

Программа конференции «РусКрипто'2025»

18 марта, вторник

День заезда

15:00	Трансфер от станции метро «Ховрино», выход 1 до отеля «Солнечный Park Hotel & SPA»
16:00 – 22:00	Заезд и регистрация участников, проживающих в отеле. Ужин. Вечерняя программа

19 марта, среда

08:00 – 09:00	Завтрак		
09:00 – 10:00	Регистрация участников конференции		
10:00 – 12:00	Официальное открытие конференции Пленарное заседание. Зал «Шишка»		
12:00 – 12:30	Кофе-брейк		
12:30 – 14:00	Российский рынок информационной безопасности Круглый стол. Зал «Шишка»	Конфиденциальные вычисления Круглый стол. Зал «Еловый»	HR в ИБ: поиск, мотивация, адаптация и развитие специалистов. Кадровые практики и современные технологии Тематическая секция. Киноконцертный зал
14:00 – 15:00	Обед		
15:00 – 16:30	Решения, продукты и технологии Тематическая секция. Зал «Шишка»	Разработка, внедрение и эксплуатация средств криптографической защиты информации Тематическая секция. Зал «Еловый»	Искусственный интеллект в кибербезопасности: защита будущего или новые угрозы? Тематическая секция. Зал «Сосновый»
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Защита данных Тематическая секция. Киноконцертный зал	Криптография и криптоанализ. 1 часть Тематическая секция. Зал «Еловый»	Криптографические решения для киберфизических систем Тематическая секция. Зал «Сосновый»
19:00 – 23:00	Ужин. Вечерняя программа		



20 марта, четверг

08:00 – 10:00	Завтрак		
10:00 – 11:30	Технологии электронной подписи Тематическая секция. Зал «Шишка»	Криптография и криптоанализ, 2 часть Тематическая секция. Зал «Еловый»	Криптография в NGFW Круглый стол. Зал «Сосновый»
11:30 – 12:00	Кофе-брейк		
12:00 – 14:00	Информационная безопасность и криптография в банковской сфере, 1 часть Тематическая секция. Зал «Шишка»	Криптография и криптоанализ, 3 часть Тематическая секция. Зал «Еловый»	Квантовые коммуникации и квантовая криптография Тематическая секция. Зал «Сосновый»
14:00 – 15:00	Обед		
15:00 – 16:30	Банковский бизнес VS криптографическая отрасль Дискуссионная панель. Зал «Шишка»	Криптография и криптоанализ, 4 часть Тематическая секция. Зал «Еловый»	Стандартизация и совместимость криптографических механизмов, продуктов и решений Тематическая секция. Зал «Сосновый»
16:30 – 17:00	Кофе-брейк		
17:00 – 19:00	Информационная безопасность и криптография в банковской сфере, 2 часть Тематическая секция. Зал «Шишка»	Криптография в микроэлектронике и аппаратный корень доверия Круглый стол. Зал «Еловый»	Перспективные исследования в области кибербезопасности Тематическая секция. Зал «Сосновый»
19:00 – 23:00	Ужин, вечерняя программа		

21 марта, пятница

09:00 – 11:00	Завтрак
12:00	Трансфер из отеля «Солнечный Park Hotel & SPA» до станции метро «Ховрино»



Деловая программа

19 марта, среда

<p>09:00 – 10:00</p>	<p>Регистрация участников конференции</p>
<p>10:00 – 12:00 Зал «Шишка»</p>	<p>Открытие конференции «РусКрипто’2025»</p> <p>Пленарное заседание, посвященное официальному открытию ежегодной конференции «РусКрипто’2025». Приветственные слова.</p> <p>Доклады:</p> <p>Огонь, вода и медные трубы: 10 лет стандартизации «Кузнечика» Иванов Алексей Владимирович, НКЦКИ Маршалко Григорий Борисович, ТК 26 Матюхин Дмитрий Викторович, ТК 26 Шишкин Василий Алексеевич, НПК «Криптонит»</p> <p>Конфиденциальные вычисления и российская криптография Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор, КриптоПро</p> <p>Современная информационная безопасность криптографических средств Баранов Александр Павлович, д.ф.-м.н., действительный член Академии криптографии РФ</p> <p>Квантово-устойчивые криптографические решения Федоров Алексей Константинович, вице-президент, Газпромбанк</p>
<p>12:30 – 14:00 Зал «Шишка»</p>	<p>Круглый стол «Российский рынок информационной безопасности: настоящее и будущее»</p> <p>Ведущий:</p> <p>Малинин Юрий Витальевич, директор, Ассоциация «РусКрипто»</p> <p>Эксперты:</p> <p>Петров Алексей Владимирович, ФСБ России Хасин Евгений Владимирович, ВРИО директора Департамента обеспечения кибербезопасности Минцифры РФ Кувшинников Дмитрий Игоревич, председатель комитета по информационной безопасности, АПКИТ Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор, КриптоПро Гусев Дмитрий Михайлович, к.т.н., первый заместитель генерального директора, ИнфоТеКС</p>
<p>12:30 – 14:00 Зал «Еловый»</p>	<p>Круглый стол «Конфиденциальные вычисления»</p> <p>Ведущие:</p> <p>Маршалко Григорий Борисович, ТК 26 Кяжин Сергей Николаевич, к.ф.-м.н., заместитель начальника отдела криптографических исследований, КриптоПро, доцент НИЯУ МИФИ</p> <p>Эксперты:</p> <p>Никифорова Лидия Олеговна, ведущий криптограф-исследователь, АНО «НТЦ ЦК», ведущий инженер-аналитик, КриптоПро Елистратов Андрей Алексеевич, к.ф.-м.н., Банк России Саттаров Виталий Джалолович, основатель, Блумтех Сатиров Юрий Константинович, архитектор ДЭГ, директор блока цифровизации избирательных процессов, Ростелеком Гребнев Сергей Владимирович, руководитель направления прикладных исследований, QApp</p>



12:30 – 14:00

Киноконцертный зал

Секция «HR в ИБ: поиск, мотивация, адаптация и развитие специалистов. Кадровые практики и современные технологии»

Ведущий:

Хайров Игорь Евгеньевич, к.т.н., доцент, заместитель директора, АИС

Доклады:

Практикоориентированная подготовка специалистов по защите информации. Взаимодействие образовательных организаций и работодателей

Белов Евгений Борисович, заместитель председателя в сфере информационной безопасности ФУМО ВО ИБ

Безопасность технологий с искусственным интеллектом: спекуляции, домыслы и прогнозы

Лось Владимир Павлович, Президент Ассоциации Защиты Информации

Как отличаются ожидания соискателей и работодателей в сфере ИБ?

Ковардакова Ольга Александровна, Директор по работе с персоналом Инфосистемы Джет

Панельная дискуссия в рамках сессии. Вопросы для обсуждения:

- Соотношение спроса и предложения в ИБ
- Роль образования и сертификаций
- Использование ИИ в подборе кадров
- Эффективные и работающие механизмы адаптации новых сотрудников
- Механизмы и инструменты мотивации и удержания сотрудников ИБ
- Работы с персоналом ИБ в стрессовых ситуациях
- Предотвращение выгорания

Эксперты:

Старостина Екатерина Вячеславовна, IThub, архитектор кафедры ИБИСА

Платонов Антон Борисович, директор компании HRB Software

Пилипенко Галина Васильевна, директор по комплексной безопасности, МТС Диджитал

Ткачева Оксана Сергеевна, независимый эксперт по организационному развитию и управлению персоналом в ИБ

Арефьева Елена Владимировна, директор по персоналу и административным вопросам, АО «Инфозащита»

Ковардакова Ольга Александровна, директор по работе с персоналом, Инфосистемы Джет

15:00 – 16:30

Зал «Шишка»

Секция «Решения, продукты и технологии»

Ведущие:

Поташников Александр Викторович, заместитель директора центра разработки, ИнфоТекС

Горелов Дмитрий Львович, управляющий партнер, Компания «Актив», директор Ассоциации «РусКрипто»

Доклады:

Использование смарт-карт для распределения квантово-защищенных ключей пользователям

Кузнецов Андрей Сергеевич, к.ф.-м.н., инженер-программист 1 категории отдела разработки встроенного ПО и СКЗИ, АО «НИИМЭ»

Клиентская аутентификация на шлюзе удаленного доступа. Проблемы, решения, опыт реализации

Никитков Александр Александрович, эксперт по сетевой безопасности, КриптоПро



	<p>Отраслевой технологический удостоверяющий центр. Типовое решение подключения к ЕСИА Пьянченко Андрей Андреевич, заместитель руководителя проектной дирекции, АНО «НТЦ ЦК»</p> <p>Аппаратный модуль безопасности центра аутентификации сети подвижной радиотелефонной связи с защитой ключей аутентификации на локальных мастер-ключах Емельянов Виктор Михайлович, к.ф.-м.н., руководитель направления, Системы практической безопасности Мареева Елена Владимировна, заместитель генерального директора по науке, Системы практической безопасности</p>
<p>15:00 – 16:30 Зал «Еловый»</p>	<p>Секция «Разработка, внедрение и эксплуатация средств криптографической защиты информации»</p> <p>Ведущий: Петров Алексей Владимирович, ФСБ России</p> <p>Доклады: Обзор изменений законодательства. Что ждёт нас в 2025 году Толстолицкая Анастасия Васильевна, ФСБ России</p> <p>Развитие «гражданской» криптографии. Выпуск обновлений мобильных приложений с встроенным СКЗИ: проблемы и частные решения Кондратенко Роман Сергеевич, старший системный аналитик Департамента развития технологий ЭП и ЭДО, РТ Лабс</p> <p>Встраивание и использование СКЗИ в решениях на базе интерпретируемых языков программирования Петров Алексей Владимирович, ФСБ России</p>
<p>15:00 – 16:30 Зал «Сосновый»</p>	<p>Секция «Искусственный интеллект в кибербезопасности: защита будущего или новые угрозы?»</p> <p>Ведущие: Зегжда Дмитрий Петрович, чл.-корр. РАН, директор Института кибербезопасности и защиты информации СПбПУ Петра Великого Полтавцева Мария Анатольевна, д.т.н., профессор, директор Высшей школы кибербезопасности СПбПУ Петра Великого</p> <p>Доклады: Противодействие развитию компьютерных атак в гетерогенной сетевой инфраструктуре на основе анализа графов Завадский Евгений Владимирович, Высшая школа кибербезопасности СПбПУ Петра Великого</p> <p>Интеллектуальная система адаптивной защиты от сетевых атак на основе реконфигурации сети Горецкий Илья Александрович, Высшая школа кибербезопасности СПбПУ Петра Великого</p> <p>Применение мультиагентных систем на базе больших языковых моделей в киберпсихологии Богина Василиса Михайловна, Высшая школа кибербезопасности СПбПУ Петра Великого</p> <p>Снижение объема испытаний при оценке уровня доверия к ПО на основе методов машинного обучения Грибков Никита Андреевич, Высшая школа кибербезопасности СПбПУ Петра Великого</p>



17:00 – 19:00

Киноконцертный зал

Секция «Защита данных»

Ведущий:

Качалин Игорь Федорович, генеральный директор, АНО «НТЦ ЦК»

Доклады:

О механизмах криптографической защиты данных публичных облачных хранилищ и перспективах стандартизации технических спецификаций к прикладным протоколам облачных хранилищ данных

Тихов Станислав Вячеславович, ведущий специалист, НТП «Криптософт»

Минаков Сергей Сергеевич, заместитель генерального директора, АНО «НТЦ ЦК»

Использование криптографических средств и методов в технологиях обезличивания персональных данных

Минаков Сергей Сергеевич, заместитель генерального директора АНО «НТЦ ЦК»

Клочко Юрий Борисович, генеральный директор, Дамаск цифровая безопасность

Буланов Андрей Владимирович, генеральный директор, Поисковый портал «Спутник»

Практические подходы к реализации актуальных требований по защите данных в автоматизированных системах

Сидак Алексей Александрович, генеральный директор, Центр безопасности информации

Лузин Виктор Петрович, директор департамента, Центр безопасности информации

Василенко Владимир Васильевич, заместитель генерального директора,

Центр безопасности информации

Сидак Дарья Алексеевна, инженер, Центр безопасности информации

Перспективные направления защиты информации в машине баз данных Tantor Xdata

Яценко Вадим Александрович, генеральный директор, Тантор Лабс

Технологии повышения конфиденциальности: возможные направления регулирования и стандартизации

Левава Ирина Юрьевна, директор по стратегическим проектам, Ассоциация больших данных

Дискуссия в рамках секции

Качалин Игорь Федорович, генеральный директор, АНО «НТЦ ЦК»

Сидак Алексей Александрович, генеральный директор, Центр безопасности информации

Левава Ирина Юрьевна, директор по стратегическим проектам, Ассоциация больших данных

Ярунин Александр Андреевич, начальник управления криптографии, X5 Group

17:00 – 19:00

Зал «Еловый»

Секция «Криптография и криптоанализ». Часть 1

Ведущие:

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

Алексеев Евгений Константинович, к.ф.-м.н., АНО «НТЦ ЦК»

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

Доклады:

Обзор результатов анализа хэш-функции ГОСТ Р 34.11-2012. 10 лет спустя

Матюхин Дмитрий Викторович, ТК 26

Маршалко Григорий Борисович, ТК 26

Соловник Дмитрий Александрович, ТК 26

Фомин Денис Бониславович, ТК 26

Подход к автоматизации дифференциального метода анализа

Тавокин Михаил Александрович, специалист, СФБ Лаб

Бондакова Ольга Сергеевна, старший преподаватель, РТУ МИРЭА



	<p>Концепции построения малоресурсных блочных шифрсистем: так ли нужны максимально рассеивающие линейные преобразования? Давыдов Степан Андреевич, старший специалист-исследователь лаборатории криптографии, НПК «Криптонит» Чичаева Анастасия Александровна, специалист-исследователь лаборатории криптографии, НПК «Криптонит» Шкуратов Юрий Дмитриевич, младший специалист-исследователь лаборатории криптографии, НПК «Криптонит»</p> <p>Об одном обобщении FLEX-подобных алгоритмов блочного шифрования и его алгебраических свойствах Смирнов Антон Михайлович, НИЯУ МИФИ</p> <p>Алгоритмы аутентифицированного шифрования на основе отечественных криптографических примитивов в сценариях с вычислительными ограничениями Буинов Борис Юрьевич, инженер-программист, Компания «Актив» Васин Антон Романович, к.ф.-м.н., старший аналитик-криптограф, Компания «Актив» Скоробогатова Марина Андреевна, старший аналитик, Компания «Актив»</p> <p>Об одном подходе к построению режимов работы блочных шифров для защиты информации на системных носителях с блочно-ориентированной структурой Коренева Алиса Михайловна, к.ф.-м.н., начальник отдела криптографического анализа, Код Безопасности, доцент кафедры ИБ, Финансовый университет при Правительстве РФ Фирсов Георгий Валентинович, руководитель группы разработки, Код Безопасности, аспирант кафедры «Криптология и кибербезопасность», НИЯУ «МИФИ»</p>
<p>17:00 – 19:00 Зал «Сосновый»</p>	<p>Секция «Криптографические решения для киберфизических систем»</p> <p>Ведущая: Сорокина Марина Викторовна, руководитель направления отдела развития продуктов, ИнфоТеКС</p> <p>Доклады:</p> <p>Встраиваемые криптографические средства в промышленных системах Сорокина Марина Викторовна, руководитель направления отдела развития продуктов, ИнфоТеКС</p> <p>Проблема распределения криптографических ключей в Интернете вещей Мытник Константин Яковлевич, начальник отдела разработки встроенного ПО и СКЗИ, АО «НИИМЭ»</p> <p>О модификации протокола OSDP с использованием российских криптографических алгоритмов Архипов Максим Дмитриевич, инженер-аналитик, Компания «Актив»</p> <p>Расширение системы команд RISC-V для ускорения алгоритмов ГОСТ-криптографии Матюков Андрей Викторович, руководитель рабочей группы, Альянс RISC-V</p> <p>Развитие рынка защиты киберфизических систем. Взгляд из будущего Колесников Андрей Вячеславович, Ассоциация интернета вещей Лазарев Алексей Станиславович, Компания «Актив», Ассоциация интернета вещей</p>



20 марта, четверг

<p>10:00 – 11:30 Зал «Шишка»</p>	<p>Секция «Технологии электронной подписи»</p> <p>Ведущие:</p> <p>Малинин Юрий Витальевич, президент, Ассоциация «РОСЭУ» Смирнов Павел Владимирович, к.т.н., директор по развитию, КриптоПро, эксперт РОСЭУ</p> <p>Доклады:</p> <p>Эволюция технологии средств электронной подписи и способов её применения Маслов Юрий Геннадьевич, коммерческий директор, КриптоПро, эксперт ассоциации «РОСЭУ»</p> <p>Электронная подпись и МЧД для бизнеса Новиков Федор Вадимович, начальник управления электронного документооборота, ФНС России</p> <p>Опыт эксплуатации технологии мобильной электронной подписи Верестникова Дарья Дмитриевна, генеральный директор, STCrypt Дегтярев Алексей Валерьевич, Т-Банк</p> <p>Правильная проверка электронной подписи, в том числе иностранной и архивной Кирюшкин Сергей Анатольевич, советник — начальник удостоверяющего центра, Газинформсервис</p>
<p>10:00 – 11:30 Зал «Еловый»</p>	<p>Секция «Криптография и криптоанализ». Часть 2</p> <p>Ведущие:</p> <p>Матюхин Дмитрий Викторович, к.ф.-м.н., ФСБ России Алексеев Евгений Константинович, к.ф.-м.н., АНО «НТЦ ЦК» Жуков Алексей Евгеньевич, к.ф.-м.н., МГТУ им. Баумана, Ассоциация «РусКрипто»</p> <p>Доклады:</p> <p>Сложность решения систем полиномиальных уравнений с помощью квантового алгоритма Гровера на примере блочного алгоритма шифрования КБ-256 Поляков Михаил Вадимович, Код Безопасности, МГТУ им. Баумана Коренева Алиса Михайловна, к.ф.-м.н., начальник отдела криптографического анализа, Код Безопасности, доцент кафедры ИБ, Финансовый университет при Правительстве РФ</p> <p>О применении квантово-вычислительных методов в некоторых атаках на алгоритм «Магма» Щербаченко Андрей Александрович, специалист, СФБ Лаб</p> <p>Вариационные квантовые алгоритмы как перспективный метод универсального криптоанализа Манько Софья Дмитриевна, Центр научных исследований и перспективных разработок, ИнфоТеКС Моисеевский Алексей Денисович, Центр научных исследований и перспективных разработок, ИнфоТеКС, Центр квантовых технологий МГУ имени М.В. Ломоносова</p> <p>Пример применения квантового алгоритма Шора для решения задачи дискретного логарифмирования в группе точек эллиптической кривой над конечным простым полем Денисенко Денис Витальевич, Академия криптографии РФ, МГТУ им. Н.Э. Баумана</p> <p>Об особенностях квантовых генераторов случайных чисел Науменко Антон Павлович, заместитель начальника отдела, СФБ Лаб Арбеков Игорь Михайлович, к.ф.-м.н., главный специалист, СФБ Лаб Кирюхин Виталий Александрович, главный специалист, СФБ Лаб Щербаченко Андрей Александрович, ведущий специалист, СФБ Лаб</p>



<p>10:00 – 11:30 Зал «Сосновый»</p>	<p>Круглый стол «Криптография в NGFW»</p> <p>Ведущие:</p> <p>Батранков Денис Владимирович, эксперт по NGFW Веселов Александр Геннадьевич, автор и ведущий телеграм-канала ГОСТ VPN</p> <p>Эксперты:</p> <p>Смирнов Николай Валерьевич, директор по продуктам, ИнфоТеКС Коростелёв Павел Владимирович, руководитель отдела продвижения продуктов, Код Безопасности Петренко Сергей Анатольевич, директор по работе с госструктурами, UserGate Сахаров Павел Владимирович, заместитель технического директора, Positive Technologies</p>
<p>12:00 – 14:00 Зал «Шишка»</p>	<p>Секция «Информационная безопасность и криптография в банковской сфере». Часть 1</p> <p>Ведущие:</p> <p>Елистратов Андрей Алексеевич, к.ф.-м.н., Банк России Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор, КриптоПро</p> <p>Доклады:</p> <p>Новая редакция требований к HSM, POS, банкоматам и картам Зинюк Борис Федорович, Академия криптографии РФ</p> <p>Межбанковский биоэквайринг: технология и безопасность Литвинов Игорь Олегович, Банк России Лысенко Сергей Леонидович, НСПК</p> <p>Безопасность OpenAPI: когда «открытый» не значит «уязвимый» Стародубов Константин Владимирович, к.т.н., Банк России Грунтович Михаил Михайлович, к.ф.-м.н., руководитель обособленного подразделения, ИнфоТеКС</p> <p>Криптография в банковских цифровых каналах как способ борьбы с мошенничеством Верестникова Дарья Дмитриевна, генеральный директор, STCrypt</p> <p>Отечественная криптография в мобильном приложении банка будущего Агеев Святослав Витальевич, директор департамента государственных проектов, Т-Банк</p>
<p>12:00 – 14:00 Зал «Еловый»</p>	<p>Секция «Криптография и криптоанализ». Часть 3</p> <p>Ведущие:</p> <p>Матюхин Дмитрий Викторович, к.ф.-м.н., ФСБ России Алексеев Евгений Константинович, к.ф.-м.н., АНО «НТЦ ЦК» Жуков Алексей Евгеньевич, к.ф.-м.н., МГТУ им. Баумана, Ассоциация «РусКрипто»</p> <p>Доклады:</p> <p>Методы защиты от атак по побочным каналам аппаратной реализации схем постквантовой подписи, построенных на основе протокола идентификации Штерна Смирнов Дмитрий Константинович, МГУ имени М.В. Ломоносова, ИнфоТеКС Чижов Иван Владимирович, к.ф.-м.н., доцент, МГУ имени М.В. Ломоносова, Федеральный исследовательский центр «Информатика и управление» РАН, Криптонит</p>



	<p>Гиперикум 2.0: проект квантово-устойчивой схемы цифровой подписи для стандартизации в России Турченко Олег Юрьевич, к.т.н., старший исследователь, QApp Гребнев Сергей Владимирович, руководитель группы прикладных исследований, QApp</p> <p>Схема электронной подписи на решетках «Облепиха» Леевик Антон Георгиевич, криптограф-исследователь, QApp Малыгина Екатерина Сергеевна, к.ф.-м.н., криптограф-исследователь, QApp Мельничук Евгений Михайлович, криптограф-исследователь, QApp Набоков Денис Алексеевич, криптограф-исследователь, QApp</p> <p>Механизм инкапсуляции ключа на решетках «Земляника» Зеленецкий Алексей Сергеевич, старший исследователь, QApp, аспирант, МГТУ им. Баумана</p> <p>Гибридизация ключей — однократного хэширования достаточно Кирюхин Виталий Александрович, главный специалист, СФБ Лаб</p> <p>Способы интеграции квантовых ключей в протоколы IPsec, TLS 1.3 и IPQIR Бородин Михаил Алексеевич, старший исследователь, ИнфоТеКС, АНО «НТЦ ЦК»</p>
<p>12:00 –14:00 Зал «Сосновый»</p>	<p>Секция «Квантовые коммуникации и квантовая криптография»</p> <p>Ведущие: Корольков Андрей Вячеславович, Академия криптографии РФ Науменко Антон Павлович, СФБ Лаб, ИнфоТеКС</p> <p>Доклады:</p> <p>О подходах к снижению эксплуатационных издержек при использовании систем квантового распределения ключей с доверенными промежуточными узлами (ДПУ) Науменко Антон Павлович, СФБ Лаб, ИнфоТеКС</p> <p>Широкополосная рефлектометрия для анализа уязвимостей систем квантового распределения ключей в ближнем инфракрасном диапазоне Бондарь Клим Дмитриевич, СФБ Лаб</p> <p>Пользовательские приложения для сетей КРК Павлов Игорь Денисович, технический директор, QRate</p> <p>Квантово-безопасное федеративное глубокое обучение Воробей Сергей Сергеевич, заместитель начальника отдела лицензирования и сертификации, QRate</p> <p>Особенности проведения анализа безопасности квантово-криптографических систем выработки и распределения ключа Лохматов Роман Юрьевич, ведущий специалист, СФБ Лаб</p>



<p>15:00 –16:30 Зал «Шишка»</p>	<p>Дискуссионная панель «Банковский бизнес VS криптографическая отрасль»</p> <p>Ведущая: Желунова Екатерина Геннадиевна, Банк России</p> <p>Эксперты: Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор, КриптоПро Гусев Дмитрий Михайлович, к.т.н., первый заместитель генерального директора, ИнфоТеКС Маркосьянц Дмитрий Александрович, руководитель транзакционного бизнеса юридических лиц, Ozon банк Репин Максим Михайлович, заместитель директора Департамента информационной безопасности, РСХБ</p>
<p>15:00 –16:30 Зал «Еловый»</p>	<p>Секция «Криптография и криптоанализ». Часть 4</p> <p>Ведущие: Матюхин Дмитрий Викторович, к.ф.-м.н., ФСБ России Алексеев Евгений Константинович, к.ф.-м.н., АНО «НТЦ ЦК» Жуков Алексей Евгеньевич, к.ф.-м.н., МГТУ им. Баумана, Ассоциация «РусКрипто»</p> <p>Доклады:</p> <p>Об одной схеме динамической групповой подписи Утехина Мария Павловна, инженер-аналитик 2 категории, КриптоПро</p> <p>О скрытых возможностях отечественного варианта уравнения Эль-Гамала Гуселев Антон Михайлович, Академия криптографии РФ</p> <p>Мультипликативно и линейно связанные ключи подписи Бахарев Александр Олегович, младший специалист-исследователь лаборатории криптографии, НПК «Криптонит» Царегородцев Кирилл Денисович, инженер 1 категории лаборатории вычислительных методов, Механико-математический факультет МГУ имени М.В. Ломоносова</p> <p>Об одном подходе к оценке нагрузки на ключ для протоколов CRISP и IPIir Кирюхин Виталий Александрович, главный специалист, СФБ Лаб</p> <p>«Подводные камни» при обеспечении защиты в системах VoIP Ахметзянова Лилия Руслановна, к.ф.-м.н., заместитель начальника отдела криптографических исследований, КриптоПро, эксперт АНО «НТЦ ЦК»</p>
<p>15:00 –16:30 Зал «Сосновый»</p>	<p>Секция «Стандартизация и совместимость криптографических механизмов, продуктов и решений»</p> <p>Ведущий: Бондаренко Александр Иванович, Академия криптографии Российской Федерации, ТК 26</p> <p>Доклады:</p> <p>О некоторых особенностях применения межгосударственных стандартов, национальных стандартов, рекомендаций по стандартизации и технических спецификаций в СКЗИ Тыщенко Никита Сергеевич, ФСБ России</p>



	<p>Тестирование совместимости создаваемых СКЗИ различных производителей, использующих криптографические алгоритмы, утверждённые в качестве национальных стандартов Минаков Сергей Сергеевич, заместитель генерального директора, АНО «НТЦ ЦК»</p> <p>Предложения по модификации протокола APDU с целью возможной реализации ряда постквантовых алгоритмов электронной подписи в смарт-картах Панасенко Сергей Петрович, к.т.н., директор по научной работе, Компания «Актив»</p> <p>Возможности использования российских криптографических стандартов в протоколах динамической маршрутизации телекоммуникационного оборудования отечественных производителей Додонов Александр Сергеевич, начальник управления, НПП Цифровые решения»</p> <p>Исследование специальных видов постквантовых электронных подписей и проблем их реализации Гребнев Сергей Владимирович, руководитель направления прикладных исследований, QApp Давыдов Вадим Валерьевич, к.т.н., криптограф-исследователь, QApp Полтавская Ирина Вячеславовна, коммерческий директор, QApp Курочкин Алексей Вячеславович, руководитель направления, Sberbank of Russia, Blockchain Laboratory</p>
<p>17:00 –19:00 Зал «Шишка»</p>	<p>Секция «Информационная безопасность и криптография в банковской сфере». Часть 2</p> <p>Ведущие: Елистратов Андрей Алексеевич, к.ф.-м.н., Банк России Смышляев Станислав Витальевич, д.ф.-м.н., генеральный директор, КриптоПро</p> <p>Доклады:</p> <p>Обеспечение безопасности при подключении к ГИС ЕБС Семенов Евгений Николаевич, заместитель генерального директора, Центр биометрических технологий</p> <p>Что важно учесть при внедрении форматов архивного хранения подписанных документов? Опыт банка ВТБ Голубцова Алёна Сергеевна, директор проектов, ПАО «ВТБ» Ващенко Ольга Петровна, руководитель службы реализации проекта, Иннотех</p> <p>Цифровые удостоверения: управление персональными данными при аутентификации Попов Владимир Александрович, ПАО «Сбербанк»</p> <p>Криптография при работе с цифровыми активами Калихов Артем Владимирович, генеральный директор, Веб3 Технологии</p> <p>Межбанковский скоринг на основе технологий конфиденциальных вычислений Митрофанов Александр Александрович, к.т.н., директор по развитию бизнеса, Блумтех</p> <p>Возможность использования протокола SECUNDA для защищенной загрузки данных в процессе эмиссии платежных карт Грезина Софья Валерьевна, ведущий инженер-исследователь, ООО «СПБ» Герасимова Алла Геннадьевна, руководитель направления, ООО «СПБ»</p>



<p>17:00 –19:00 Зал «Еловый»</p>	<p>Круглый стол «Криптография в микроэлектронике и аппаратный корень доверия»</p> <p>Ведущие:</p> <p>Горелов Дмитрий Львович, управляющий партнер, Компания «Актив», директор Ассоциации «РусКрипто» Карантаев Владимир Геннадьевич, к.т.н., МЭИ, Альянс RISC-V</p> <p>Эксперты:</p> <p>Мытник Константин Яковлевич, начальник отдела разработки встроенного ПО и СКЗИ, АО «НИИМЭ» Миронкин Владимир Олегович, ФСБ России Решетов Андрей Борисович, директор по информационной безопасности, Аквариус Лебедев Александр Владимирович, НМ-Тех</p> <p>Доклад в рамках круглого стола:</p> <p>Теоретико-вероятностные модели физических генераторов случайных чисел</p> <p>Богданов Дмитрий Сергеевич, ФСБ России Миронкин Владимир Олегович, ФСБ России Логачев Александр Станиславович, Гознак</p>
<p>17:00 –19:00 Зал «Сосновый»</p>	<p>Секция «Перспективные исследования в области кибербезопасности»</p> <p>Ведущий:</p> <p>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</p> <p>Доклады:</p> <p>Большие языковые модели для кибербезопасности: текущие решения и направления развития</p> <p>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</p> <p>Технологии противодействия ранее неизвестным квантовым киберугрозам</p> <p>Петренко Сергей Анатольевич, д.т.н., профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия</p> <p>Предупреждение инсайдерских угроз на основе выявления аномального поведения пользователей</p> <p>Шелухин Олег Иванович, д.т.н., профессор, заведующий кафедрой ИБ, МТУСИ Осин Андрей Владимирович, к.т.н., доцент, доцент кафедры ИБ, МТУСИ</p> <p>Оценка эффективности систем управления информационной безопасностью: проблемы и механизмы их решения</p> <p>Минзов Анатолий Степанович, д.т.н, профессор кафедры БИТ, МЭИ Невский Александр Юрьевич, к.т.н, доцент, заведующий кафедрой БИТ, МЭИ Баронов Олег Рюрикович, к.т.н, доцент кафедры БИТ, МЭИ</p>



Определение аномальных сетевых состояний на основе измерений односторонней сетевой задержки

Сагатов Евгений Собирович, к.т.н., доцент, с.н.с, Самарский национальный исследовательский университет им. академика С.П. Королева

Черныш Дмитрий Петрович, старший преподаватель кафедры КИМ, Крымский федеральный университет им. В.И. Вернадского

Сухов Андрей Михайлович, д.т.н., профессор, Самарский национальный исследовательский университет им. академика С.П. Королева

Оценка декларируемых показателей моделей машинного обучения в средствах защиты информации на объектах КИИ

Виткова Лидия Андреевна, к.т.н., Газинформсервис, СПб ФИЦ РАН