости для случая, когда алгоритм используется для перебора ε-секретных ключей, вырабатываемых в результате сеанса квантового распределения ключей. Обобщено на случай смешанного состояния.

О свойствах безопасности одного режима работы блочных шифров при наличии у нарушителя доступа к квантовому оракулу

***Коренева Алиса Михайловна,** к.ф.-м.н., начальник отдела криптографического анализа ООО «Код Безопасности», доцент кафедры ИБ Финансового университета при Правительстве РФ*

***Фирсов Георгий Валентинович,** старший системный программист 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. Данный режим представляет собой модификацию режима гаммирования со специальным алгоритмом выработки синхропосылки и начального значения счетчика из номера раздела и номера сектора. В данной работе построена эффективная атака различения на режим DEC в условиях доступа нарушителя к квантовому оракулу.

Квантовые технологии в информационной безопасности: новые подходы для криптоанализа и квантово-устойчивые алгоритмы

***Фёдоров Алексей Константинович**, директор Института физики и квантовой инженерии НИТУ МИСИС*

Одним из приложений квантовых вычислительных устройств является криптоанализ существующих алгоритмов шифрования, в частности алгоритмов с открытым ключом. Вместе с тем, квантовые технологии развиваются и в направлении защиты информации: разрабатываются технологии распределения криптографических ключей с помощью квантовых устройств и квантово-устойчивые алгоритмы шифрования. В докладе будет дан обзор последних достижений в области квантовых алгоритмов для криптоанализа, включая результаты в области вариационной квантовой факторизации. Также будет представлен прогресс в области разработки и внедрения квантово-устойчивых систем, основанных на синергии квантовых коммуникаций и постквантовой криптографии.

10:00 – 11:30 Секция «Криптографические механизмы в подвижной радиотелефонной связи»

Зал «Сосновый»

В рамках секции будут обсуждаться вопросы безопасности технологий, применяемых в подвижной радиотелефонной связи. Основное внимание будет уделено технологиям 5G и eSIM и сосредоточено на таких вопросах, как разработка, анализ безопасности и внедрение отечественных криптографических механизмов, национальная и международная стандартизация, безопасная реализация механизмов.

Ведущие:

- **Шишкин Василий Алексеевич,** к.ф.-м.н., руководитель лаборатории криптографии, АО «НПК «Криптонит»
- **Мареева Елена Владимировна,** заместитель генерального директора по НТР, ООО «СПБ»

Разработка протокола аутентифицированной выработки ключей 5G-AKA-GOST

***Давыдов Степан Андреевич**, старший специалист-исследователь лаборатории криптографии, АО «НПК «Криптонит»*

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

***Шкуратов Юрий Дмитриевич**, младший специалист-исследователь лаборатории криптографии, АО «НПК «Криптонит»*

В рамках выполненной в 2023 году НИР АНО «НТЦ ЦК» «Мобильность» на основе стандартов 3GPP был разработан отечественный механизм аутентификации в сетях 5G, содержащий схему ECIES и протокол 5G-AKA-GOST. Обоснована стойкость разработанного механизма, рассмотрены вопросы внедрения в отечественный сегмент ПРТС и гармонизации с международными стандартами.

Сегменты криптографической защиты в сетях ПРТС 5-го поколения

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

***Самохвалов Роман Игоревич**, специалист-исследователь в области телекоммуникаций лаборатории телекоммуникаций и спецтехники, АО «НПК «Криптонит»*

В докладе рассматриваются подлежащие защите сегменты ПРТС, используемые в них криптографические механизмы и вопросы внедрения их отечественных аналогов. Особое внимание уделяется стойкости алгоритмов обеспечения конфиденциальности и целостности трафика (NEA, NIA), а также возможностям перехода на российские стандартизованные криптографические механизмы (IPSec, IKEv2, TLS).

Защищенный универсальный протокол передачи данных и управления микросхемой интеллектуальной карты UICC / eUICC в сетях подвижной радиосвязи (secure universal protocol for downloading data and managing the smart card chip – SECUNDA)

***Грезина Софья Валерьевна**, ведущий инженер-аналитик, ООО «СПБ»*

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

В докладе будут освещены основные принципы построения протокола SECUNDA: ключевая система, процедура взаимной аутентификации хост-системы и микросхемы интеллектуальной карты, механизмы защиты передаваемых в рамках устанавливаемой сессии сообщений и конфиденциальных данных, а также возможные сценарии применения протокола в сети подвижной радиотелефонной связи.

Адаптивная методика построения модели угроз для процедур генерации, хранения и доведения цифрового профиля абонента сети подвижной радиосвязи

***Гончаров Сергей Александрович**, ведущий специалист, ООО «СПБ»*

***Емельянов Виктор Михайлович**, к.ф.-м.н., руководитель направления, ООО «СПБ»*

В докладе будет представлена адаптивная методика построения модели угроз для процедур генерации, хранения и доведения цифрового профиля абонента сети подвижной радиотелефонной связи, которая позволяет получить актуализированный перечень угроз на основании векторов целей и возможностей нарушителей, на основе которого формулируются требования по защите информации и могут быть уточнены механизмы работы с цифровым профилем.

О некоторых результатах в области информационной безопасности перспективных сетей подвижной радиосвязи в Российской Федерации

***Науменко Антон Павлович**, руководитель направления, ООО «СФБ Лаб», АО «ИнфоТеКС»*

В докладе рассматриваются результаты, полученные в ходе работ по направлению развития сетей подвижной радиосвязи в Российской Федерации и возможные перспективы их использования.

12:00 – 14:00 Круглый стол «Импортоопережение в банковской сфере»

Зал «Шишка»

Ведущие:

- **Елистратов Андрей Алексеевич,** Банк России
- **Горелов Дмитрий Львович,** управляющий партнер, Компания «Актив», директор Ассоциации «РусКрипто»

Участники:

- **Зинюк Борис Фёдорович,** Академия криптографии Российской Федерации
- **Шибина Ольга Михайловна,** ООО «Штрих-М»
- **Евтушенко Владимир Олегович,** ООО «СмартКардСервис»
- **Лебедев Александр Владимирович,** ООО «НМ-Тех»
- **Мареева Елена Владимировна,** ООО «СПБ»
- **Луцик Павел Иванович,** КриптоПро
- **Голубцов Павел Евгеньевич,** генеральный директор ООО «Пэй Киоск»

Основные темы:

- Требования и порядок сертификации российских СКЗИ для проведения карточных платежей.
- Как информационная безопасность карточных платежей уже сейчас обеспечивается российскими СКЗИ.
- Темпы и перспективы внедрения российских СКЗИ в банковской сфере (карта, POS, банкомат, HSM и т.п.).

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

Зал «Еловый»

Ведущие:

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

Анализ устойчивости постквантовой электронной подписи «Шиповник» к атакам, нацеленным на хэш-функции

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

***Дас Диана Кантаевна,** НПК «Криптонит», МГУ им. М.В. Ломоносова*

Постквантовая схема подписи «Шиповник» на основе кодов, исправляющих ошибки, является одним из кандидатов на новый российский стандарт. Поэтому на данном этапе крайне важно рассмотреть и выявить все ее возможные уязвимости. В работе будет приведена классификация атак на «Шиповник» с использованием алгоритмов, решающих задачи поиска прообраза и второго прообраза внутренней троичной хэш-функции. Также работа будет содержать анализ стойкости схемы подписи на основе сложности этих атак.

Модифицированная схема электронной подписи на основе схемы Штерна

***Ниткин Иван Сергеевич**, университет ИТМО, факультет Безопасности информационных технологий, магистратура*

***Давыдов Вадим Валерьевич**, к.т.н., университет ИТМО, факультет Безопасности информационных технологий*

В рамках описанного исследования предложен алгоритм генерации перестановки для модифицированной схемы подписи на основе схемы Штерна, произведена сравнительная оценка характеристик стандартной и модифицированной схем подписи, а также рассчитана сравнительная оценка уровня криптографической стойкости этих схем.

Постквантовая схема инкапсуляции ключа «Кодиеум»

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

***Чижов Иван Владимирович,** НПК «Криптонит», МГУ им. М.В. Ломоносова, ФИЦ ИУ РАН*

Быстрый прогресс в сфере квантовых технологий явно свидетельствует о необходимости разработки постквантовых механизмов. Такая работа ведется уже некоторое время, однако в России до сих пор нет стандартизированных постквантовых схем. В работе будет представлен новый постквантовый механизм инкапсуляции ключа, предназначенный для последующей стандартизации в России, под названием «Кодиеум». Схема опирается на сложные задачи из теории кодирования. В докладе также будет дана комплексная оценка стойкости «Кодиеума» в классической и квантовой моделях, предварительные наборы параметров и эксплуатационные характеристики полученной схемы.

Обзор применений SAT-решателей в целях криптоанализа симметричных криптографических алгоритмов

***Скоробогатова Марина Андреевна**, Компания «Актив»*

***Панасенко Сергей Петрович,** к.т.н., Компания «Актив»*

Алгоритмы решения проблемы булевой выполнимости (SAT – от Satisfiability) и реализующие их средства (SAT-решатели) позволяют определить выполнимость булевой формулы – существует ли такой набор определенных булевых значений («ложь/истина») переменных формулы, при которых результат формулы становится истинным. Данные алгоритмы широко используются в криптоанализе – различные криптоаналитические задачи могут быть закодированы в виде булевой формулы, после чего для решения такой задачи может быть задействован хорошо изученный и эффективный алгоритмический аппарат SAT-решателей. Доклад посвящен обзору направлений применения SAT-решателей в криптоанализе симметричных криптографических алгоритмов и основных из достигнутых с их помощью результатов.

Применение SAT-решателей для анализа стойкости криптографических хеш-функций

***Давыдов Вадим Валерьевич**, к.т.н., Университет ИТМО, Санкт-Петербургский Государственный Университет Аэрокосмического Приборостроения*

***Заикин Олег Сергеевич**, к.т.н., Институт динамики систем и теории управления им. В.М. Матросова СО РАН*

***Кирьянова Анастасия Павловна**, Университет ИТМО*

Рассмотрены перспективы применения SAT-подхода для анализа стойкости современных криптографических хеш-функций и поточных шифров. В качестве примера успешного применения данного подхода были найдены прообразы неполнораундовых версий хеш-функций финалистов конкурса SHA-3.

Анализ стойкости XSL-семейства алгоритмов блочного шифрования с *a*-отражением к атакам двумерным методом встречи посередине

***Мухортова Алёна Андреевна,** НИЯУ МИФИ, Институт Интеллектуальных Кибернетических Систем*

Низкоресурсные XSL-алгоритмы блочного шифрования MANTIS и PRINCE, предложенные на конференциях ASIACRYPT-2016 и CRYPTO-2012, обладают свойством *a*-отражения. К ним было предложено множество атак на основе дифференциального, интегрального методов, метода встречи посередине и другие. В работе вводится XSL-семейство алгоритмов блочного шифрования с *a*-отражением, обобщающих алгоритмы шифрования MANTIS и PRINCE.

На редуцированные 8-раундовые алгоритмы, относящиеся к этому семейству, предложена атака, основанная на двумерном методе встречи посередине, из которой вытекают атаки на алгоритмы MANTIS и PRINCE. Атака на MANTIS предложена впервые, ее временная сложность составляет 2**110.8 функций зашифрования, объём памяти: 2**67 ячеек памяти по 72 бита. Применение предложенной атаки на PRINCE согласуется с результатами 2016 года.

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

Зал «Сосновый»

Секция посвящена вопросам доказательства криптостойкости, вопросам внедрения и развития квантовых технологий для обеспечения безопасности цифровых данных и сервисов.

Ведущий: Корольков Андрей Вячеславович, Академия криптографии Российской Федерации

Подходы к интеграции технологии квантового распределения ключей в протоколы сетевой защиты данных

***Бородин Михаил Алексеевич**, старший исследователь АО «ИнфоТеКС»*
***Жиляев Андрей Евгеньевич**, к.т.н., старший исследователь, АО «ИнфоТеКС»*

Исследование посвящено пока не нашедшей широкого отражения в научных работах и стандартизующих документах теме использования ключей, полученных с применением технологии КРК, в массово используемых протоколах. Наиболее перспективными для интеграции ключей, полученных с применением технологии КРК, представляются стандартизованные в Российской Федерации протоколы защиты на транспортном и сетевом уровнях: TLS, IPsec, IPlir. В работе были определены основные тенденции в области использования технологии КРК в сетях связи, которые показали, что наиболее перспективной областью развития сетей КРК является построение сетей с доверенными промежуточными узлами. Описан способ взаимодействия СКЗИ, реализующих протоколы защиты информации, с сетями КРК с целью получения квантовозащищенного ключа на основе протокола Протока. В результате показано, что использование ключей, полученных с применением технологии КРК, в протоколах TLS, IPsec, IPlir, позволяет улучшить криптографические качества этих протоколов и не приводит к существенной деградации их эксплуатационных свойств.

Практический анализ защищенности системы КРК от атаки «Trojan Horse»

***Вахрушева Вероника Михайловна**, специалист отдела специальных исследований и разработок, ООО «СФБ Лаб»*

В настоящей работе рассмотрены подходы к анализу защищенности систем квантового распределения ключей от атаки с зондирующим излучением («Trojan Horse»). К предложенным подходам относятся рефлектометрия системы КРК, исследование спектров пропускания защитных компонентов и оценка максимально возможной величины зондирующего излучения. Данные методы позволяют провести оценку среднего числа фотонов, возвращающихся злоумышленнику, которая может быть связана с вероятностью успешного проведения атаки.

Способ защиты от атак, использующих мощное лазерное излучение на основе оптического плавкого предохранителя

***Бугай Кирилл Евгеньевич**, ведущий специалист отдела специальных исследований и разработок, ООО «СФБ Лаб»*

Несанкционированное проникновение излучения всегда было серьезной угрозой для практической безопасности систем квантового распределения ключей (КРК). В настоящей работе представлен оптический предохранитель, основанный на эффекте оптического разряда. Нами были проведены испытания оптического предохранителя на имитационной модели системы КРК, что позволило сформировать методы тестирования и анализа, которые могут быть применены к другим компонентам способным ограничивать мощность в системах КРК.

Исследование и перспективы квантовых коммуникаций с использованием квантового повторителя на многомодовых когерентных состояниях

***Гончаров Роман Константинович,** научный сотрудник, ООО «СМАРТС-Квантателеком», инженер лаборатории квантовых коммуникаций, Университет ИТМО*

Проведен анализ производительности схемы квантового повторителя на многогодовых когерентных состояниях. В рассмотрении применялся подход удвоения числа звеньев, что снижает сложность построения конечной сети и позволяет использовать более простые приближенные выражения. Были определены значения вероятности успешной генерации запутанности и вероятности переброса запутанности, при которых приближенные выражения приближаются к точным. Также проведен сравнительный анализ схем квантового повторителя на многомодовых когерентных состояниях и на источниках фотонных пар. Показано, что использование когерентных состояний дает несколько преимуществ перед источниками фотонных пар.

Построение высокоскоростных систем квантового распределения ключей

Павлов Игорь Денисович, *технический директор, QRate*

Необходимость защиты больших потоков данных в реальном времени требует от промышленных устройств КРК высокой скорости генерации секретных ключей. Эта задача не выполнима без разработки новых, более перспективных квантовых протоколов, выбора оптимальной оптической схемы и разработки нового поколения детекторов одиночных фотонов.

Исследование уязвимостей систем квантового распределения ключа

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

В работе будет предложена классификация, позволяющая разделить атаки, направленные на поиск уязвимостей в аппаратной реализации систем КРК («квантовый хакинг») на несколько основных групп. Для каждой из них будет приведен пример и разработан подход к оценке доступной нарушителю информации. В частности, будут рассмотрены атаки с постселекцией и управлением детектора, а также комбинация атаки «Троянский конь» и атаки на квантовые состояния общего вида. Помимо этого, необходимо выделить набор наблюдаемых, позволяющих отслеживать подобные атаки. Как будет показано в работе, некоторые из них могут быть получены путем модификации протокола КРК, тогда как другие потребуют конструктивных изменений в аппаратной части. Основным результатом работы является сформулированный подход к включению подобных атак в общий критерий стойкости систем КРК.

15:00 – 16:30 Секция «Новые информационные технологии и криптография в финансах»

Зал «Шишка»

Секция, посвященная технологиям безопасности и криптографии в кредитно-финансовой сфере.

Ведущие:

- **Папаев Игорь Сергеевич,** независимый эксперт
- **Елистратов Андрей Алексеевич,** Банк России

Безопасность Открытых API

Товстолип Александр Игоревич, *руководитель управления информационной безопасности, Ассоциация ФинТех*

Протокол конфиденциального скоринга с точки зрения криптографии

Емельянов Петр Николаевич, *генеральный директор, ООО «Блумтех»*

Способы обеспечени требований 833-П у финансового посредника для Цифрового рубля

Косякин Иван Валерьевич, *заместитель генерального директора, ООО «Грин Лайт Технолоджи»*

Цифровой рубль. Подходы к реализации требований по информационной безопасности

Бадмаева Римма Викторовна, *старший менеджер, АО «ИнфоТеКС»*

Возможности применения пороговой подписи в финансах

Курочкин Алексей Вячеславович, *ведущий системный аналитик отдела криптографического анализа, ООО «Код Безопасности»*

Современные биометрические технологии в финансах. Типовые ошибки при внедрении и типовые решения для их исключения

Николаев Данила Евгеньевич, *председатель ТК 098*

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

Зал «Еловый»

Ведущие:

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

О точности оценок стойкости криптопротокола CRISP

Кирюхин Виталий Александрович, *архитектор системы ООО «СФБ Лаб»*

Доказательство стойкости протокола CRISP, включая верхние оценки на вероятность успеха противника, было представлено на CTCrypt 2023. В настоящей работе получены оценки снизу – построены атаки на конфиденциальность и целостность протокола. Тем самым продемонстрировано, что оценки стойкости протокола являются точными. Атака на свойство конфиденциальности основывается на известных методах дешифрования режима гаммирования (CTR). Метод навязывания построен за счёт адаптации атак Митчела на режим имитозащиты (CMAC).

Об использовании российских криптографических алгоритмов в протоколе QUIC

Смыслов Валерий Анатольевич, *АО «ЭЛВИС-ПЛЮС»*

QUIC – новый транспортный протокол с интегрированными средствами защиты на основе протокола TLS 1.3. По сравнению с TCP он обеспечивает многопоточность, быстрое создание соединения, миграцию соединения при изменении IP-адресов сторон, адекватную реакцию на потери пакетов и т.д. QUIC является компонентом http/3 и поддерживается всеми современными web-браузерами и http-серверами. В работе рассматривается возможность использования российских криптонаборов, определенных для TLS 1.3, в протоколе QUIC, описываются потенциальные проблемы и возможные пути их решения.

О применении схемы ECQV для защиты интеллектуальных транспортных систем

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

Развитие интеллектуальных транспортных систем требует передачи большого объёма информации в ограниченный период времени, что делает крайне важной задачу минимизации издержек (overhead), порождаемых средствами защиты. Схема ECQV вместо сертификата (публичный ключ, подпись) формирует специальное значение, позволяющее восстановить публичный ключ и проверить его подлинность. Это позволяет сократить издержки примерно втрое. С использованием методов «доказуемой стойкости» для ECQV были получены верхние оценки на вероятность нарушения свойств безопасности, а также оценена стойкость к известным методам криптоанализа.

Логический вывод в протоколах многосторонних безопасных вычислений

Столовник Дмитрий Александрович*, ТК 26*

В докладе рассматриваются стратегии нарушителя в роли легитимного участника протокола, который путем навязывания вычисляемых функций пытается получить дополнительную информацию о конфиденциальных входах других участников протокола. Анализируются возможные способы противодействия.

О некоторых системах подтверждения персональных данных без их разглашения, использующих неклассические криптографические механизмы

Кяжин Сергей Николаевич, *к.ф.-м.н., АНО «НТЦ ЦК», НИЯУ МИФИ, КриптоПро*

Утехина Мария Павловна, *АНО «НТЦ ЦК», МГУ им М.В. Ломоносова, КриптоПро*

Зюзин Юрий Васильевич, *АНО «НТЦ ЦК», МГУ им М.В. Ломоносова, КриптоПро*
Махонин Илья Владимирович, *АНО «НТЦ ЦК», НИЯУ МИФИ*
Лебедев Вадим Андреевич, *АНО «НТЦ ЦК», НИЯУ МИФИ*
Задача подтверждения персональных данных без их разглашения при предоставлении некоторым сервисом услуги клиенту может быть решена как с помощью классических механизмов (известен, например, протокол ИКС), так и с использованием иных криптографических механизмов. В докладе будут представлены результаты аналитического обзора систем Idemix, U-Prove, ePCS, Privacy Pass, Nymble, использующих неклассические криптографические механизмы.

Обзор подходов к созданию низкоресурсных блокчейн-решений для применения в устройствах интернета вещей

Панасенко Сергей Петрович, *к.т.н., директор по научной работе, Компания «Актив»*
Блокчейн-технологии оказались востребованными в системах Интернета вещей (IoT) и находят достаточно широкое применение в их составе. Основной проблемой в данном случае является высокая ресурсоемкость ряда применяемых в блокчейнах механизмов, прежде всего, криптографических алгоритмов, а также некоторых из методов достижения консенсуса, тогда как IoT-устройства обычно являются ограниченными в вычислительных ресурсах. Данное противоречие решается путем применения низкоресурсных блокчейнов, специально разрабатываемых для использования в условиях ограниченных ресурсов. Доклад посвящен обзору различных подходов к созданию низкоресурсных блокчейнов.

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

Зал «Сосновый»

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

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

Обнаружение атак в интернете вещей с использованием многозадачного обучения и гибридных методов сэмплирования

Котенко Игорь Витальевич, *д.т.н., профессор, заслуженный деятель науки РФ, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН*
Хуэйао Дун, *аспирант, Университет ИТМО*
Предложен подход к обнаружению атак в сетях интернета вещей на основе многозадачного обучения. Проведено сравнение эффективности моделей однозадачного обучения и моделей многозадачного обучения с жестким и мягким совместным использованием параметров. Представлен гибридный метод сэмплирования, сочетающий случайную субдискретизацию с передискретизацией на основе генеративной состязательной сети. Реализован алгоритм инициализации весов для устранения несбалансированной классификации. Результаты экспериментов показали, что модели многозадачного обучения превосходят однозадачное обучение, достигая более высокой эффективности обнаружения, особенно при редких атаках.

Защищенное исполнение нейросетевых алгоритмов классификации образов для задач биометрической аутентификации на базе сетей корреляционных нейронов

Сулавко Алексей Евгеньевич, *д.т.н., доцент кафедры комплексной защиты информации, ведущий научный сотрудник, Омский Государственный технический университет (ОмГТУ)*
Одной из важнейших проблем для систем биометрической аутентификации является обеспечение конфиденциальности биометрических шаблонов и защита от компьютерных атак. В докладе рассматривается новая модель искусственного нейрона и модель нейросетевого преобразователя биометрия-код, которые позволяют построить архитектуру системы биометрической аутентификации, изначально устойчивую к состязательным атакам и другим деструктивным воздействиям со стороны злоумышленника, приводящим к нарушению конфиденциальности биометрических шаблонов.

Приведены результаты экспериментов, подтверждающих эффективность предложенных моделей. В качестве инструмента для моделирования систем классификации биометрических образов применялся пакет программ AIConstructor.

Методы преобразования табличных данных в изображения в задаче выявления аномалий в киберфизических системах

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

Бухтияров Марат Андреевич, *СПбГЭТУ «ЛЭТИ»*

В последнее время для обнаружения вторжений и аномалий в киберфизических системах были предложены различные методы глубокого обучения. В докладе рассматриваются различные подходы к преобразованию табличных данных в изображения и анализируется их влияние на эффективность обнаружения атак, в том числе на способность обнаруживать новые и ранее неизвестные атаки. Эксперименты выполнялись как с использованием сетевого трафика, так и на данных от физических датчиков. На основе проведенного исследования делается вывод о применимости рассмотренного преобразования входного потоках данных в задаче выявления аномалий в киберфизических системах.

Прогнозирование уязвимостей в устройствах Интернета вещей

Левшун Дмитрий Сергеевич, *к.т.н., PhD, доцент кафедры защищенных систем связи, СПбГУТ, старший научный сотрудник лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН*

Построение графов атак с учетом устройств, уязвимости которых не представлены в открытых базах данных, представляет собой сложную задачу. В докладе представлен подход, позволяющий с помощью методов искусственного интеллекта прогнозировать наличие уязвимостей в устройствах на основе схожести их конфигурации с конфигурациями других устройств. Приведены результаты экспериментов, подтверждающих эффективность предложенного решения.

Обеспечение информационной безопасности комплексных очистных сооружений: методология сбора данных

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

Успешные кибератаки на промышленные системы, такие как системы очистки воды, могут привести к непоправимым последствиям для экономики и здоровья населения. Для обнаружения и прогнозирования ранее неизвестных кибератак применяют методы искусственного интеллекта, в частности, машинное обучение и глубокое обучение. Однако применение данных методов ограничено доступностью и качеством наборов данных для обучения. Анализ исследований в данной области показывает, что существует потребность в единой методологии формирования набора данных. В рамках данного исследования предлагается методология создания набора данных для обеспечения кибербезопасности комплексных очистных сооружений. Определены основные этапы методологии и их особенности. Дается сценарий применения методологии, описывающий подготовительные этапы формирования набора данных, а именно спецификацию технологического процесса, разработку тестового стенда и разработку модели атак для рассматриваемого технологического процесса. Набор данных, полученный с использованием разработанной методологии, будет использоваться для разработки и тестирования методов обнаружения кибератак на основе машинного и глубокого обучения, а также для усиления безопасности комплексных очистных сооружений.

17:00 – 19:00 Секция «Подготовка кадров в области информационной безопасности. Облик специалиста по защите информации 2030»

Кино-концертный зал

Круглый стол, посвященный вопросам обучения и повышения квалификации в области информационной безопасности.

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

Образовательные программы специализаций ФГОС ВО 4-го поколения по укрупненной группе специальностей и направлений подготовки (УГСНП) 10.00.00 «Информационная безопасность»

Белов Евгений Борисович, *заместитель председателя ФУМО ВО ИБ*

Гармонизация паспортов научных специальностей 1.2.4. Кибербезопасность, 2.3.6. Методы и системы защиты информации, информационная безопасность и образовательных программ высшего образования

Лось Владимир Павлович, *Президент-Председатель Правления АЗИ, заместитель Председателя КИБ СПК ИТ*

Падарян Вартан Андроникович, *представитель ИСП РАН*

Хорев Анатолий Анатольевич, *заведующий кафедрой НИУ МИЭТ*

Профессиональные стандарты в области информационной безопасности. Профессиональный стандарт «Специалист по защите персональных данных».
Профессиональный стандарт «Специалист по криптографической защите информации»
Профессиональный стандарт «Специалист по защите объектов КИИ»

Белов Евгений Борисович, *Председатель КИБ СПК ИТ*

Лось Владимир Павлович, *Президент-Председатель Правления АЗИ, заместитель Председателя КИБ СПК ИТ*

Пушкин Павел Юрьевич, *директор Института перспективных технологий и индустриального программирования РТУ МИРЭА*

Правиков Дмитрий Игоревич*, заведующий кафедрой РГУ нефти и газа имени И.М. Губкина*

17:00 – 19:00 Круглый стол «Настоящее и будущее криптографии в информационных системах»

Зал «Еловый»

Круглый стол, на котором признанные эксперты в области криптографии обсудят что наиболее важное произошло в криптографической отрасли в последние годы и как это повлияло и будет дальше влиять на информационные системы и пользователей цифровых продуктов.

Ведущий: Качалин Алексей Игоревич, Сбербанк

Участники:

- **Маршалко Григорий Борисович,** Академия криптографии Российской Федерации
- **Алексеев Евгений Константинович,** КриптоПро, АНО «НТЦ ЦК»
- **Шишкин Василий Алексеевич,** АО «НПК «Криптонит»
- **Уривский Алексей Викторович,** АО «ИнфоТеКС»
- **Смыслов Валерий Анатольевич,** АО «ЭЛВИС-ПЛЮС»
- **Елистратов Андрей Алексеевич,** Банк России

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

Зал «Сосновый»

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

Моделирование устойчивости критической информационной инфраструктуры на основе иерархических гиперсетей и сетей Петри

Васинев Дмитрий Александрович, *к.т.н., сотрудник Академии ФСО России*

Бочков Максим Вадимович, *доктор технических наук, профессор, ЧОУ ДПО «Центр предпринимательских рисков»*

Целью работы является моделирование объектов критической информационной инфраструктуры (КИИ) на основе математического аппарата гиперсетей и сетей Петри. Предлагаемый способ построения математических моделей позволяет разработать параметрически точные имитационные модели для исследования свойств защищенности и устойчивости объектов КИИ и моделировать воздействия на них компьютерных атак (КА). Предлагаемый способ имитационного моделирования позволяет учитывать конфигурационные и коммуникационные особенности построения и функционирования, динамику воздействия нарушителя на объекты КИИ, существующую политику безопасности, проводить моделирование функциональных и структурных свойств устойчивости, а также исследовать степень влияния этих элементов на защищенность объекта КИИ. Это позволяет осуществлять оценку защищенности, обеспечивать информационную безопасность объектов КИИ с учетом конфигурационных и коммуникационных параметров объекта КИИ, уменьшать зависимость от экспертных оценок.

Двухфакторная авторизация для обеспечения безопасности устройств Интернета вещей

Сагатов Евгений Собирович, *к.т.н., доцент, Самарский национальный исследовательский университет*
Сухов Никита Сергеевич, *ПАО «Промсвязьбанк»*
Сухов Андрей Михайлович, *д.т.н., профессор кафедры суперкомпьютеров и общей информатики, Самарский национальный исследовательский университет*

Принцип двухфакторной авторизации предполагает, что при входе в систему управления сервисом требуется ввести два ключа, полученных при помощи двух или более независимых технологий связи. В большинстве технологий IoT устройства подключаются посредством беспроводных технологий связи. Беспроводное подключение предполагает только однофакторную аутентификацию в момент подключения, которую можно легко обойти. Единственный способ добавить дополнительный процесс аутентификации заключается в использовании прикладных протоколов. Требуется разработать такую последовательность действий, которая бы исключала доступ в публичную сеть до процедуры вторичной аутентификации. Для этого необходимо увязать процессы вторичной аутентификации и авторизации (снятия ограничений с сетевого подключения IoT устройства). В предложенном в докладе способе подключения IoT устройств по беспроводной технологии DECT первоначально выполняется аутентификация абонентского устройства DECT, сопряженного с IoT устройством. Разрешение на функционирование абонентского устройства должно выдаваться только после проверки базовой станции, этот процесс является второй стадией аутентификации. Протокол прикладного уровня MQTT также можно попытаться использовать для дополнительного процесса аутентификации.

Цифровые двойники в системах управления информационной безопасностью

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»*

Термин «цифровой двойник» (Digital twin, сокр. DT) появился около десяти лет назад и до сих пор не имеет четкого определения. Тем не менее интерес к этому направлению постоянно возрастает особенно в тех областях, где много неформализуемых задач, нечетких значений параметров, случайных и непредвиденных ситуаций. DT во многом могут решать часть этих задач на этапах проектирования и работы сложных систем управления. В докладе рассматривается модель DT, ориентированная на системы управления информационной безопасностью (СУИБ), позволяющая находить обоснованные решения по выбранным критериям при проектировании СУИБ.

Метод оценки исходного уровня доверия к выбранному фактору в многофакторной системе аутентификации

Беззатеев Сергей Валентинович, *д.т.н., заведующий кафедрой информационной безопасности, Государственный университет аэрокосмического приборостроения*
Афанасьева Александра Валентиновна, *старший преподаватель, Государственный университет аэрокосмического приборостроения*
Волошина Наталия Викторовна, *к.т.н., доцент, Университет ИТМО*

Разработанный метод позволяет определить исходные уровни доверия для таких факторов (FAR, FRR, EER и др.), не зависящие от используемой дальнейшей обработки. Выбирается некоторое число параметров фактора. Выбираются наиболее значимые параметры фактора, если они замеряются вручную или с использованием автоматического детектора/ов, либо берутся компоненты вектора признаков при использовании детекторов нейронной сети. Число наиболее значимых параметров фактора определяет размерность пространства, в котором строятся соответствующие каждому субъекту гиберсферы. Взаимное расположение этих гиперсфер определяет основные характеристики фактора - FAR, FRR, ERR и др.

Концепция взвешенной структуры контейнера как ключевой подход к стеганографической защите мультимедиа данных

Волошина Наталия Викторовна, *к.т.н., доцент, Университет ИТМО*
Калабишка Михаил Михайлович, *аспирант, Университет ИТМО*
Беззатеев Сергей Валентинович, *д.т.н., заведующий кафедрой информационной безопасности, Государственный университет аэрокосмического приборостроения*

Представлен анализ возможностей применения концепции взвешенной структуры контейнера как подхода для реализации эффективной защиты мультимедиа данных, обладающих неравномерной избыточностью, а также позволяющей противодействовать атакам фальсификации. Предложен комплексный подход по организации защиты мультимедиа данных, включающих решение задачи определения параметров взвешенного контейнера, поиска оптимальных кодовых конструкций во взвешенной метрике Хэмминга.

Повышение защищенности интеллектуальных систем в условиях деструктивного воздействия на основе генеративно-состязательных сетей

Васильев Никита Алексеевич, *с.н.с., Военная академия связи*
Лаута Олег Сергеевич, *д.т.н., доцент, ГУМРФ С.О. Макарова*
Котенко Игорь Витальевич, *д.т.н., профессор, заслуженный деятель науки РФ, главный научный сотрудник и руководитель научно-исследовательской лаборатории проблем компьютерной безопасности, СПб ФИЦ РАН*
Делова Мария Алексеевна, *к.м.н, Военная академия связи*

В докладе обобщаются признаки классификации атак на системы машинного обучения и меры защиты от них. Выделяются и рассматриваются наиболее распространенные угрозы, которые по своему типу относятся к атакам «белого ящика» или «черного ящика». Обосновываются наиболее распространенные методы защиты от атак на системы машинного обучения. Для ряда наиболее сложных методов приводится их детальное описание на уровне отдельных этапов. Выделяются особенности реализации методов защиты, позволяющие повысить эффективность обнаружения атак на системы машинного обучения.

Мультиагентное обучение с подкреплением в задачах информационной безопасности

Чернышов Юрий Юрьевич, *к.ф.-м.н., доцент кафедры ИТиСУ ИРИТ-РТФ УрФУ*

Обучение с подкреплением является популярным инструментов в задачах с высокой степенью неопределенности и изменчивости условий. Взаимодействие агента и среды позволяет находить эффективные стратегии поведения и, основываясь на постоянном эксперименте, оптимизировать эти стратегии при изменении условий. При моделировании поведения нескольких агентов возникает вопрос о взаимном обучении, передаче знаний от одного агента к другому, что позволяет повысить эффективность обучения. В докладе рассматриваются различные подходы к организации мультиагентного обучения с подкреплением и их применение к задачам кибербезопасности.

Форматно-логический контроль, как основа безопасности микросервисов

Юрьев Артемий Сергеевич, *аспирант ИСП РАН / исполнительный директор, Департамент развития технологий защиты информации, АО Газпромбанк*
Крибель Александр Михайлович, *к.т.н., директор проекта, Департамент развития технологий защиты информации, АО Газпромбанк*
Ирхин Артем Александрович, *МТУСИ, кафедра инфокоммуникационных технологий и систем связи*
Алхимов Василий Юрьевич, *РТУ МИРЭА, кафедра КБ-1 «Защита информации»*

В ходе исследования были рассмотрены современные прикладные архитектурные подходы к защите микросервисов от вредоносных атак с акцентом на анализ эффективности файерволов веб-приложений. Проанализированы возможности применения белых списков в сочетании с форматно-логическим контролем входных данных. С помощью анализа эффективности каждого метода авторы пришли к выводу, что их совместное применение позволяет эффективно противодействовать современным угрозам. Вместе с тем, в докладе подчеркивается необходимость осознания потенциальных рисков и недостатков данного подхода, которые необходимо учитывать при проектировании различных информационных бизнес решений.

Уровни доверия аутентификации при использовании одиночных криптографических механизмов и многосторонних криптографических протоколов аутентификации субъектов доступа

***Сабанов Алексей Геннадьевич**, д.т.н., профессор, МГТУ им. Н.Э. Баумана, АНО «НТЦ ЦК»*

Целью работы является повышение доверия к идентификации и аутентификации субъектов доступа в двух проектах АНО НТЦ ЦК, связанных с совершенствованием криптографических механизмов и протоколов с помощью имплементации российских криптографических методов и средств. Первый проект посвящен разработке и испытаниям макета доверенного программно-технического решения, обеспечивающего повышение достоверности взаимной аутентификации в протоколах маршрутизации сетевого трафика с использованием российских криптографических механизмов. Также рассмотрен проект обеспечения делегированной идентификации и аутентификации пользователей по запросам от внешних информационных систем, клиентов провайдера идентификации и аутентификации, согласно протоколу аутентификации, расширяющему состав спецификации протокола OpenID Connect 1.0 с учетом применения отечественных криптографических алгоритмов.

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 28 лет АИС предоставляет образовательные услуги по информационной безопасности, информационным технологиям, конкурентной разведке и экономической безопасности. Обучение своих кадров нам доверяют Социальный 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, 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;
- 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.

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

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

АИС

#УЧИСЬВАИС

Академия Информационных Систем

www.infosystems.ru
www.vipforum.ru

Учебный центр профессионального образования в сфере информационной и экономической безопасности, информационных технологий, конкурентной разведки и электронного документооборота.

- Учебные курсы, согласованные с регуляторами (ФСБ России, ФСТЭК России, ФУМО ВО ИБ, Банк России)
- Организация вебинаров, семинаров, митапов в собственной студии
- Организация конференций, форумов, выездных мероприятий

+7 (495) 120-04-02

СОПРИКОСНИСЬ С БУДУЩИМ

ТИМБИЛДИНГ
НЕЙРО-ГАЛЕРЕЯ

ВИПФОРУМ
Организация деловых событий

ЗАЛ «ЕЛОВЫЙ»
19 МАРТА, 20:00

конференция
РусКрипто

АИС

ВЫ МОЖЕТЕ ВЫИГРАТЬ!
НЕТ НИЧЕГО ПРОЩЕ!

РОЗЫГРЫШ ПРИЗОВ СРЕДИ УЧАСТНИКОВ «РУСКРИПТО 2024»
БУДЕТ ПРОВОДИТЬСЯ ВО ВРЕМЯ ГАЛА-УЖИНА

ГЛАВНЫЙ ПРИЗ
SONY PLAYSTATION 5 (PS5)

СКАЧИВАЙТЕ ПРИЛОЖЕНИЕ,
БУДЬТЕ АКТИВНЫМ УЧАСТНИКОМ
РУСКРИПТО 2024


ГАЛА-ВЕЧЕР
В СТИЛЕ КИБЕР-РОК
ЗАЛ «ШИШКА»
20 МАРТА, 20:00
ВИПФОРУМ
Организация деловых событий
конференция
РусКрипто
АИС

ИГРА В ИМИТАЦИЮ

ИНТЕЛЛЕКТУАЛЬНЫЙ КРИПТОГРАФИЧЕСКИЙ КВИЗ С АЛЕКСЕЕМ ЛУКАЦКИМ

ЗАЛ «ШИШКА»

21 МАРТА, 20:00

ВИПФОРУМ
Организация деловых событий

конференция
РусКрипто

АИС

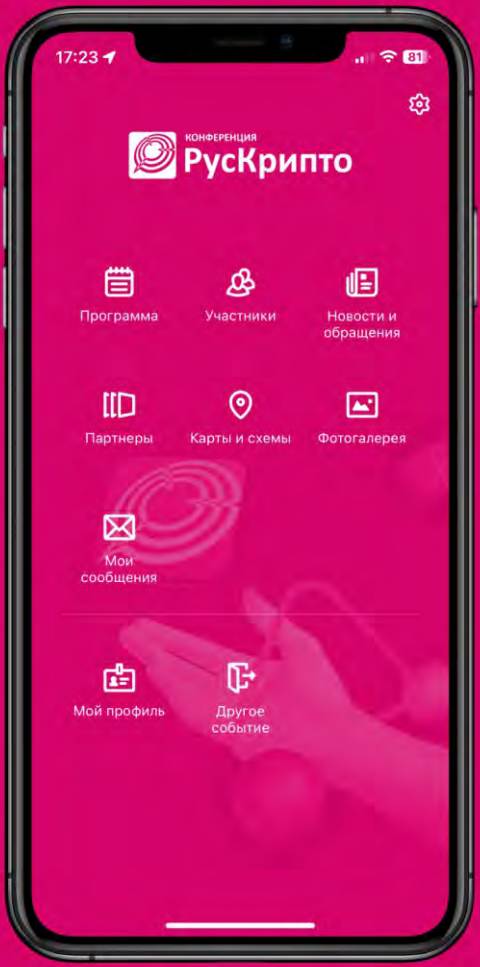
Практика на Досках с Гвоздями

20, 21 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)!

ДЛЯ ЗАМЕТОК



Event.Rocks

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

В приложении введите
ID события —

РусКрипто

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

Скачать из Google Play

+7 (495)902-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru