Ассоциация РусКрипто

ОРГАНИЗАТОРЫ

АИС

РУСКРИПТО'2020

XXII МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ПРОГРАММА

17-20 МАРТА 2020 Г.

БЛАГОДАРИМ СПОНСОРОВ И ПАРТНЕРОВ ЗА ОКАЗАННУЮ ПОДДЕРЖКУ!

ЗОЛОТОЙ ПАРТНЕР

КРИПТОПРО
ключевое слово в защите информации

СЕРЕБРЯНЫЕ ПАРТНЕРЫ

Компания АКТИВ

infotecs®

БРОНЗОВЫЕ ПАРТНЕРЫ

КОД БЕЗОПАСНОСТИ

КРИПТОНИТ

ОФИЦИАЛЬНЫЙ ПАРТНЕР

ФАКТОР-ТС

СТРАТЕГИЧЕСКИЙ ПАРТНЕР

Ростелеком
Солар

НАУЧНЫЙ ПАРТНЕР

НЕОБИТ

ПАРТНЕРЫ КОНФЕРЕНЦИИ

АПКИТ

АССОЦИАЦИЯ РОСЭУ

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

ФГУП "НПП "Гамма"
Искусство безопасности

s•terra

STAFF-COP

ФИНТЕХ АССОЦИАЦИЯ

НИИ ВОСХОД

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

BIS JOURNAL

Единый портал Электронной подписи

Б.О

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'2020» указано в программе.

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

18 марта в 08:00 утра трансфер метро Войковская - отель «Солнечный Park Hotel & SPA»

18 марта в 20:00 вечера трансфер отель «Солнечный Park Hotel & SPA» - метро Войковская

19 марта в 08:00 утра трансфер метро Войковская - отель «Солнечный Park Hotel & SPA»

19 марта в 20:00 вечера трансфер отель «Солнечный Park Hotel & SPA» - метро Войковская

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

20 марта в 12:15 трансфер отель «Солнечный Park Hotel & SPA» - метро Войковская
Подача автобусов в 12:00 у ворот отеля.

Внимание! *Автобусы с табличкой «РусКрипто'2020» отправятся ровно в 12:15. Просьба заранее сдать номера и не опаздывать.*

АДРЕС ОТЕЛЯ «СОЛНЕЧНЫЙ PARK HOTEL & SPA»

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

Расчетный час:
Заезд - 17 марта с 16:00
Выезд - 20 марта до 12:00

18 и 19 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»

ОБЩАЯ ИНФОРМАЦИЯ ДЛЯ УЧАСТНИКОВ

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

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

- Получить закрывающие документы вы сможете на стойке регистрации 18-19 марта

ОБСЛУЖИВАНИЕ В ОТЕЛЕ ПО СИСТЕМЕ «ALL INCLUSIVE»:

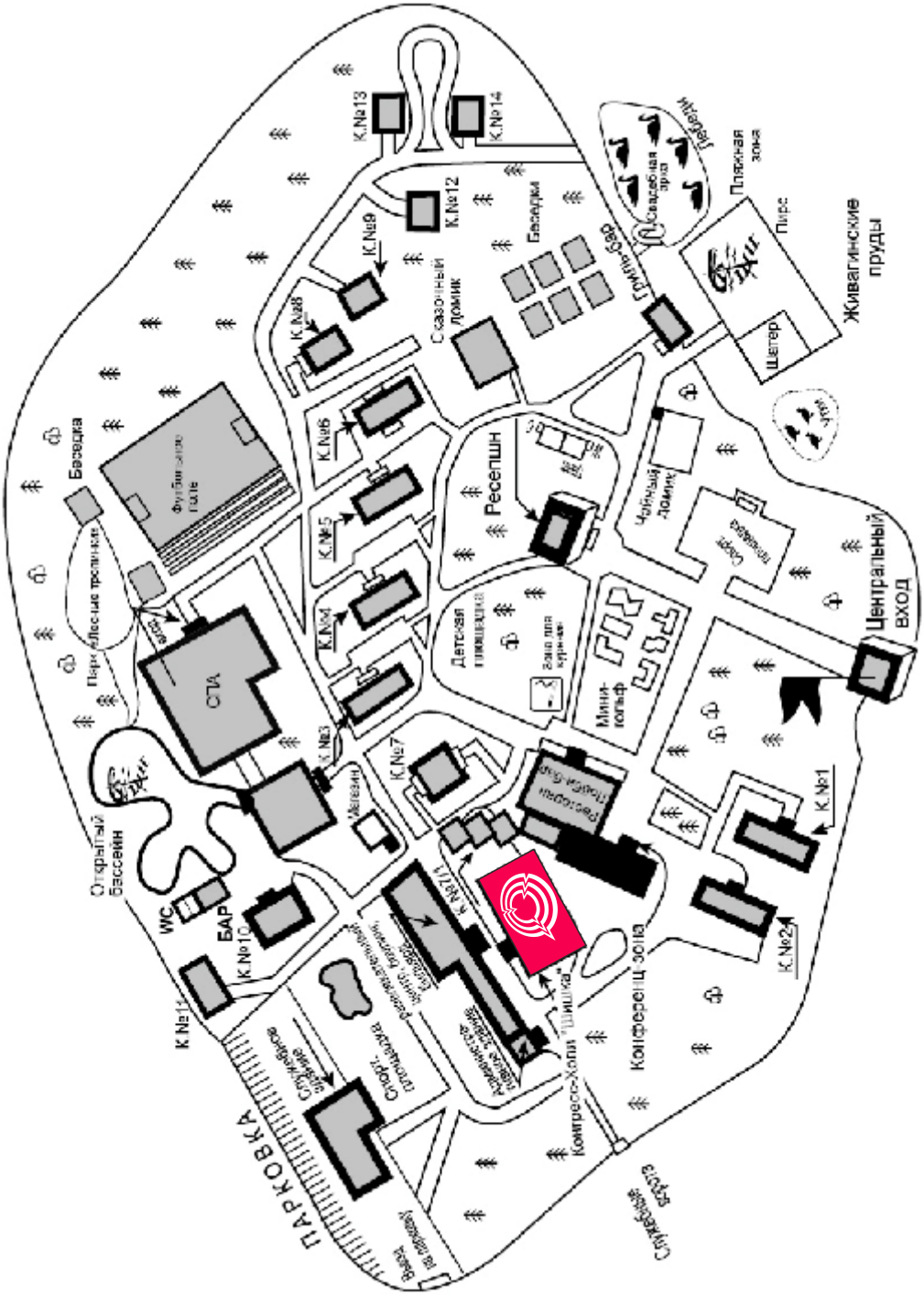
- расширенный шведский стол: завтрак (08:00-11:00), обед (13:00-16:00), ужин (19:00-23:00);
- в течение всего дня с 8-00 до 23-00 кофе, чай, выпечка, мороженое, соки, лимонады, разливное пиво, алкогольные напитки;
- бильярд, боулинг, пинг-понг;
- посещение термальной зоны SPA-комплекса (10 бассейнов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

ДОПОЛНИТЕЛЬНЫЙ СЕРВИС (ОПЛАЧИВАЕТСЯ ДОПОЛНИТЕЛЬНО):

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

18 и 19 марта по всем организационным вопросам
просьба обращаться к нашим менеджерам
на стойке регистрации в конференц-холле «Шишка»

КАРТА ОТЕЛЯ


Ресепшн
Центральный вход
Живаганские пруды
Открытый Бассейн
СПА
Конференц зона
Компресс-Холл "Шишка"
ПАРКОВКА
Беседка
Футбольное поле
Детская площадка
Мини-гольф
Пляжная зона
Шатер
Пирс
Сезонный домик
Беседки
К.№1
К.№3
К.№4
К.№5
К.№6
К.№7
К.№8
К.№9
К.№10
К.№11
К.№12
К.№13
К.№14
К.№24
WC
БАР

17 МАРТА, ВТОРНИК. ДЕНЬ ЗАЕЗДА

15:00 – 16:30	Трансфер: метро Войковская – отель «Солнечный Park Hotel & SPA» Заезд и регистрация участников, проживающих в отеле
17:00 – 18:30	Соревнования в СПА-комплексе (плавание, сквош, армрестлинг)
17:00 – 19:00	Спортивные турниры в развлекательном комплексе (бильярд, настольный теннис, боулинг)
20:00 – 22:00	Фестиваль крафтового пива «CryptoBeerFest». Награждение участников турниров. Лобби ресторанного комплекса, 1 этаж

18 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

09:00 – 10:00	Регистрация участников	
10:00 – 12:30	**Официальное открытие конференции. Пленарное заседание** *Зал «Шишка», 2 этаж* *10 стр.*	
12:30 – 12:50	Кофе-брейк	
12:50 – 14:30	**Секция «Квалифицированная электронная подпись»** Ведущие: • Баранов А.П., Академия криптографии РФ • Малинин Ю.В., Ассоциация «РОСЭУ» *Зал «Шишка»* *11 стр.*	**Секция «Инженерно-технические и правовые аспекты цифровой криминалистики и судебной экспертизы»** Ведущие: • Яковлев А.Н., ФГБУ «ЦЭКИ» • Чиликов А.А., МГТУ им. Баумана *Зал «Еловый»* *11 стр.*
14:30 – 15:30	Обед	
15:30 – 17:00	**Секция «Криптография и информационная безопасность в банковской сфере»** Ведущий: · Простов В.М., ФСБ России *Зал «Шишка»* *13 стр.*	**Круглый стол «Тонкости российского маркетинга информационной безопасности»** *Зал «Еловый»* *14 стр.*
17:00 – 17:30	Кофе-брейк	
17:30 – 19:30	**Секция «Секреты, ключи, сертификаты и идентификационная информация в современных ИТ-инфраструктурах»** Ведущий: · **Качалин А.И.,** Сбербанк *Зал «Сосновый»* *14 стр.*	**Секция «Криптография и криптоанализ», 1 часть** Ведущие: · Матюхин Д.В., ФСБ России · Попов В.О., КриптоПро · Жуков А.Е., МГТУ им. Баумана *Зал «Еловый»* *15 стр.*
19:30 – 20:00	Ужин	
20:00 – 23:00	**Торжественное открытие «РусКрипто'2020».** Зал «Шишка», 2 этаж	

19 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 10:00	Крипто-завтрак		
10:00 – 11:40	**Секция «Криптография в энергетическом секторе»** Ведущие: · Батяев С.В., Россети · Бондаренко А.И., ТК26 *Зал «Шишка»* *17 стр.*	**Секция «Криптография и криптоанализ», 2 часть** Ведущие: · Матюхин Д.В., ФСБ России · Попов В.О., КриптоПро · Жуков А.Е., МГТУ им. Баумана *Зал «Еловый»* *18 стр.*	
11:40 – 12:00	Кофе-брейк		
12:00 – 13:00	**Секция «Криптография на транспорте и в промышленности»** Ведущие: · Ткаченко Е.И., Министерство транспорта РФ · Бирман А.А. ЗащитаИнфоТранс *Зал «Шишка»* *19 стр.*	**Секция «Криптография и криптоанализ», 3 часть** Ведущие: · Матюхин Д.В., ФСБ России · Попов В.О., КриптоПро · Жуков А.Е., МГТУ им. Баумана *Зал «Еловый»* *19 стр.*	
13:00 – 13:20	Кофе-брейк		
13:20 – 14:30	**Секция «Информационная безопасность и криптография в государственных проектах»** Ведущие: · Тютрюмов А.А., Минкомсвязь России · Пьянченко А.А., НИИ «Восход» · Горелов Д.Л. компания «Актив» *Зал «Шишка»* *20 стр.*	**Секция «Системы квантового распределения ключей и квантовые коммуникации»** Ведущий: · Уривский А.В., ИнфоТеКС *Зал «Еловый»* *21 стр.*	
14:30 – 15:30	Обед		
15:30 – 17:00	**Круглый стол «Информационная безопасность Интернета вещей»** Ведущий: · Елисеев И.Ю., АИС *Зал «Шишка»* *22 стр.*	**Секция «Технологии распределенного реестра»** Ведущие: · Шумский Л.С., ФинТех · Конкин А.Ю., ФитТех *Зал «Еловый»* *23 стр.*	**Секция «Интеллектуальные методы обеспечения кибербезопасности промышленных систем»** Ведущие: · Зегжда Д.П., СПбПУ ИБКС · Москвин Д.А., НеоБИТ *Зал «Сосновый»* *23 стр.*
17:00 – 17:30	Кофе-брейк		

17:30 – 19:30	**Секция «Российский вектор развития безопасной радиочастотной идентификации (RFID)»** Ведущий: · Хачатуров В.М., Криптонит *Зал «Шишка»* *25 стр.*	**Секция «Перспективные исследования в области кибербезопасности»** Ведущий: · Котенко И.В., СПИИРАН *Зал «Еловый»* *26 стр.*	**Секция «Доклады студентов и аспирантов»** Ведущая: · Пудовкина М.А., МГТУ им. Баумана, ассоциация «РусКрипто» *Зал «Сосновый»* *27 стр.*
19:30 – 20:00	Ужин		
20:00	Караоке Баттл *Чайный домик*		
20:00 – 23:00	Интеллектуальная игра Крипто Quiz с Алексеем Лукацким и другие развлекательные мероприятия *Зал «Шишка», 2 этаж*		

20 МАРТА, ПЯТНИЦА. ДЕНЬ ОТЪЕЗДА

09:00 – 11:00	Завтрак
12:15	Трансфер отель «Солнечный Park Hotel & SPA» – м. Войковская

В рамках конференции «РусКрипто'2020» Академия Информационных Систем предлагает участникам пройти **бесплатное обучение (18-19 марта).**
Регистрация и начало обучения – 18 марта в 12.50, после Пленарного заседания в залах «Марс» и «Нептун». При прохождении итоговой аттестации участнику выдается **удостоверение о повышении квалификации.**

18 МАРТА, СРЕДА

12:50 – 14:30	**Нормативное правовое регулирование в области ИБ** Ведущий: Ковалев А.Н. *Зал «Нептун»*	**Построение процесса в DevSecOps организации** Ведущий: Зюзин М.А. *Зал «Марс»*
14:30 – 15:30	Обед	
15:30 – 17:00	**Нормативное правовое регулирование в области ИБ (продолжение)** Ведущий: Ковалев А.Н. *Зал «Нептун»*	**Построение процесса в DevSecOps организации (продолжение)** Ведущий: Зюзин М.А. *Зал «Марс»*

19 МАРТА, ЧЕТВЕРГ

10:00 – 12:30	**Нормативное правовое регулирование в области ИБ (продолжение)** Ведущий: Ковалев А.Н. *Зал «Нептун»*	**Построение процесса в DevSecOps организации (продолжение)** Ведущий: Зюзин М.А. *Зал «Марс»*
12:30 – 12:50	Кофе-брейк	
12:50 – 14:30	**Нормативное правовое регулирование в области ИБ (продолжение)** Ведущий: Ковалев А.Н. *Зал «Нептун»*	**Построение процесса в DevSecOps организации (продолжение)** Ведущий: Зюзин М.А. *Зал «Марс»*
14:30 – 15:30	Обед	
15:30 – 17:00	**Мастер-класс. Код Безопасности** **Особенности обеспечения информационной безопасности в корпоративных информационных системах** *По окончании выдается Сертификат о прохождении мастер-класса* *Зал «Марс»*	

20 МАРТА, ПЯТНИЦА

10:00 – 11:30	**Нормативное правовое регулирование в области ИБ** Ведущий: Ковалев А.Н. *Зал «Нептун»*	**Построение процесса в DevSecOps организации** Ведущий: Зюзин М.А. *Зал «Марс»*

ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

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

Официальное открытие конференции.

Приветственные слова
- **Шойтов Александр Михайлович,** ФСБ России
- **Бокова Людмила Николаевна,** Статс-секретарь - заместитель министра цифрового развития и массовых коммуникаций РФ
- **Бражко Вячеслав Сергеевич,** начальник управления режима секретности и безопасности информации, Федеральное казначейство

Вопросы криптографической защиты информации в Интернете вещей и индустриальных системах
Матюхин Дмитрий Викторович, *ФСБ России*

О деятельности Академии криптографии Российской Федерации в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»
Бондаренко Александр Иванович*, Академия криптографии Российской Федерации*

Криптографические системы и внутренний нарушитель
Баранов Александр Павлович*, д.ф-м.н., Академия криптографии Российской Федерации*
Применение криптографических методов защиты информации позволяет вполне успешно противостоять внешнему нарушителю. Иначе обстоит дело с защитой от внутреннего нарушителя, и это становится все более актуальной проблемой. Рассматривается адекватность имеющихся средств обеспечения информационной безопасности, построенных на основе криптосистем к современным запросам применения компьютерных технологий. Ставится задача стыковки технологий защиты программного обеспечения и криптографических функций, относящихся к сферам полномочий разных регуляторов, в целях достижения реальной защищенности информации от деструктивных действий внутреннего нарушителя. Формулируются технические задачи, решение которых позволит, по мнению докладчика, устранить ряд имеющихся проблем.

Настоящее и будущее криптопротоколов в сети Интернет
Смышляев Станислав Витальевич*, к.ф.-м.н., заместитель генерального директора, КриптоПро*
В докладе будут освещены наиболее значимые тенденции в области синтеза и анализа основных криптопротоколов в сети Интернет, формируемые на основных конференциях, встречах рабочих групп и комитетов, – в частности, с участием экспертов ТК 26. Также будет рассказано о достижениях, текущем состоянии и перспективах поддержки российских криптографических алгоритмов в протоколах сети Интернет, в том числе и в самых современных версиях.

Криптографические алгоритмы в КНР: разработка и применение
Zhenhai Huang, *Vice General Manager, China IWNCOMM Co., Ltd. (онлайн участие)*
История и текущее состояние процессов разработки криптографических алгоритмов в Китайской Народной Республике. Области применения криптографических алгоритмов в КНР, в том числе в сфере индустриальных систем. Обзор работ экспертов из КНР в области стандартизации, как в части международного признания китайских алгоритмов, так и в целом в части влияния на политики применения криптографических алгоритмов. А в завершение доклада будет рассказано об основных планах специалистов из КНР в сфере криптографии на будущее .
(Эксперт примет участие в программе дистанционно)

12:50 – 14:30 Секция «Квалифицированная электронная подпись»

Зал «Шишка»

Изменения в Федеральный закон «Об электронной подписи» заметно повлияют и на технические, и на организационные аспекты применения квалифицированной электронной подписи в нашей стране. Эксперты обсудят возможные сценарии развития событий, новые возможности и риски, дадут свои рекомендации операторам информационных систем, использующих электронную подпись. В работе секции примут участие представители Министерства цифрового развития, связи и массовых коммуникаций, ФСБ России, Федеральной налоговой службы, Федерального казначейства и Банка России.

Ведущие:

- **Баранов Александр Павлович,** д.ф-м.н., Академия криптографии Российской Федерации
- **Малинин Юрий Витальевич,** президент Ассоциации РОСЭУ

Участники:

- **Аристархов Иван Владимирович,** ФСБ России (по согласованию)
- Представитель Министерства цифрового развития и массовых коммуникаций РФ
- **Матвеева Татьяна Владимировна**, начальник Управления информационных технологий ФНС России (по согласованию)
- **Нагдаев Артем Юрьевич**, заместитель начальника Управления режима секретности и безопасности информации, Федеральное казначейство
- **Лабуцкая Анастасия Сергеевна,** Ассоциация РОСЭУ, эксперт ТРГ «Цифровая среда доверия» АНО «Цифровая экономика»

Реализация Федеральным казначейством функций удостоверяющего центра для организаций государственного сектора
Нагдаев Артем Юрьевич, *заместитель начальника Управления режима секретности и безопасности информации, Федеральное казначейство*

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

Зал «Еловый»

Задачи, стоящие перед экспертами-криминалистами, постоянно усложняются и требуют новых профессиональных навыков и новых инструментов. В рамках секции ведущие эксперты-практики и разработчики криминалистического инструментария поделятся своим опытом, а также расскажут о правовых и практических аспектах цифровой криминалистики.

Ведущие:

- **Яковлев Алексей Николаевич,** к.ю.н., заместитель начальника Управления экспертизы результатов мероприятий по информатизации Департамента экспертиз ФГБУ «Центр экспертизы и координации информатизации»
- **Чиликов Алексей Анатольевич,** МГТУ им. Баумана, Passware

Экспертиза компонент информационных систем по 44-ФЗ
Филимонов Александр Александрович, *ФГБУ «Центр экспертизы и координации информатизации»*
Шухнин Михаил Николаевич, *ФГБУ «Центр экспертизы и координации информатизации»*

Выявление аномальных ситуаций на видеозаписях стационарных систем видеофиксации с применением искусственного интеллекта

Причко Илья Олегович, *эксперт КТЭ и ИАЭ, экспертно-криминалистический отдел СУ СК России по Иркутской области*

Афанасьев Александр Диомидович, *д.ф.-м.н., профессор, ФГБОУ ВО «Иркутский национальный исследовательский технический университет»*

Для органов следствия и дознания информация, которая содержится в видеозаписях систем видеонаблюдения, имеет большое, а в некоторых случаях – ключевое значение для раскрытия и расследования преступлений. Ее выделение из видеозаписей отягощено рядом факторов, таких как сложность обработки данных человеком или невозможность глубокого анализа происходящих событий. В докладе будет представлен подход к решению задачи поиска аномальных ситуаций, которые возникают в процессе подготовки, совершения или сокрытия преступления, а также будут рассмотрены основные методы минимизации неинформативных данных.

Об одном подходе к получению доступа к MacBook Pro с чипом T2 в рамках проведения криминалистической экспертизы

Хоруженко Георгий Игоревич, Passware

Одной из ключевых задач при проведении криминалистической экспертизы является получение доступа к защищенным данным. Долгое время для решения этой задачи применительно к компьютерам Apple достаточно было известными методами получить образ диска и перебрать пароль пользователя. Однако с появлением программно-аппаратных схем защиты с чипом T2 задача значительно усложнилась, в частности, на данный момент нет возможности перебирать пароль пользователя на машине с включенной системой FileVault2. В докладе предлагается альтернативный подход к получению доступа к защищенным данным при наличии резервной копии iPhone.

Особенности извлечения данных из Android Go устройств

Карондеев Андрей Михайлович*, специалист отдела исследований, Оксиджен Софтвер*

Android Go - это облегченная версия операционной системы Android, предназначенная для бюджетных смартфонов. Встроенные в нее приложения оптимизированы для работы на устройствах даже с самыми скромными техническими характеристиками. Тем не менее Android Go устройства должны соответствовать всем требованиям безопасности перечисленным в Android Compatibility Definition Document (Android CDD), включая шифрование пользовательских данных защищенным на аппаратном уровне ключом. Таким образом, если смотреть чисто со стороны операционной системы, то такие устройства должны обеспечивать достаточный уровень защищенности пользовательских данных. Однако многие бюджетные устройства содержат критические уязвимости на уровне железа, что делает механизмы защиты операционной системы Android частично или даже полностью неэффективными. В частности, в ряде случаев это позволяет извлечь пользовательские данные, чему и посвящен доклад.

Физическое извлечение данных из iOS устройств: новые возможности, уязвимости и ограничения.

Малышев Андрей*, компания Элкомсофт*

Физический доступ к мобильным устройствам – одна из важнейших областей мобильной криминалистики. Многие секреты, хранящиеся в iOS устройствах, невозможно извлечь другим способом. Рассказ об уязвимостях программной и аппаратной части, которые были открыты за последнее время, а также о новых подходах к извлечению данных.

15:30 – 17:00 Секция «Криптография и информационная безопасность в банковской сфере»

Зал «Шишка»

Использование средств криптографической защиты информации в организациях кредитно-финансовой сферы, для внутрикорпоративных информационных систем и для систем удаленного взаимодействия. Криптография в платежных системах. Защита каналов связи, защищенный документооборот. Стандарты и требования.

Ведущий: Простов Владимир Михайлович, ФСБ России

Требования к СКЗИ, используемым в национально значимых платежных системах

Простов Владимир Михайлович, *ФСБ России*

Доклад посвящен обзору требований, предъявляемым к средствам криптографической защиты информации, которые могут использоваться в национально значимых платежных системах Российской Федерации.

Применение отечественных средств криптографической защиты информации в рамках банковских технологий

Косякин Иван Валерьевич*, Главный инженер, Отдел информационной безопасности и киберустойчивости финансовых технологий, Департамент информационной безопасности Банка России.*

Современные банковские технологии немыслимы без использования стойкой криптографии. В каких сценариях и каких сферах возможен полный переход на российские сертифицированные СКЗИ? Каков должен быть долговременный план по переводу банковских информационных систем на российскую криптографию?

Каким требованиям должен соответствовать аппаратный модуль безопасности для систем платежных карт

Мареева Елена Владимировна, *заместитель директора по научно-техническим разработкам ООО «Системы практической безопасности»*

Шкоркина Елена Николаевна*, высшая школы кибербезопасности и защиты информации СПбПУ Петра Великого*

Сравнение требований PCI PTS HSM и требований к серверным компонентам платежных систем (HSM модулям), используемым при осуществлении переводов денежных средств, указанных в пункте 2.20 положения Банка России от 9 июня 2012 г. № 382-П.

Облачная подпись в банковском секторе

Левиев Дмитрий Олегович*, ООО «НПО «Спецремонт», МГТУ им.Н.Э.Баумана*

В рамках доклада рассматриваются риски интеграции систем Удостоверяющего центра и систем дистанционного банковского обслуживания. Рассматривается формирование требований к указанным системам и проблемы их реализации в текущем законодательстве Российской Федерации.

Опыт разработки СКЗИ с применением отечественных решений для удаленной биометрической идентификации клиента в кредитной организации

Улыбин Дмитрий Львович*, директор по спецпроектам проектного офиса «Цифровая идентичность» ПАО «Ростелеком»*

Как реализовать удаленную биометрическую идентификацию клиента без прерывания клиентского пути? Как при этом выполнить требования регуляторов к использованию отечественной криптографии для защиты канала связи? Что делать с контролем встраивания СКЗИ в каждом релизе приложения? В ходе доклада попытаемся ответить на эти и связанные вопросы.

15:30 – 17:00 Круглый стол «Тонкости российского маркетинга информационной безопасности»

Зал «Еловый»

Круглый стол, посвященный маркетингу информационной безопасности в целом и продвижению продуктов в частности. Мир стремительно меняется, подходы, которые раньше безотказно работали, уже не приносят результата. Как продвигать решения в области информационной безопасности? Как завоевывать доверие заказчиков? Где искать новых клиентов? Как доносить информацию о сложных продуктах? Как строить план развития? Можно ли сделать рыночный продукт из заказной разработки? Где кончается продажа и начинается платный консалтинг? Какие маркетинговые инструменты работают на российском рынке информационной безопасности? На эти и другие вопросы постараются ответить эксперты круглого стола.

Эксперты круглого стола:

- **Шабанов Илья Олегович,** основатель и генеральный директор Anti-Malware.ru
- **Голов Андрей Викторович,** генеральный директор Код безопасности
- **Горелов Дмитрий Львович,** управляющий партнер компании «Актив», директор ассоциации «РусКрипто»
- **Конусов Андрей Юрьевич,** генеральный директор Аванпост
- **Салманова Шахноза Алмазовна,** начальник отдела маркетинга и внедрения, Анкад

17:30 – 19:30 Секция «Секреты, ключи, сертификаты и идентификационная информация в современных ИТ-инфраструктурах»

Зал «Сосновый»

Жизненный цикл паролей, ключей и сертификатов в современных инфраструктурах (динамические/облачные инфраструктуры, интегрированные инфраструктуры, сервисы 3-х организаций и т.д). Ключи и пароли в циклах DevOps. Системы управления ключами и сертификатами. Требования, промышленные решения, международные стандарты.

Ведущий: Качалин Алексей Игоревич, исполнительный директор Центра Киберзащиты, Сбербанк

Контроль доступа к данным в облаке при помощи Key Management Service

Иванов Андрей Вячеславович, *руководитель подразделения, ООО «Яндекс.Облако»*

В докладе затрагиваются темы защиты пользовательских данных в Облаке, принципы организации единого центра по управлению криптографическими ключами (KMS - Key Management Service), конкретные схемы шифрования данных в сервисах платформы Яндекс.Облако.

Автоматизация выдачи сертификатов в платежной системе

Шумицкий Александр Владимирович*, начальник отдела, Управление безопасности АО «НСПК»*

Типы и назначение сертификатов, используемых в деятельности платежных систем. Выдача сертификатов – общие принципы и практика. Проблемы выдачи сертификатов и их решение с помощью автоматизированного сервиса. Обзор и особенности созданного АО «НСПК» продукта.

Эволюция систем управления идентификационной информацией

Лукацкий Алексей Викторович, *бизнес-консультант по ИБ*

Сегодня, когда идентифицировать и аутентифицировать надо не только пользователей, но и устройства, которые подключаются к внутренним и внешним ресурсам изнутри корпоративной сети или снаружи ее, когда проверка подлинности проходит не только на уровне ОС или сетевого устройства, но и на уровне приложений, собственных или чужих, внутренних или облачных, мы должны по-другому посмотреть на то, как должна быть реализована и внедрена система управления идентификационной информацией и предоставления доступа. Как эволюционировали системы идентификации и аутентификации и какие решения нового поколения сейчас доступны заказчикам?

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

Зал «Еловый»

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

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Попов Владимир Олегович**, Ассоциация «РусКрипто», КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

О реализации высокоскоростного аппаратного шифратора в HSM на базе ПЛИС

Истомин Александр Александрович, *советник генерального директора, ФГУП "НПП "Гамма", МГТУ им. Баумана*

Пьер Фийоль, *ENSTA-Bretagne*

Седрик Делоне, *ENSTA-Bretagne*

Эрик Фийоль, *профессор, ENSIBS Cybersecurity Department, ВШЭ*

В докладе представлен проект под названием «ALGIZ / АЛЬГИЗ», реализованный совместно с французскими учеными. Это проект по созданию прототипа устройства для высокоскоростного аппаратного шифрования по ГОСТ 34.12.2015, на базе ПЛИС.

Построение атаки на основе инвариантных подпространств для XSL-алгоритма блочного шифрования на основе 3D подхода

Коновалов Никита Алексеевич, *студент 2-го курса магистратуры, НИЯУ МИФИ*

Рассматривается способ построения атаки, основанной на существовании инвариантных подпространств линейного преобразования 3D алгоритмов блочного шифрования. Анализируется 64 - битный алгоритм CUBE. Описаны свойства его линейного и нелинейного преобразований, а также алгоритма развертывания ключа. Найдены инвариантные подпространства линейного преобразования, существование которых является потенциальной слабостью алгоритма CUBE. Описан класс потенциально слабых ключей, позволяющий провести атаку на редуцированный алгоритм CUBE, а также приведен алгоритм атаки.

О комбинации квантовых алгоритмов перечисления и поиска на примере квантового разностного метода

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

В докладе представлен анализ корректности применения комбинации квантовых алгоритмов перечисления и поиска в квантовом дифференциальном методе криптоанализа. Показано, что процедура квантового перечисления должна выполняться не один раз, как считалось ранее, а на каждой итерации квантового алгоритма поиска. При восстановлении раундовых ключей с помощью квантового дифференциального метода ускорение вычислений за счет квантового параллелизма отсутствует, так как использование квантового перечисления в качестве «подпрограммы» алгоритма поиска нивелирует квантовое ускорение.

Разработка нового симметричного алгоритма шифрования «QAMAL»

Алгазы Кунболат Тлеуханулы, *Институт информационных и вычислительных технологий КН МОН РК, г. Алматы, Республика Казахстан*

Предлагается алгоритм симметричного блочного шифрования «Qamal». Описаны алгоритм формирования раундовых ключей и криптографические преобразования, используемые при создании алгоритма «Qamal».

О групповых свойствах TH-обобщения алгоритма Фейстеля

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

В настоящее время предложены различные обобщения алгоритма Фейстеля. Они различаются длиной регистра сдвига, а также выбором номеров ячеек, от координат которых зависят функции усложнения. Частным случаем TH-обобщения алгоритма Фейстеля являются MARS-подобные алгоритмы Фейстеля. В работе описываются групповые свойства TH-обобщения алгоритма Фейстеля. Для группы, порожденной его частичными раундовыми функциями, получены условия транзитивности, примитивности и условия подобия подгруппе группы экспоненцирования.

Об одном подходе к построению кратно транзитивного множества блочных преобразований

***Чередник Игорь Владимирович**, МГУ имени М.В. Ломоносова*

Рассматривается конструкция семейства блочных преобразований, которая предполагает использование фиксированной бинарной функциональной сети при ключевом выборе бинарной операции. Исследуется вопрос о практическом построении классов блочных преобразований, обладающих свойством кратной транзитивности.

Об одной атаке на модель шифров гаммирования

***Бабаш Александр Владимирович.,** д.ф-м.н., профессор, НИУ ВШЭ, РЭУ им. Г.В. Плеханова*

В работе предложена атака на модель шифров гаммирования с расчетом трудоемкости и надежности.

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 11:40 **Секция «Криптография в энергетическом секторе»**
Зал «Шишка»

Секция, посвящённая вопросам применения криптографической защиты информации на предприятиях энергетического сектора

Ведущие:

- **Батяев Сергей Васильевич,** Начальник Управления информационной безопасности и аналитики Департамента обеспечения безопасности, Россети
- **Бондаренко Александр Иванович**, ТК26

О стандартизации цифровых технологий

Уткин Никита Александрович, *Председатель технического комитета по стандартизации «Кибер-физические системы» (ТК 194)*

Развитие цифровых технологий ставит новые требования и подходы к их регулированию. Современное регулирование цифровых технологий должно быть полноценным, адаптивным и способствовать их развитию. В этой связи значительно повышается роль нормативно-технического регулирования. Подобно тому, как цифровые технологии имеют сквозной характер, в сфере их регулирования сквозной характер имеют аспекты безопасности в широком смысле и криптографические вопросы в частности.

Практика применения встраиваемых средств защиты информации в электроэнергетике

Сорокина Марина Викторовна, *руководитель продуктового направления, ИнфоТеКС*

Презентация посвящена рассмотрению вопроса организации защиты информации на уровне конечных устройств в системах электроэнергетики. В современных реалиях все чаще говорят о переходе от защиты периметра к защите устройств, а также о концепции “security by design”. Автор прежде всего попытается разобраться, что это за веяния, возможно ли в принципе внедрить механизмы защиты, в том числе криптографические, в контроллер, и что уже сегодня можно делать в реальных системах. В конце доклада будут приведены несколько примеров использования встроенных механизмов защиты информации в конечных устройствах из собственной практики автора.

Реализация криптографии в протоколе связи для Интернета Вещей "NB-Fi"

Бакуменко Андрей Викторович*, Заместитель генерального директора, ВАВИОТ*

Ограничением для реализации шифрования в сетях Интернета вещей является только небольшой размер передаваемого пакета данных, в котором должны содержаться как полезная нагрузка, так и дополнительные данные для обеспечения конфиденциальности и целостности, а также ограничения по вычислительной мощности оконечных устройств. Кроме этого, особенностью работы протокола NB-Fi является отсутствие гарантии доставки пакетов данных сторонам информационного взаимодействия, вызванное физическими ограничениями среды передачи данных и малой мощность конечных устройств. Такое ограничение порождает необходимость осуществления дополнительных действий для синхронизации используемых сторонами ключей, для обеспечения их периодической смены. В докладе будет описана история развития протокола NB-Fi и основные подходы, которые позволили обеспечить в протоколе NB-Fi высокий уровень конфиденциальности и целостности с учетом указанных ограничений.

Аспекты криптографической защиты протокола NB-Fi

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

Протокол NB-Fi предназначен для использования в автоматизированных беспроводных системах контроля и учета различного типа ресурсов. Его спецификация имеет статус предварительного национального стандарта РФ. В докладе будет описана модель противника, актуальная для этого протокола, и результаты анализа криптографических свойств его текущей версии. Также в докладе будут представлены и обоснованы предложения по улучшению криптографических качеств протокола NB-Fi.

Безопасность протокола LoRaWAN RU

***Шемякина Ольга Викторовна**, системный аналитик, ИнфоТеКС*

В 2019 году ТК194 «Кибер-физические системы» был представлен проект предварительного национального стандарта «Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением». Данный протокол позиционируется как региональная спецификации протокола LoRaWAN 1.1 – LoRaWAN RU. При этом утверждается, что LoRaWAN RU поддерживает российские криптографические алгоритмы и позволяет обеспечить необходимый уровень безопасности передачи данных. Однако анализ описанных механизмов показывает, что утверждение о безопасности LoRaWAN RU и соответствии его требованиям российского законодательства и регулятора в области криптографической защиты информации преждевременно.

Организация криптографической защиты информации в интеллектуальной системе учета электрической энергии

***Костромин Игорь Сергеевич,** начальник отдела, АО «ПКК МИЛАНДР»*

Интеллектуальные системы учета электрической энергии (ИСУЭ) обеспечивают высокий уровень прозрачности и эффективности предоставления услуг потребителям. Использование для передачи данных информационных сетей общего доступа снижает стоимость и повышает надежность разворачиваемых систем, однако делает их более уязвимыми к атакам. Важно предложить схему защиты информации, одновременно удобную для электроснабжающих компаний, прозрачную для пользователей и стойкую к действиям злоумышленников. Доклад посвящен вариантам построения такой системы.

10:00 – 11:40 Секция «Криптография и криптоанализ». 2 часть

Зал «Еловый»

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Попов Владимир Олегович**, Ассоциация «РусКрипто», КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

Автоматическая трансляция спецификаций криптографических протоколов в нотации CMN.1 в нотацию ProVerif

***Прокопьев Сергей Евгеньевич,** к.т.н., ТК26*

Нотация CMN.1 позволяет получать лаконичные декларативные исполнимые спецификации криптографических протоколов и нацелена на применение в документах RFC. В докладе рассмотрена одна из возможностей, возникающих в рамках данной технологии: автоматическая трансляция спецификаций в нотации CMN.1 в спецификации на языках анализаторов безопасности схем протоколов, таких как Scyther, ProVerif, Tamarin и т.п. (на примере анализатора ProVerif).

Усовершенствованная схема разделения секрета и шифрование на основе атрибутов

***Кудинов Михаил Александрович,** научный сотрудник, Российский Квантовый Центр*

Представлена новая схема двух криптографических примитивов. Первая конструкция улучшает существующую в настоящее время обобщенную схему разделения секретов. На основе этого улучшения предлагается конструкция, которая позволяет разработать схему шифрования на основе атрибутов, относящуюся к некоторой структуре доступа с точки зрения атрибутов. Были проведены доказательства безопасности для обеих конструкций.

Обобщенные (L,G)-коды в современном алгоритме Нидеррайтера

Беззатеев Сергей Валентинович, *д.т.н., зав.каф. Технологий защиты информации, ГУАП*

Рассматривается модификация постквантового современного алгоритма Нидеррайтера (“Modern Niederreiter Encryption Algorithm”) использующая обобщенные (L,G)- коды с сепарабельным многочленом G(x) и рациональными функциями со степенью знаменателя большей 1 в качестве нумераторов позиций L. Предложены параметры обобщенных (l,G) - кодов для модифицированного алгоритма шифрования, удовлетворяющие 1,3 и 5 уровню защищенности по классификации NIST.

Об одном биологическом генераторе псевдослучайных чисел

Цыпышев Вадим Николаевич, *к.ф.-м.н., ведущий инженер, С-Терра СиЭсПи*

В докладе предлагается биологический датчик(генератор) псевдослучайных чисел, обосновываемый из теории хаотических процессов.

Физически неклонируемые функции в криптографии

Чичаева Анастасия Александровна, *младший специалист исследователь лаборатории криптографии АО «Научно-производственная компания «Криптонит»*

В работе исследуется возможность применения физически неклонируемых функций в криптографических задачах, таких как генерация ключей и аутентификация объектов. Рассмотрены преимущества и недостатки использования физически неклонируемых функций в протоколах аутентификации.

12:00 – 13:00 Секция «Криптография на транспорте и в промышленности»

Зал «Шишка»

Вопросы криптографической защиты беспроводных узкополосных сетей в транспортной отрасли Российской Федерации. Требования к протоколам, сравнительный анализ существующих протоколов и вопросы стандартизации в этой области. Криптография и информационная безопасность в Индустриальном интернете вещей.

Ведущие:

- **Ткаченко Евгений Иванович**, заместитель директора Департамента цифровой трансформации Министерства транспорта РФ
- **Бирман Александр Абрамович,** ФГУП «ЗащитаИнфоТранс»

Результаты НИОКР «Разработка системы криптографической защиты узкополосных беспроводных сетей передачи данных транспортной телематики»

Бирман Александр Абрамович, *ФГУП «ЗащитаИнфоТранс»*

Индустриальный интернет вещей. Особенности реализации и проблемы защиты на объектах добычи, транспортировки и хранения газа

Исаев Андрей Викторович*, генеральный директор ООО «Цифровое кольцо»*

12:00 – 13:00 Секция «Криптография и криптоанализ». 3 часть

Зал «Еловый»

Ведущие:

- **Матюхин Дмитрий Викторович,** ФСБ России
- **Попов Владимир Олегович,** Ассоциация «РусКрипто», КриптоПро
- **Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана

О необходимости реализации мер защиты от атак по побочным каналам для алгоритмов, основанных на использовании функции хеширования

***Матвеев Сергей Васильевич**, Пензенский филиал ФГУП «НТЦ «Атлас»*

В докладе рассматривается конструкция HMAC на основе ключевой функции хэширования, широко используемая в отечественных стандартизированных решениях. Показано, что для конструкции HMAC наравне с алгоритмами блочного шифрования, также необходимо предусматривать реализацию мер защиты от атак по побочным каналам. Предложены возможные подходы к реализации мер защиты.

О новом алгоритме контроля целостности данных

***Коренева Алиса Михайловна,** к.ф.-м.н., начальник отдела криптографического анализа ООО «Код Безопасности»*

***Фомичев Владимир Михайлович**, д.ф.-м.н., научный консультант, Код Безопасности*

При проведении анализа программного обеспечения актуальна задача контроля целостности данных больших массивов, при решении которой важно обеспечить приемлемый компромисс между криптографическими свойствами алгоритма контроля целостности (АКЦ) и ресурсами, необходимыми для его реализации. Предложен алгоритм генерации 128-битового кода для контроля целостности блоков данных размера 1 КБайт. Алгоритм удовлетворяет ряду важных требований к свойствам алгоритмов данного класса: невысокая вычислительная и емкостная (по памяти) сложность реализации; высокая вычислительная сложность определения двух блоков данных, порождающих одинаковый код; полное перемешивание входных данных, то есть существенная зависимость каждого бита кода от каждого бита блока данных.

Об одной низкоресурсной функции хэширования

***Бондакова Ольга Сергеевна,** Российский технологический университет (РТУ МИРЭА)*

В докладе формулируются требования к низкоресурсной функции хэширования, предназначенной для обеспечения защиты данных на нижних уровнях иерархической структуры системы автоматизации датчиков и других полевых устройств, расположенных в рамках контура защиты предприятия. Приводятся описание синтезированной хэш-функции, соответствующей сформулированным требованиям и результаты ее криптографического анализа.

13:20 – 14:30 Секция «Информационная безопасность и криптография в государственных проектах»

Зал «Шишка»

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

Ведущие:

- **Тютрюмов Александр Александрович**, заместитель директора Департамента развития цифрового государства, Министерство цифрового развития, связи и массовых коммуникаций
- **Пьянченко Андрей Андреевич,** руководитель научно-исследовательского департамента НИИ «Восход»
- **Горелов Дмитрий Львович**, управляющий партнер компании «Актив», директор ассоциации «РусКрипто»

Информационная безопасность в госсекторе. Основные направления развития
***Парфенов Юрий Владимирович**, заместитель директора Департамента реализации стратегических проектов, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации*
Глобальная цифровизация государственного управления и перевод основных государственных услуг в электронный вид предъявляют новые требования к информационной безопасности. Какие ближайшие и долговременные пути развития технологий информационной безопасности в госсекторе?

Электронный паспорт гражданина РФ
***Чижевский Игорь Евгеньевич,** заместитель руководителя департамента, НИИ «Восход»*
***Вдовина Мария Сергеевна,** системный архитектор, НИИ «Восход»*
Что такое электронный паспорт, зачем он нужен и что дает? Что смогут делать органы власти и коммерческие организации при помощи электронного паспорта? Инфраструктура и сценарии работы. Методы и механизмы защиты, используемые протоколы, стандарты и алгоритмы защиты.

Рабочее место госслужащего, аутентификация и электронная подпись
***Горелов Дмитрий Львович**, управляющий партнер компании Актив, директор ассоциации «РусКрипто»*
Сквозная цифровизация процессов госуправления предъявляет новые требования к рабочему месту госслужащего, к тому как происходит процесс аутентификации в информационных системах, как устанавливается доверие и как применяются технологии электронной подписи. Варианты решения, российский и мировой опыт, эволюция технологий.

Национальный Удостоверяющий Центр. Внедрение отечественной криптографии на российский сегмент сети Интернет.
***Пьянченко Андрей Андреевич,** руководитель научно-исследовательского департамента НИИ «Восход»*
Проект «Национальный Удостоверяющий Центр». Что он даст государству и гражданам? Влияние на государственные информационные системы. Этапы внедрения российской криптографии в российский сегмент Интернет.

13:20 – 14:30 Секция «Системы квантового распределения ключей и квантовые коммуникации»
Зал «Еловый»

Готовность разработок систем квантового распределения ключей к практическому внедрению, возможные горизонты массового применения. Свойства и качества этих систем с точки зрения потребителя. Насущные вопросы стандартизации систем квантового распределения ключей.

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

Направления работ в области создания квантовой коммуникационной инфраструктуры ОАО «РЖД»
***Глейм Артур Викторович,** начальник департамента квантовых коммуникаций, ОАО «РЖД»*
В докладе будет представлена сформированная стратегия развития ОАО «РЖД» по направлению «Квантовые коммуникации». Обсуждены основные поставленные цели, запланированные экосистемные, инфраструктурные и научно-исследовательские мероприятия.

Квантовые технологии: современное состояние и перспективы.
***Кулик Сергей Павлович,** д.ф-м.н., профессор кафедры квантовой электроники, МГУ имени М.В. Ломоносова*

Квантовые системы и сети

Верещагина Елена Валентиновна, *генеральный директор, ООО «Квантителеком»*

Общая концепция и обоснование использования доверенных узлов в квантовых коммуникационных сетях. Перешифрование данных на квантовых ключах и перешифрование ключей в сетях на основе доверенных промежуточных узлов (понятие квантово-защищенных ключей). Система управления ключами и система управления сетью. Генерация и распределение квантово-защищенных ключей между пользователями сети. Задачи управления и мониторинга протяженных квантовых сетей: управление сервисами, ресурсное планирование, контроль параметров качества оказания услуг.

Международная стандартизация в области квантового распределения ключей: текущее состояние и перспективы

Уривский Алексей Викторович, *заместитель генерального директора по науке и инновациям, ИнфоТеКС*

В докладе рассматриваются активности по стандартизации КРК в международных, региональных и отраслевых организациях по стандартизации. Будет приведен краткий обзор разрабатываемых документов ISO/IEC JTC 1/SC27, ITU-T SG13, SG17 и Focus Group on Quantum Information Technology for Networks, ETSI Industry Specification Group on QKD, IETF Quantum Internet Proposed Research Group. Будет проведен краткий анализ и сравнение разрабатываемых стандартизующих документов по объектам и целям стандартизации.

15:30 – 17:00 Круглый стол «Информационная безопасность Интернета вещей»

Зал «Шишка»

Обсуждение вопросов безопасности Интернета вещей на пользовательском и индустриальном уровнях. Злоумышленники удаленно взламывают устройства и, получив контроль над ними, используют для совершения распределенных DDoS-атак, майнинга криптовалют и похищения личной информации о владельцах. Однако, несмотря на очевидные угрозы, пользователи домашних Интернет-вещей не придают особого значения вопросам кибербезопасности. Что сделать, чтобы изменить отношение массового пользователя к этой проблеме? Как обезопаситься от несанкционированного сбора информации с цифровых устройств и вмешательства в частную жизнь, могут ли сами производители повысить безопасность выпускаемой «умной техники», какие подходы и промышленные стандарты используются для обеспечения безопасности решений IoT, и поможет ли здесь импортозамещение? Каковы перспективы использования российской криптографии в индустриальных сетях и в LPWAN. Эксперты постараются дать всестороннюю оценку данной проблеме и обозначить пути ее решения.

Ведущий: Елисеев Игорь Юрьевич, заместитель директора, Академия Информационных Систем

Эксперты круглого стола:

- **Бугаенко Андрей Валерьевич**, заместитель директора ФГБУ НИИ «Восход»
- **Уткин Никита Александрович**, Председатель технического комитета по стандартизации «Киберфизические системы» (ТК 194)
- **Масалович Андрей Игоревич**, ведущий эксперт-преподаватель Академии Информационных Систем по конкурентной разведке и OSINT
- **Скляров Дмитрий Витальевич**, руководитель отдела анализа приложений, Positive Technologies
- **Гурин Олег Дмитриевич**, к.ф-м.н., старший менеджер по развитию бизнеса, компания QRate

15:30 – 17:00 Секция «Технологии распределенного реестра»

Зал «Еловый»

Блокчейн сервисы имеют свои особенности обеспечения требований информационной безопасности. Что нужно знать, чтобы обеспечить безопасную эксплуатацию таких сервисов? Из каких элементов состоят блокчейн системы и на что могут быть направлены атаки злоумышленников? Какие отличия в процессах настойки и запуска распределенных и классических систем, которые должен знать и уметь диагностировать специалист по информационной безопасности? На эти и другие вопросы попытаются дать ответы эксперты, а также дать оценку скорости перехода рынка на технологии распределенного реестра.

Ведущие:

- **Шумский Лев Станиславович,** директор по информационной безопасности, Ассоциация ФинТех
- **Конкин Анатолий Юрьевич**, руководитель направления развития распределённых реестров, Ассоциация ФинТех

Построение архитектуры финансовых сервисов на блокчейн. Практика эксплуатации Мастерчейн
Цветков Алексей Игоревич, *руководитель группы разработки, Ассоциация ФинТех*

Разработка безопасных блокчейн приложений. Использование платформы Waves в разных отраслях
Калихов Артём, *Директор по продукту Waves Enterprise*

Внедрение распределенных систем в Банке: особенности использования технологии блокчейн
Портнягин Сергей Юрьевич, *старший менеджер подразделения цифровых инноваций и технологических исследований, Райффайзенбанк*

Виды консенсусов и атаки на них
Руль Валентин, *QIWI Blockchain Technologies*

15:30 – 17:00 Секция «Интеллектуальные методы обеспечения кибербезопасности промышленных систем»

Зал «Сосновый»

Цифровизация промышленности привела к появлению в индустрии новых проблем, связанных с обеспечением информационной безопасности. Новому классу угроз, названных, в соответствии с требованиями времени, «киберугрозами» ставится в соответствие новый класс систем обеспечения безопасности: систем кибербезопасности цифрового производства.

Ведущие:

- **Зегжда Дмитрий Петрович,** д.т.н., профессор РАН, Директор Высшей школы кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого, главный конструктор ООО «НеоБИТ»
- **Москвин Дмитрий Андреевич**, к.т.н., доцент Высшей школы кибербезопасности и защиты информации Санкт-Петербургского Политехнического университета Петра Великого, технический директор ООО «НеоБИТ»

Современные подходы к обеспечению кибербезопасности промышленных систем
Москвин Дмитрий Андреевич*, к.т.н., ООО «НеоБИТ», Санкт-Петербург*

Подход к оценке и обеспечению киберустойчивости систем цифрового производства*

***Павленко Евгений Юрьевич**, к.т.н. Санкт-Петербургский Политехнический университет Петра Великого*

**Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1689.2019.5*

В докладе предлагается рассмотреть подход к оценке киберустойчивости на основе графового представления функционирования системы ЦП. Подход ориентирован на развивающиеся системы ЦП, сетевая инфраструктура которых является гибкой и обладает избыточностью, а также характеризуется взаимозаменяемостью компонентов. Предлагается оценивать киберустойчивость как способность системы ЦП к переконфигурированию, сохраняющему целевую функцию системы даже в условиях деструктивных воздействий. Предлагается развитие подхода к оценке киберустойчивости для высокоинтеллектуальных систем ЦП, наделяемых способностью к самообучению и саморазвитию.

Метод формирования обучающей выборки для нейросетевой системы выявления киберугроз в промышленных сетях

***Крундышев Василий Михайлович**, Санкт-Петербургский Политехнический университет Петра Великого*

В докладе представлен метод формирования обучающей выборки, приведены характеристики полученных наборов данных. В результате проведенного моделирования предложенный метод показал свою высокую эффективность, сформированные наборы данных оказались репрезентативными и не противоречивыми.

Применение адаптивного управления для противодействия атакам внутренних нарушителей в WSN-сетях

***Овасапян Тигран Джаникович**, ООО «НеоБИТ», Санкт-Петербург*

В докладе рассматривается обеспечение безопасности беспроводных сенсорных сетей (WSN) от атак вредоносных узлов. Проанализированы типовые угрозы и выявлены актуальные атаки на WSN-сети. Предложен подход обеспечения защиты от вредоносных узлов с использованием адаптивного поведения. В рамках предложенного подхода узлы способны изменять свое поведение и сохранять устойчивость функционирования в условиях совершения кибератак.

Групповая аутентификация на решетках в Промышленном интернете вещей

***Ярмак Анастасия Викторовна**, ООО «Лаборатория Кибербезопасности», Санкт-Петербург*

Промышленный интернет вещей (Industrial Internet of Things, IIoT) объединяет множество устройств от маленьких датчиков до сложных станков в единую интеллектуальную систему с возможностью автоматизации производства и оптимизации бизнес-процессов. Групповая аутентификация является одним из способов, призванным оптимизировать процесс организации защищенного взаимодействия с учетом специфики Промышленного интернета вещей путем обработки аутентификационных данных не на уровне конкретных узлов, а на уровне подсистем и групп устройств, агрегированных по каким-либо критериям (технологическим подпроцессам, местоположению, вычислительным характеристикам и т.п.).

Оценка защищенности блокчейн-систем от угроз, обусловленных неравномерным распределением вычислительных мощностей

***Бусыгин Алексей Геннадьевич**, ООО «НеоБИТ», Санкт-Петербург*

Блокчейн является технологией, позволяющей решать задачи обеспечения информационной безопасности в различных областях деятельности человека: в обработке данных финансовых транзакций, ценных бумаг, юридически значимых документов, реестров, систем доменных имен, инфраструктур открытых ключей, логистических систем. При этом блокчейн-системы подвержены угрозам информационной безопасности, обусловленным неравномерным распределением вычислительных мощностей. Примером реализации таких угроз является атака большинства («51%»). В докладе приводится обзор предложенных на данный момент способов противодействия данному классу угроз и показывается, что рассмотренные в ней механизмы также обладают значительными недостатками.

17:30 – 19:30 Секция «Российский вектор развития безопасной радиочастотной идентификации (RFID)»

Зал «Шишка»

Развитие радиочастотной идентификации в России с учетом существенного влияния вопросов безопасности на перспективы этой технологии. В рамках докладов и открытой дискуссии будут рассмотрены технологические, организационные и другие аспекты разработки и внедрения решений RFID по идентификации и аутентификации. Место российской криптографии в RFID, варианты конкретных решений на основе российских криптографических алгоритмов, направления и этапы стандартизации.

Ведущий: Вартан Микаэлович Хачатуров, генеральный директор, НПК «Криптонит»

Криптографические механизмы в технологии RFID

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

Технология радиочастотной идентификации (RFID) продолжает развиваться и используется во многих областях нашей жизни. Основными способами обеспечения безопасности RFID при аутентификации или осуществлении бесконтактных платежей являются криптографические механизмы. При этом использование криптографии в RFID имеет ряд особенностей, связанных как с самой технологией, так и с существующими стандартами. В докладе рассматривается место и роль криптографических механизмов для защиты технологии RFID. Кроме того, в докладе предлагаются подходы к использованию российских криптографических алгоритмов и обозначены направления по стандартизации отечественных решений.

Государственное регулирование средств и систем защиты (контроля), основанных на технологии RFID.
Петров Алексей Владимирович, *ТК 26*

Системы обеспечения защиты или контроля за различными процессами с использованием RFID могут оказаться системами, обрабатывающими данные подлежащие обязательной защите. В таком случае роль государства определена соответствующими нормативными правовыми актами. В докладе будет рассмотрены некоторые параллели с существующими системами, не использующими RFID, приведено несколько примеров систем, подлежащих государственному регулированию, а также систем, где государственное участие в настоящее время не предполагается.

Применение отечественной микросхемы с RF интерфейсом для защищенных электронных документов
Вараксин Денис Владимирович, *ПАО «Микрон»*

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

Зал «Еловый»

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

Ведущий: Котенко Игорь Витальевич, д.т.н., профессор, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности, СПИИРАН

Интеллектуальные технологии киберситуационной осведомленности

Котенко Игорь Витальевич, *д.т.н., профессор, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности, СПИИРАН*

Рассматривается современное состояние исследований и разработок в области создания компонентов киберситуационной осведомленности. Анализируются модели, методики и средства киберситуационной осведомленности, в том числе на основе технологий Advanced Security Analytics. Выделяются перспективные направления исследований и разработок.

Моделирование динамических информационных конфликтов при противоборстве сложных многоуровневых систем (на примере систем связи)

Макаренко Сергей Иванович, *д. т. н., доцент, СПбГЭТУ «ЛЭТИ»*

Реальные профессиональные нарушители – это специально подготовленные подразделения, имеющие доступ к новейшим технологиям и поддержку на уровне официальных государственных структур. В докладе представлен новый научный подход, основанный на теории конфликтов, который позволяет формализовать и исследовать процессы взаимодействия профессионального нарушителя и подсистемы защиты сложной технической системы.

Подход к классификации последовательностей, сформированных алгоритмами сжатия и шифрования

Козачок Александр Васильевич*, д.т.н., Академия ФСО*

Спирин Андрей Андреевич*, Академия ФСО*

В виду увеличившегося количества утечек информации по вине внутренних нарушителей и отсутствия у современных DLP-систем механизмов противодействия утечкам информации в зашифрованном или сжатом неизвестным алгоритмом виде, в работе предлагается подход к классификации последовательностей, сформированных алгоритмами шифрования, сжатия и генераторами псевдослучайных последовательностей. Для решения задачи классификации использовался метод машинного обучения на основе деревьев решений. В качестве признакового пространства был выбран массив частот двоичных последовательностей длины 9 бит. Разработанный подход показал точность классификации псевдослучайных последовательностей более 0.98.

Обнаружение вредоносных информационных объектов в сети Интернет с использованием методов машинного обучения

Браницкий Александр Александрович*, к.т.н., СПИИРАН*

В докладе рассматривается методика обнаружения вредоносных информационных объектов в сети Интернет. В качестве анализируемых объектов выступают html-страницы, структура и текст которых обрабатываются при помощи методов машинного обучения с целью обнаружения вредоносного контента. Приводятся результаты экспериментов, полученных для различных классификаторов машинного обучения и их комбинирования в виде метода взвешенного голосования.

Моделирование атак истощения энергоресурсов на беспилотные летательные аппараты в системах антикризисного управления

Десницкий Василий Алексеевич*, к.т.н., СПбГУТ*

В работе исследуются атаки, направленные на истощение энергоресурсов беспилотных летательных аппаратов (БПЛА). На примере БПЛА для лабораторного прототипа системы кризисного управления, собранного на базе Parrot A.R. Drone 2.0, моделируются атаки несанкционированного утяжеления и нарушения центровки, аппаратного отъема энергоресурса, модификации траектории движения и внесения избыточных движений, атака типа Denial-of-Sleep и др. На основе экспериментов определены сравнительные характеристики смоделированных атак, влияющие на возможности их практической выполнимости.

Комплексный подход к моделированию железнодорожных объектов

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

***Бахтин Юрий Евгеньевич**, СПИИРАН*

Железные дороги представляют собой критически важную инфраструктуру, успешные атаки на которую могут привести к серьезным финансовым и репутационным потерям. В докладе представляется комплексный подход к моделированию, объединяющий аналитическое, имитационное, полунатурное и покомпонентное представление железнодорожных объектов. Данный подход позволяет как оценить защищенность существующих систем, так и проанализировать возможные новые решения, направленные на обеспечение безопасности железнодорожного транспорта.

Аппаратная поддержка доверенной среды исполнения в микроконтроллерах и микропроцессорах с ядрами ARM v.7, ARM v.8A и ARM v.8M

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

Наиболее надежной считается криптографическая защита информации, которая строится в предположении недоступности так называемых закрытых ключей. Преодолев механизмы реакции на несанкционированный доступ к устройству, нарушитель может инжектировать в среду исполнения различного рода вредоносное ПО, предназначенное для получения этих ключей (так же, как и других активов) непосредственно из контекста выполняемых преобразований данных. В докладе рассматриваются способы создания доверенной среды для выполнения критичных операций с целью ограничения доступа к активам со стороны стороннего ПО на уровне аппаратных средств современных микроконтроллеров и микропроцессоров архитектуры ARMv8-A и ARMv8-M.

17:30 – 19:30 Секция «Доклады студентов и аспирантов»

Зал «Сосновый»

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

Детектирование атак по времени на реализации криптографических алгоритмов

***Набоков Денис Алексеевич**, МГТУ им. Баумана*

Рассматривается подход к детектированию атак на основе непосредственного запуска программы на различных входных данных и сбора времени выполнения. На собранных данных проводятся два статистических теста: т-тест Уэлча (Welch's t-test) и тест Колмогорова-Смирнова. Первый широко распространен в контексте атак по сторонним каналам, тогда как последний не использовался для задач по детектированию атак по времени, хотя представляет интерес.

Разработка параметризованной криптографической хеш-функции Hamsi-n

***Ермаков Кирилл Дмитриевич**, НИЯУ МИФИ Институт интеллектуальных кибернетичеких систем*

В работе рассматривается параметризованное семейство Hamsi-подобных хеш-функций. Описан класс линейных преобразований, коэффициент рассеивания которых равен коэффициенту рассеивания линейного преобразования Hamsi. Найдены инвариантные подпространства этих преобразований. Каждая хеш-функция семейства задается линейным преобразованием из этого класса. Получены оценки (теоретические и практические) скорости работы хеш-функций семейства.

Исследование многочленов специального вида для использования фильтрующих генераторов

***Фонарева Алиса Вадимовна**, МИЭМ им. Тихонова (НИУ ВШЭ)*

В криптографических приложениях используют различные способы усложнения линейных рекуррентных последовательностей с целью избежать простой аналитической связи знаков выходной гаммы с начальным состоянием ЛРП. Одним из них является фильтрующий генератор, задаваемый парой (L,f) функций, где L – линейная функция обратной связи регистра сдвига, f – нелинейная функция выхода (фильтр). К фильтрующему генератору предъявляются требования равновероятности выходных n-грамм и максимальности периода выходной последовательности. В данной работе проведено исследование по нахождению некоторых множеств пар (L,f), удовлетворяющих указанным свойствам. Полученные результаты могут быть применены для построения датчиков случайных чисел.

Возможно ли создание низкоресурсных RFID-меток на основе российской криптографии?

***Высоцкая Виктория Владимировна**, МГУ им. М. В. Ломоносова*

В докладе сравниваются российские и соответствующие им международные криптографические алгоритмы с точки зрения низкоресурсности. Разработаны прототипы всех рассматриваемых алгоритмов на языке описания схем Verilog. Показано, что по основным параметрам российские аналоги сопоставимы со своими международными аналогами, признанными низкоресурсными.

Теория-игровой подход к обеспечению безопасности саморегулирующихся систем

***Соловей Роман Сергеевич**, Высшая Школа Кибербезопасности и Защиты Информации (ВШКиЗИ) Санкт-Петербургского политехнического университета Петра Великого (СПбПУ)*

В современном мире, на фоне непрерывно возрастающего интереса к Интернету вещей, все более широкое распространение получают динамические информационные системы. К привычным MANET, VANET и FANET сетям активно добавляются сети Промышленного интернета вещей, объединяющие физические и информационные процессы. Одним из наиболее перспективных подходов к обеспечению безопасности в данных условиях является концепция динамической защиты, подразумевающая саморегуляцию системы «на лету». Для решения задачи реконфигурации структуры саморегулирующейся информационной системы предлагается использовать теоретико-игровой подход, позволяющий найти оптимальную стратегию изменения топологии системы в условиях компьютерной атаки.

Обнаружение угроз безопасности современных веб-сайтов

***Кубрин Георгий Сергеевич**, Высшая Школа Кибербезопасности и Защиты Информации (ВШКиЗИ) Санкт-Петербургского политехнического университета Петра Великого (СПбПУ)*

Веб-технологии, начавшиеся со статических HTML-документов для распространения научных статей, на сегодняшний день проникли в большинство сфер человеческой деятельности. По данных компании Netcraft, на февраль 2020 года в сети Интернет насчитывалось более 1260 миллионов веб-сайтов, что отражает широкое применение веб-технологий. Современные веб-сайты используются для предоставления доступа к широкому спектру услуг, от заказа такси до оформления кредита в банке. Для увеличения эффективности динамического анализа предлагается метод, реализующий интерпретацию JavaScript-сценариев, эмитируя работу современных веб-браузеров. Разработанный прототип инструмента динамического анализа показал лучшие результаты по составлению карты страниц и точек получения параметров от пользователя для динамических веб-сайтов и веб-приложений относительно существующих сканеров уязвимостей.

Ассоциация «РусКрипто»

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

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

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

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

Контактная информация:
www.ruscrypto.ru

Академия Информационных Систем

Академия Информационных Систем (АИС) создана в 1996 году. Более 20 лет АИС предоставляет образовательные услуги по информационной безопасности, информационным технологиям, конкурентной разведке и экономической безопасности. Обучение своих кадров нам доверяют Пенсионный фонд РФ, ФСС РФ, ФСКН России, ФСО России, ФССП России, ФСБ России, «Сбербанк», «Газпромбанк», «Альфа банк», «Северсталь», МТС, «Ростелеком» и многие другие.

Академия Информационных Систем сегодня это:

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

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

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

КРИПТОПРО

ключевое слово в защите информации

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

Продукты компании КриптоПро включают поддержку всех современных платформ, имеют версии для мобильных устройств, интегрированы с ведущими российскими и зарубежными IT решениями, широко используются органами власти и коммерческими организациями всех отраслей. Они применяются в системах электронного документооборота, исполнения госзаказа, сдачи бухгалтерской и налоговой отчетности и т.п. Средства электронной подписи КриптоПро CSP/JCP установлены более чем на 10 000 000 серверах, рабочих местах и мобильных устройствах пользователей. Разработанные компанией КриптоПро средства обеспечения деятельности удостоверяющих центров внедрены более чем в 1000 организациях; в том числе и в составе Головного удостоверяющего центра Минкомсвязи России.

www.cryptopro.ru

КЛЮЧЕВОЕ СЛОВО

В ЗАЩИТЕ ИНФОРМАЦИИ

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

Продуктовый портфель компании содержит эффективные решения, направленные на повышение уровня информационной безопасности предприятий. У «Актива» накоплен обширный опыт реализации значимых проектов в ИКТ, корпоративном, финансовом и государственном секторах. Для этого у компании есть все необходимые лицензии ФСБ и ФСТЭК России на разработку и производство средств защиты информации.
Рутокен — первая в России полностью отечественная линейка аппаратных продуктов и решений для аутентификации и создания электронной подписи. Ключевые носители Рутокен используются везде, где требуется безопасное хранение и использование паролей, цифровых сертификатов, ключей шифрования и ключей электронной подписи. Электронные идентификаторы Рутокен представлены в различных форм-факторах: от стандартного USB-токена или смарт-карты до Bluetooth-устройств.

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

www.aktiv-company.ru; www.rutoken.ru; www.guardant.ru

РОССИЙСКИЙ
разработчик
и производитель

Входим в
ТОП-20
компаний в сфере
защиты информации

Более
25 лет
на рынке ИБ

Лучшие
ЭКСПЕРТЫ
отрасли

ПРОДУКТЫ
И РЕШЕНИЯ
для государственного,
коммерческого
и финансового сегментов

БОЛЕЕ 1000
реализованных
проектов

Компания «Актив» — крупнейший российский производитель аппаратных средств аутентификации и электронной подписи, разработчик и поставщик решений в сфере информационной безопасности.

РУТОКЕН

Продукты и решения в области аутентификации, защиты информации и электронной подписи

- Защита систем электронного документооборота
- Реализация российских криптоалгоритмов
- Защита персональных данных
- Защита электронной переписки
- Работа с ЭП в недоверенной среде и на мобильных платформах
- Безопасность каналов передачи данных
- Аутентификация и ЭП для web-порталов и облачных решений
- Соответствие требованиям ФСТЭК, ФСБ
- Зашифрованное хранение данных пользователя
- Интеграция со СКУД

Guardant

Средства защиты
и лицензирования
программного обеспечения.

- Защита от пиратства
- Лицензирование shareware
- Мобильные приложения
- Фискальные регистраторы
- Аппаратные DRM-системы

Россия, Москва,
Шарикоподшипниковская ул., 1
+7 495 925-77-90

www.aktiv-company.ru
www.guardant.ru
www.rutoken.ru

ИнфоТеКС (ОАО «Информационные Технологии и Коммуникационные Системы») — ведущий производитель программных и программно-аппаратных VPN-решений и средств криптографической защиты информации. Помимо разработки и продвижения средств защиты информации, компания обеспечивает их поддержку и обслуживание, ведет научно-исследовательскую и консалтинговую деятельность.

Ключевой разработкой ИнфоТеКС является технология ViPNet. На сегодняшний день это самое масштабируемое отечественное решение для построения универсальных защищенных сетей. Торговая марка ViPNet объединяет целый ряд продуктов и сетевых решений, рассчитанных на обработку информации ограниченного доступа, включая персональные данные.

www.infotecs.ru


infotecs
Мы защищаем
информацию,
которую вы цените
>1000
сотрудников
29
лет работы
на рынке ИБ
Топ-5
компаний в сфере
защиты информации
в России
10
офисов по всей
стране
>50
продуктов
для защиты
информации
>1 млн
рабочих станций
защищенных
продуктами ViPNet
www.infotecs.ru
+7 495 737-6192
8 800 250-0-260 (бесплатный звонок по России)
soft@infotecs.ru
hotline@infotecs.ru

КОД БЕЗОПАСНОСТИ

«Код Безопасности» - российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям российских, отраслевых и международных стандартов.

Продукты «Кода Безопасности» применяются для защиты конфиденциальной информации, коммерческой тайны, персональных данных и сведений, составляющих государственную тайну. «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации. Сервисный центр компании готов предоставить профессиональную техническую поддержку партнерам и Заказчикам компании 24 часа и 7 дней в неделю.

Познакомиться с отзывами о наших продуктах, и узнать, кто является нашими заказчиками, вы можете на сайте компании www.securitycode.ru.

www.securitycode.ru

КОД БЕЗОПАСНОСТИ

НА СТРАЖЕ ЦИФРОВОГО СУВЕРЕНИТЕТА

РОССИЙСКИЙ РАЗРАБОТЧИК

программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям стандартов.

КОМПАНИЯ ОСНОВАНА В 2008 ГОДУ

Ведет свою деятельность на основании девяти лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации.

БОЛЕЕ 400

сотрудников в штате компании.
R&D-специалисты имеют уникальные компетенции в области программирования и разработки продуктов для обеспечения информационной безопасности.

БОЛЕЕ 60

действующих сертификатов соответствия подтверждают высокое качество продуктов и позволяют использовать их в информационных системах с самыми жесткими требованиями к безопасности.

БОЛЕЕ 32000

государственных и коммерческих организаций в России доверяют продуктам «Кода Безопасности».

БОЛЕЕ 1000

авторизованных партнеров. Продукты компании «Код Безопасности» представлены во всех регионах РФ.

www.securitycode.ru

КРИПТОНИТ

Бренд «Криптонит» объединяет группу технологических компаний, которые ставят своей целью поддержку и развитие отечественных технологий, разработок и ИТ-талантов. «Криптонит» был основан в марте 2018 года и является частью «ИКС Холдинг» —многопрофильной ИТ-структуры.
Научно-производственная компания «Криптонит» - это совместный проект с Госкорпорацией «Ростех» на базе концерна «Автоматика».
Компания создает гражданские ИТ-продукты, используя лучшие российские военно-технические разработки. На базе НПК формируется уникальный научно-исследовательский центр (R&D), включающий в себя несколько лабораторий, в том числе:

- Лаборатория криптографии
- Лаборатория информационной и сетевой безопасности
- Лаборатория телекоммуникаций и спецтехники
- Лаборатория больших данных и статистики

НПК «Криптонит» является участником архитектурного совета, созданного Ростелекомом» и «Ростехом» по реализации заключенного с правительство соглашения в целях развития сетей связи 5G в России.
Важной частью совместного проекта НПК «Криптоит» с Госкорпорацией «Ростех» станет создание первого в России Музея криптографии и вычислительной техники, а также открытие выставочного комплекса.

Наша миссия
Мы помогаем российским технологиям развиваться и занимать достойное место на рынке ИТ. Мы инвестируем в отечественные таланты, технологические разработки и накопленный научный потенциал для создания высокотехнологичных продуктов и услуг, востребованных бизнесом и государством.

www.kryptonite.ru

КРИПТОНИТ

Наука. Технологии. Инновации

Ростелеком
Солар

«Ростелеком-Солар», компания группы ПАО «Ростелеком» – Национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

www.rt-solar.ru

Национальный провайдер кибербезопасности

rt-solar.ru

Ростелеком
Солар

Компания «Фактор-ТС», организованная в 1992 году, специализируется на разработке, производстве, внедрении и сопровождении программных и аппаратных средств защиты информации под торговой маркой DIONIS. Компания предлагает заказчикам решения по организации защищенных информационно-телекоммуникационных систем (ИТС) и других информационных систем в защищенном исполнении.

Технические решения компании позволяют замещать импортные аналоги в критически важных для безопасности страны сегментах национальной информационной структуры.
Изделия производства компании «Фактор-ТС» (маршрутизаторы, криптомаршрутизаторы, межсетевые экраны, клиентские средства защиты и др.) сертифицированы по требованиям ФСТЭК России и ФСБ России по самым высоким уровням защищенности и используются для организации безопасного информационного обмена во всех министерствах и ведомствах силового блока России.

www.factor-ts.ru

ФАКТОР·ТС

DIONIS DPS

UTM-РЕШЕНИЯ, СЕРТИФИЦИРОВАННЫЕ ФСБ И ФСТЭК РОССИИ

НЕОБИТ

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

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

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

www.neobit.ru

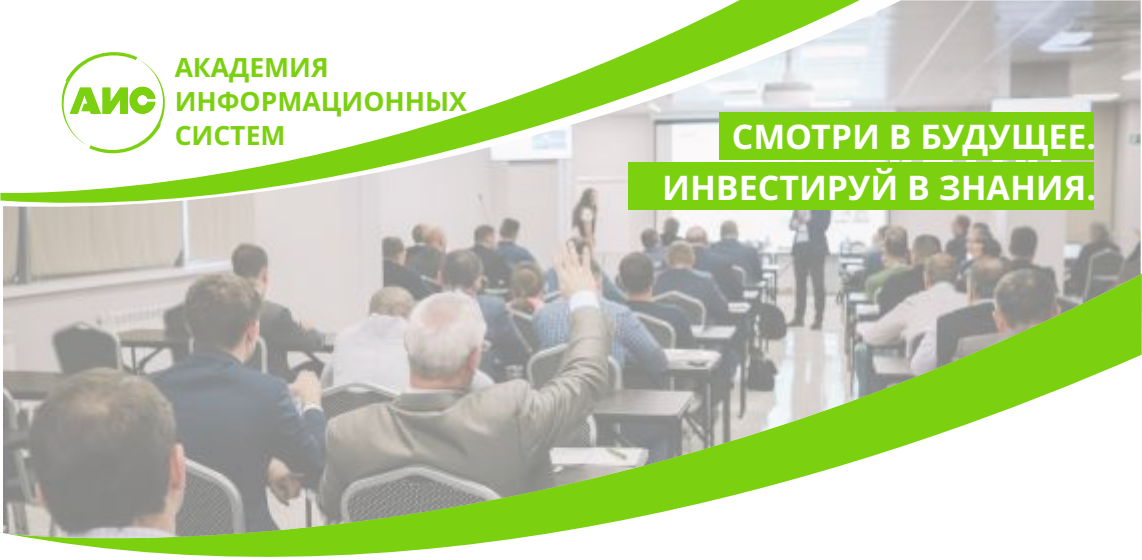
НЕОБИТ

Новые Безопасные Информационные Технологии

195220, Санкт-Петербург,
ул. Гжатская, д.21, «г».
+7 (812) 535-28-06
www.neobit.ru info@neobit.ru

АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

СМОТРИ В БУДУЩЕЕ.
ИНВЕСТИРУЙ В ЗНАНИЯ.

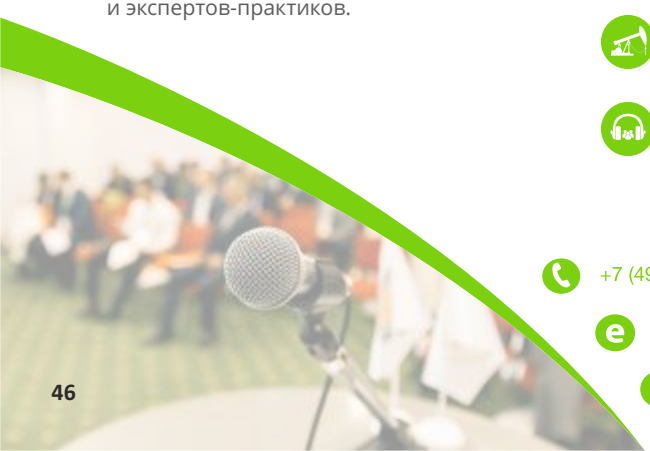


Почему выбирают нас

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

АИС известен как организатор деловых событий в России и за рубежом. Наши мероприятия проходят при поддержке и активном участии государственных ведомств и регуляторов, ассоциаций и общественных организаций, ученых и экспертов-практиков.

- Дополнительное профессиональное образование по программам, согласованным с ФУМО ИБ, ФСТЭК РФ, ФСБ РФ, Банком России
- Единственный учебный центр по направлению «Конкурентная разведка и экономическая безопасность»
- Более 300 курсов по направлению «Информационные технологии»
- Обучение для банков: НПС, СТО БР, Стандарт PCI DSS, защита ДБО, кибербезопасность и др.
- Подготовка к сертификациям CISA, CISM, CGEIT и др.
- Консалтинг по информационной безопасности
- Обучение по защите АСУ ТП, КИИ, ГосСОПКА
- Технологии дистанционного обучения, вебинары и онлайн-тестирование



+7 (495) 120-04-02

info@infosystem.ru

www.infosystems.ru www.vipforum.ru

КАЛЕНДАРЬ МЕРОПРИЯТИЙ АИС

14 АПРЕЛЯ 2020
МОСКВА

Весенняя сессия

AntiFraud Spring Russia

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

27-28 МАЯ 2020
МОСКВА

VIII научно-практическая конференция

Управление информационной безопасностью в современном обществе

Проблема обеспечения информационной безопасности разрабатываемых современных компьютерных технологий в условиях расширения импортозамещения программно-аппаратных компонентов.

7-10 СЕНТЯБРЯ 2020
КРЫМ

Ежегодный всероссийский форум

Информационная безопасность. Регулирование. Технологии. Практика. ИнфоБЕРЕГ

Нормативное правовое регулирование в области ИБ, перспективы развития, практический опыт, решение проблемных вопросов в ИБ.

ОКТЯБРЬ 2020
ПОДМОСКОВЬЕ

Ежегодная конференция

Цифровое государство: новые подходы к управлению и безопасности

Конференция посвящена вопросам развития в Российской Федерации цифровой экономики, электронных услуг и услуг в области информационной безопасности.

1-2 ДЕКАБРЯ 2020
МОСКВА

Практическая конференция

Конкурентная разведка & Экономическая безопасность

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

2-3 ДЕКАБРЯ 2020
МОСКВА

Международный форум

Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia

Организационные, юридические и технологические аспекты борьбы с мошенничеством. Управление рисками, практика расследования инцидентов и привлечение к ответственности злоумышленников. Проводится в рамках Недели безопасности АИС.

конференция
РусКрипто

СОРЕВНОВАНИЯ

В СПА-КОМПЛЕКСЕ

17 МАРТА
17:00 - 18:30

- Плавание
- Сквош
- Армрестлинг

Вручение ценных призов победителя - на CryptoBeerFest

конференция
РусКрипто

РАСПИСАНИЕ

СПОРТИВНЫХ ТУРНИРОВ

17 МАРТА
17:00 - 19:00
РАЗВЛЕКАТЕЛЬНЫЙ КОМПЛЕКС

- ТУРНИР ПО БИЛЬЯРДУ
- НАСТОЛЬНЫЙ ТЕННИС
- БОУЛИНГ

ГЛАВНЫЙ ПРИЗ ЯЩИК ПИВА!

РусКрипто'2020

ПРИГЛАШАЕМ НА ФЕСТИВАЛЬ
КРАФТОВОГО ПИВА

17 МАРТА, НАЧАЛО В 20:00

Лобби ресторанного комплекса, 1 этаж

Так же на CryptoBeerFest будет проходить награждение участников, занявших первые 3 места в спортивных мероприятиях!


РусКрипто
18
МАРТА
Торжественное
открытие
XXII международной
научно-практической конференции
РусКрипто‘2020
ЗАЛ „ШИШКА“, 2 ЭТАЖ
НАЧАЛО В 20:00

РусКрипто'2020

АНГЛИЙСКИЙ ВЕЧЕР

19 МАРТА, 20:00

ЗАЛ "ШИШКА", 2 ЭТАЖ

Интеллектуальная игра
Крипто Quiz
с Алексеем Лукацким

А так же, этим же вечером вас ждут:

РусКрипто

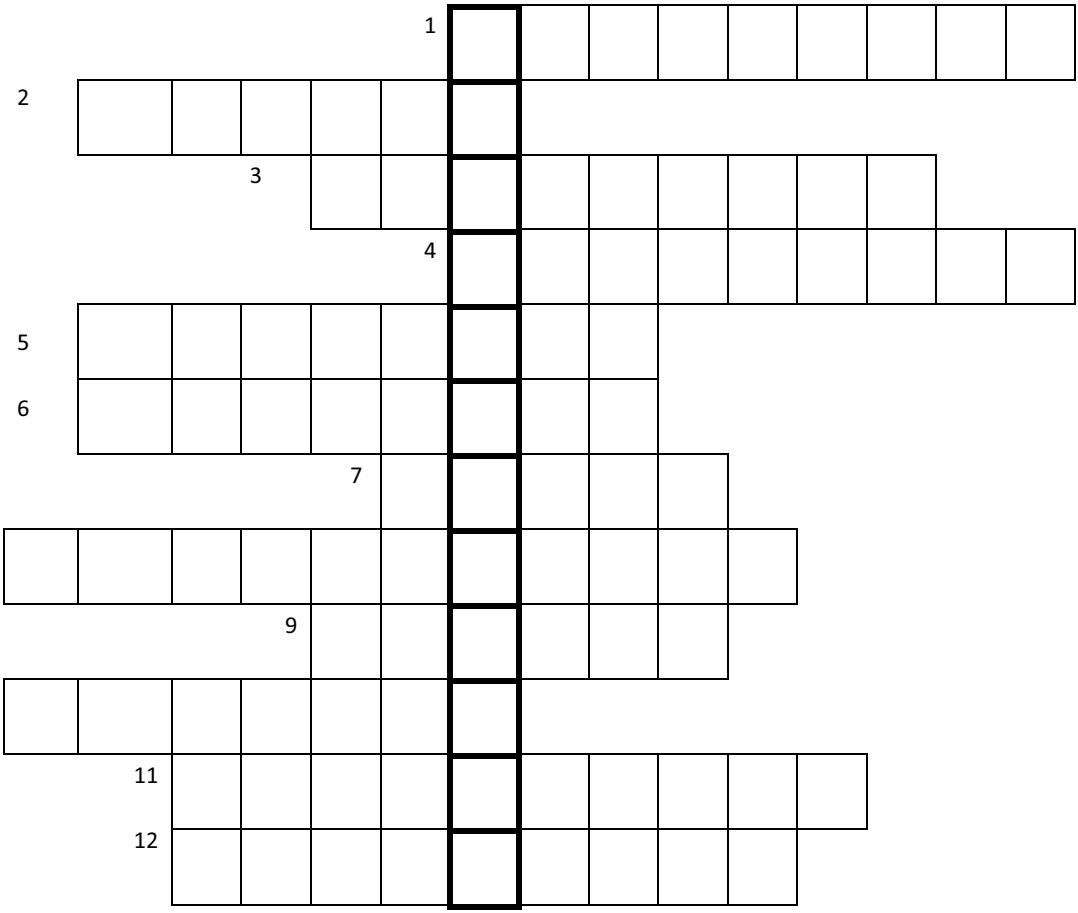
КАРАОКЕ БАТТЛ

19 МАРТА, 20:00

ЧАЙНЫЙ ДОМИК

#ИМЕНИКОМИСАРЕНКО!

КРИПТО КРОССВОРД



конференция
РусКрипто

КРИПТО КРОССВОРД

1. Русский драматург, использующий шифр Ришелье для отправки секретных донесений на Родину, пряча их в письмах жене

2. Криптоаналитик, предложивший XSL-атаку против некоторых шифров, и доказавшего существование атаки на ГОСТ 28147-89

3. Дешифрование телеграммы этого человека привело к вступлению США в войну на стороне Антанты

4. Центр Правительственной Связи Великобритании открыл новый офис в этом городе к своему 100-летию

5. Дом отдыха, в котором проходила первая РусКрипто

6. Фамилия советского разведчика, участвовавшего во взломе "Энигмы" вместе с Аланом Тьюрингом?

7. Племя индейцев, привлеченных американской армией во время Первой мировой войны к обеспечению засекреченной связи

8. Функция, осуществляющая преобразование массива входных данных произвольной длины в выходную строку фиксированной длины по определенному алгоритму

9. Советская криптографическая машина М-125, созданная после Второй мировой войны

10. Фамилия криптографа, введшего в оборот термин «криптоанализ»

11. Электронный документ, удостоверяющий принадлежность открытого ключа некоторому субъекту

конференция РусКрипто

+7 (495) 120-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru