Ассоциация РусКрипто

ОРГАНИЗАТОРЫ

АИС

XXI МЕЖДУНАРОДНАЯ
НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУСКРИПТО'2019

ПРОГРАММА

19-22 МАРТА 2019 Г.

КЛЮЧЕВОЕ СЛОВО

В ЗАЩИТЕ ИНФОРМАЦИИ

#RusCrypto

СКАЧИВАЙТЕ ПРИЛОЖЕНИЕ РУСКРИПТО’2019

- Скачивайте программу конференции!
- Обменивайтесь мнениями!
- Знакомьтесь с другими участниками!
- Назначайте встречи!
- Будьте в курсе событий!
- Участвуйте в конкурсах!
- Выигрывайте призы!

Доступно в **App Store**

Доступно в **Google play**

ИЩИТЕ ПРИЛОЖЕНИЕ ПО ЗАПРОСУ
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ИЛИ **АИС**

Благодарим спонсоров и партнеров за оказанную поддержку!

Золотой партнер

КРИПТОПРО
ключевое слово в защите информации

Серебряные партнеры

Компания АКТИВ 25

infotecs

Бронзовые партнеры

ФАКТОР-ТС

ASTRALINUX®

Научный партнер

НЕОБИТ

Партнеры конференции

АРПП Отечественный софт

АПКИТ

АССОЦИАЦИЯ БАНКОВ РОССИИ

ФИНТЕХ АССОЦИАЦИЯ

АССОЦИАЦИЯ РОСЭУ

ФГУП "НПП "Гамма"
Искусство Безопасности

Партнер секции

КОД БЕЗОПАСНОСТИ

Партнер Дней Вузов

CIS
Современные Информационные Системы

Информационная поддержка

ICTONLINE
ИНФОКОММУНИКАЦИИ ОНЛАЙН

ICT2GO

УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ.
ГАРАНТ
ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

BITCRYPTO NEWS

BIS JOURNAL

COINMANIA
доступно и объективно о криптовалютах и блокчейне

Единый портал Электронной подписи

InformationSecurity

19 МАРТА, ВТОРНИК. ДЕНЬ ЗАЕЗДА

15:00	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»
16:00 – 20:00	Заезд и регистрация участников, проживающих в отеле. Ужин
20:00 – 23:00	Вечерняя программа

20 МАРТА, СРЕДА. ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 09:00	Завтрак
09:00 – 10:00	Регистрация участников конференции
10:00 – 12:00	Официальное открытие конференции «РусКрипто'2019» **Пленарное заседание** *Место: Зал «Шишка»* *Подробнее: 7 стр.*
12:00 – 12:30	Кофе-брейк
12:30 – 14:00	**Круглый стол «Электронная подпись в России»** *Место: Зал «Шишка»* *Подробнее: 7 стр.*
12:30 – 14:00	**Секция «Реверсинг»** *Место: Зал «Еловый»* Ведущие: **Скляров Д.В.,** Positive Technologies **Пушкин А.,** Перспективный Мониторинг *Подробнее: 7 стр.*
14:00 – 15:00	Обед
15:00 – 17:00	**Секция «Технологии цепной записи данных и распределенных реестров в проектах реальной экономики»** *Место: Зал «Шишка»* Ведущие: **Шумский Л.С.,** Ассоциация ФинТех **Маршалко Г.Б.,** ТК26 **Сычев А.М.,** Банк России *Подробнее: 8 стр.*
15:00 – 17:00	**Секция «Цифровая криминалистика»** *Место: Зал «Еловый»* Ведущие: **Яковлев А.Н.,** Следственный комитет РФ **Чиликов А.А.,** МГТУ им. Н.Э. Баумана, Passware *Подробнее: 9 стр.*

17:00 – 17:30	Кофе-брейк
17:30 – 19:30	**Секция «Криптография и информационная безопасность в банковской сфере»** *Место: Зал «Шишка»* Ведущие: **Простов В.М.,** ФСБ России **Качалин А.И.,** Сбербанк **Голованов В.Б.,** ОАО «ИнфоТеКС» *Подробнее: 11 стр.*
17:30 – 19:30	**Секция «Криптография и криптоанализ. Часть I»** *Место: Зал «Еловый»* Ведущие: **Матюхин Д.В.,** ФСБ России **Попов В.О.,** КриптоПро, ассоциация «РусКрипто» **Жуков А.Е.,** МГТУ им. Баумана, ассоциация «РусКрипто» *Подробнее: 11 стр.*
21:00 – 23:00	Гала-ужин с вечерней программой в честь открытия XXI научно-практической конференции «РусКрипто'2019»

21 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 10:00	Завтрак
10:00 – 12:00	**Круглый стол «Переход на TLS с ГОСТ: дорожные карты и реальные перспективы»** *Место: Зал «Шишка»* *Подробнее: 13 стр.*
10:00 – 12:00	**Секция «Криптография и криптоанализ. Часть II»** *Место: Зал «Еловый»* Ведущие: **Матюхин Д.В.,** ФСБ России **Попов В.О.,** КриптоПро, ассоциация «РусКрипто» **Жуков А.Е.,** МГТУ им. Баумана, ассоциация «РусКрипто» *Подробнее: 13 стр.*
10:00 – 12:00	**Мастер-класс «Кибербразведка и методы OSINT в цифровом мире»** *Место: Зал «Сосновый»* Ведущий: **Масалович А.И.,** АИС *Подробнее: 15 стр.*
10:00 – 12:00	**Дни Вузов. Часть I** *Место: Зал «Кедровый»* Ведущие: **Белов Е.Б.,** ФУМО ИБ **Лось В.П.,** Ассоциация защиты информации **Баранов А.П.,** ГНИВЦ ФНС России *Подробнее: 15 стр.*
12:00 – 12:30	Кофе-брейк

12:30 – 14:00	**Секция «Информационная безопасность и современный маркетинг»** *Место: Зал «Шишка»* Ведущие: **Хайретдинов Р.Н.,** Attack Killer **Шабанов И.,** Anti-Malware.ru **Горелов Д.Л.,** Актив, ассоциация «Рускрипто» *Подробнее: 16 стр.*
12:30 – 14:00	**Секция «Высокоскоростные средства шифрования»** *Место: Зал «Еловый»* Ведущий: **Поташников А.В.,** ИнфоТеКС *Подробнее: 16 стр.*
12:30 – 14:00	**Мастер-класс «Как распознать психологические уловки социального инженера»** *Место: Зал «Сосновый»* Ведущая: **Ещенко Н.Г.,** АИС *Подробнее: 17 стр.*
12:30 – 14:00	**Дни Вузов. Часть II** *Место: Зал «Кедровый»* *Подробнее: 17 стр.*
14:00 – 15:00	Обед
15:00 – 16:30	**Круглый стол «Импортозамещение нового поколения: разработка и внедрение отечественного ПО в гармонии с заказчиками»** *Место: Зал «Шишка»* *Подробнее: 18 стр.*
15:00 – 16:30	**Секция «Информационная безопасность и криптография в IoT и M2M»** *Место: Зал «Еловый»* Ведущий: **Иванов В.Е.,** Актив *Подробнее: 18 стр.*
15:00 – 16:30	**Секция «Кибербезопасность в цифровом мире»** *Место: Зал «Сосновый»* Ведущий: **Зегжда П.Д.,** СПбПУ ИБКС *Подробнее: 19 стр.*
15:00 – 16:00	**Дни Вузов. Часть III** *Место: Зал «Кедровый»* *Подробнее: 20 стр.*
16:30 – 17:00	Кофе-брейк
17:00 – 19:30	**Секция «Жизненный цикл программного обеспечения информационной безопасности»** *Место: Зал «Шишка»* Ведущие: **Девянин П.Н.,** НПО РусБИТех **Аветисян А.И.,** ИСП РАН *Подробнее: 21 стр.*

17:00 – 19:30	**Секция «Перспективные исследования в области кибербезопасности»** *Место: Зал «Еловый»* Ведущий: **Котенко И.В., СПИИРАН** *Подробнее: 23 стр.*
19:30 – 23:00	Ужин. Вечерняя программа

22 МАРТА, ПЯТНИЦА. ДЕНЬ ОТЪЕЗДА

09:00 – 11:00	Завтрак
12:00	Трансфер отель «Солнечный Park Hotel & SPA» — м. Речной вокзал

ПЕРВЫЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 12:00 Пленарное заседание

Официальное открытие конференции
Приветственные слова

Роль и место криптографии в национальной программе «Цифровая экономика Российской Федерации»
Матюхин Дмитрий Викторович, *ФСБ России*

Криптография и информационная безопасность в цифровом обществе
Баранов Александр Павлович, *д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

Дайджест новостей международной криптографии
Жуков Алексей Евгеньевич, *председатель совета директоров Ассоциации «РусКрипто», к.ф.-м.н., доцент, МГТУ им. Баумана*

Алгоритмы ГОСТ в массовой криптографии: настоящее и будущее
Смышляев Станислав Витальевич, *к.ф.-м.н., директор по информационной безопасности, КриптоПро*

12:30 – 14:00 Круглый стол «Электронная подпись в России»

Уже два десятилетия в стране существует правовое и технологическое поле для использования электронной подписи. Тем не менее, актуальность вопросов применения электронной подписи в информационных системах не исчезает и даже не уменьшается. Мы на пороге очередного революционного преобразования в сфере электронной подписи. Что нас ждёт и к чему готовиться? Как трансформируются технологии применения электронной подписи? Каким станет ландшафт российского рынка в ближайшие годы?

Ведущий:
- **Малинин Юрий Витальевич,** Ассоциация РОСЭУ

Эксперты круглого стола:
- **Кирюшкин Сергей Анатольевич,** Газинформсервис
- **Маслов Юрий Геннадьевич,** КриптоПро
- **Димитров Илия,** омбудсмен по цифровой экономике

12:30 – 14:00 Секция «Реверсинг»

Что такое современный реверсинг. Исследование программно-аппаратных решений. Каковы технологии современного реверсинга, кто, как и почему сейчас этим занимается? Применение реверсинга в мирных и не очень целях. Эффективные технологии динамического и статического анализа. Технологии защиты от реверсинга.

Ведущие:
Скляров Дмитрий Витальевич, Positive Technologies
Пушкин Александр, Перспективный Мониторинг

Современный RE: кому он нужен и чем занимается

Скляров Дмитрий Витальевич, *Positive Technologies*

Информационная безопасность в целом, и Reverse Engineering в частности, являются очень динамичными областями знаний. В них постоянно появляется что-то новое. Но особенно интересно наблюдать, как меняются задачи, которые ставит перед реверсерами бизнес, нацеленный на предоставление продуктов и услуг в сфере информационной безопасности.

На сколько полезен реверс-инжиниринг при исследовании защищенности программно-аппаратных решений?

Овчинников Сергей, *Перспективный Мониторинг*

Способы исследования защищенности ПАК, кому и для чего это нужно. Для каких задач применяется реверс-инжиниринг при поиске уязвимостей.

Технологии защиты от реверс-инжиниринга

Бакаляров Михаил, *руководитель департамента разработки, Актив*

Задача защиты кода от статического и динамического анализа постоянно сталкивается с изменением внешней среды – появлением новых угроз, новых операционных систем и средств разработки. Такие события требуют качественных изменений в алгоритмах и методах защиты, что приводит к пересмотру всего подхода к защите от реверс-инжиниринга. Опыт компании с 25-летней историей создания средств противодействия анализу исполняемого кода.

15:00 – 17:00 Секция «Технологии цепной записи данных и распределенных реестров в проектах реальной экономики»

Текущие и будущие проекты применяющие технологии цепной записи данных и распределенных реестров. Использование российских криптографических стандартов в этих проектах. О регулировании и сертификации решений в этой области. Основной фокус секции будет направлен на освещение реальных решений, применению технологий блокчейн и распределенных реестров бизнесе и госуправлении.

Ведущие:

- **Сычев Артем Михайлович,** первый заместитель директора Департамента информационной безопасности Банка России
- **Шумский Лев Станиславович,** директор по информационной безопасности Ассоциации ФинТех.
- **Маршалко Григорий Борисович,** эксперт ТК26, руководитель рабочей группы «Безопасность технологий цепной записи данных и распределенных реестров»

Безопасные и расширяемые смарт-контракты в Мастерчейн

Цветков Алексей, *ведущий разработчик Мастерчейн*

В докладе будет рассмотрена реализация механизмов обновления смарт-контрактов и ролевая модель Мастерчейн. Вопрос безопасности смарт-контрактов открывает обширную область для исследований. В современных блокчейн-платформах сильно различаются подходы к реализации и условия работы контрактов. В стандарте контрактов Мастерчейн реализован механизм обновления в процессе использования. В платформе на смарт-контрактах реализована система разграничения прав доступа к конфиденциальным данным. Публикация таких данных в блокчейне недопустима, и сервисы платформы используют контракты для управления доступом к конфиденциальной информации.

Автоматическая сертификация смарт-контрактов на предмет надежности их бизнес-логики

Шишкин Евгений, *ведущий исследователь, Центр научных исследований и перспективных разработок, ИнфоТеКС*

Ряд инцидентов по взлому смарт-контрактов убедительно показал, что индустрия не умеет строить надежные смарт-контракты и остро нуждается в дополнительных средствах проверки корректности программных артефактов этого класса. В данной работе описывается концептуальное устройство инструмента автоматической сертификации смарт-контракта на предмет корректности реализуемой в них бизнес-логики по отношению к его спецификации.

Опыт внедрения Fabric для российского бизнеса и госорганизаций

Чеканов Михаил Николаевич, *генеральный директор, ООО «КБ Контракт»*

Особенности проектирования и внедрения решений на базе HyperLedger Fabric на примерах внедрений в нефтегазовой отрасли, финансовом секторе и госорганизациях. Проблемы и перспективы промышленных решений. Использование российских криптографических алгоритмов.

Применение технологии блокчейна в кибербезопасности. Реализованные проекты

Лукацкий Алексей, *независимый эксперт*

Для широкого круга специалистов, далеких от информационной безопасности, блокчейн ассоциируется только с криптовалютами. Однако эта технология находит применение в многих сферах, что демонстрируется просто взрывным ростом инвестиций в различные блокчейн-стартапы. В своем докладе Алексей Лукацкий раскроет применение блокчейна в кибербезопасности и расскажет о том, как эта технология применяется для ведения баз данных инцидентов, систем управления журналами регистрации, идентификацией пользователей, управлении конфигурациями, защиты от закладок и недекларированных возможностей и т.п.

Аспекты безопасности решений на основе распределенного реестра в свете российских требований

Багин Дмитрий Валерьевич, *заместитель начальника отдела анализа безопасности систем, КриптоПро*

Описание актуальных для существующих блокчейн-платформ вопросов безопасности, а также подходы к их приведению в соответствие действующим в Российской Федерации требованиям в области информационной безопасности на примере ПК Мастерчейн. Опыт рассмотрения решений, построенных на основе распределенного реестра, показывает, что несмотря на то, что они строятся на базе существующих криптографических алгоритмов и протоколов, эти алгоритмы и протоколы не являются в достаточной мере происследованными в классических моделях нарушителя, а потому требуют проведения отдельных исследований. Кроме того, разрабатываемые российские решения существенно перерабатываются по сравнению с массовыми платформами для обеспечения принципиально более высокого уровня информационной безопасности – в частности, в таких аспектах, как управление ключами, защита от несанкционированного доступа, и порядок управления пользователями.

15:00 – 17:00 Секция «Цифровая криминалистика»

Необходимость развития методов цифровой криминалистики обусловлена повсеместным проникновением информационных технологий в повседневную жизнь обычного человека. 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 иных практических аспектах цифровой криминалистики.

Ведущие:

- **Яковлев Алексей Николаевич,** Следственный комитет РФ
- **Чиликов Алексей Анатольевич,** МГТУ им. Баумана, Passware

Современные принципы шифрования Android-устройств и подходы к их расшифровыванию

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

Android-устройства предоставляют различные механизмы защиты данных. В частности, на любом современном Android смартфоне по умолчанию включено шифрование пользовательских данных, причем ключ шифрования криптографически связан с hardware-backed keystore. Таким образом без доступа к hardware-backed keystore вычислительно невозможно расшифровать пользовательские данные даже если известен или не задан пароль блокировки устройства. Тем не менее в определенных случаях расшифровывание данных все же возможно. Ключевым здесь является "в определенных случаях" - производители специализированного ПО порой делают громкие заявления порождая ряд слухов вокруг различных методов, например вокруг Emergency Download Mode (EDL). В докладе будут детально описаны подходы к расшифровыванию пользовательских данных с указанием случаев в которых они применимы.

Особенности криминалистического анализа некоторых смартфонов на базе чипсетов Qualcomm

Чиликов Алексей Анатольевич, *к.ф.м.н., доцент МГТУ им. Баумана, директор по науке, Passware*

Хоруженко Георгий Игоревич, *специалист отдела исследований, Passware*

Доклад посвящен системе полнодискового шифрования данных современных смартфонов под управлением ОС Android версии 5 и выше. Интерес к данной теме обусловлен применением программно-аппаратных механизмов защиты при вычислении ключа шифрования и/или непосредственно шифрования разделов с данными пользователя. Подобные криптографические системы значительно затрудняют криминалистическую экспертизу и, зачастую, делают невозможным получение доступа к пользовательским данным.В докладе особое внимание уделяется особенностям реализации подобных механизмов в смартфонах на базе чипсетов Qualcomm. В ряде случаев возможно извлечь данные, необходимые для организации переборной атаки без участия смартфона, и, в случае успеха, расшифровать защищенный раздел.

Автоматизированное рабочее место эксперта компьютерно-технической экспертизы: современный взгляд

Абрамец Алексей, *старший эксперт отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики (Криминалистического центра) СК России*

В мире существует большое разнообразие подходов к организации рабочего места эксперта, исследующего цифровую информацию, основанных как на идее использования портативного перемещаемого оборудования, так и на идее использования стационарного оборудования, или вообще - их комбинации. Особое внимание при этом должно быть уделено принципам подбора экспертного программного обеспечения, которое в совокупности должно позволять решать наиболее часто встречающие экспертные задачи. Проблеме комплектования рабочего места эксперта компьютерно-технической экспертизы, поддержания его в актуальном состоянии посвящен доклад.

Журналы компьютеризированных блоков автомобиля как объект криминалистического исследования

Королев Михаил, *ведущий специалист инженерно-технического отдела ООО «Тойота Мотор»,*
Бережной Игорь, *старший эксперт отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики (Криминалистического центра) СК России*

Доклад посвящен исследованию данных, формируемых блоком управления подушками безопасности автомобилей марки «Toyota» и извлекаемых средствами аппаратно-программного комплекса «Bosch Crash Data Retrieval». Технический отчет получен. Какие сведения он содержит и о чем? Как эти сведения могут использоваться в судопроизводстве? Ответы на эти вопросы представлены в докладе.

Криминалистический анализ исполнимых файлов при помощи общедоступного программного обеспечения

Вавилин Андрей, *старший эксперт отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики (Криминалистического центра) СК России*

Все привыкли к тому, что задача криминалистического анализа исполнимых файлов решается только в отношении предположительно вредоносных программ. Это не совсем так. Даже задача создания доверенной программной среды может потребовать проведения криминалистического анализа исполнимых файлов привычных и часто используемых программ. А иногда такая задача встает перед экспертом просто в силу специфики спорной ситуации, в которой использовался исполнимый файл, и которая стала предметом судебного разбирательства. Сложно ли проводить такой анализ? Для ответа на этот вопрос в докладе будут представлены как практические аспекты исследования исполнимых файлов, так и описание общедоступного программного обеспечения, необходимого для такого исследования.

Методика компьютерно-технического исследования - международный и отечественный подходы

Яковлев Алексей, *заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики (Криминалистического центра) СК России; доцент кафедры «Юриспруденция, интеллектуальная собственность и судебная экспертиза» МГТУ им. Н.Э. Баумана.*

Знаете ли Вы все пять возможных подходов к обеспечению контроля качества компьютерно-технического исследования? А как же тогда урегулируете в суде разногласия по поводу различия результатов двух компьютерно-технических экспертиз, проведенных по одному и тому же объекту исследования? Как решаете вопрос доверия к самостоятельно полученным результатам, или схожим результатам, полученным другим экспертом? О паспортизированных методиках экспертного исследования, методиках решения типовых экспертных задач, регламенте судебной компьютерно-технической экспертизы, стандартах организации выполнения компьютерно-технической экспертизы, взаимодействии с производителями экспертного оборудования и программного обеспечения – этот доклад.

Нетипичные экспертизы и исследования - задачи в рамках арбитража

Земцов Анатолий Павлович, *генеральный директор Ассоциации ЭКСПИТ*
Яковлев Илья Алексеевич, *эксперт Digatal Forensic Center*

Доклад будет посвящен применению методов компьютерной криминалистики, достаточно хорошо известных в рамках уголовного судопроизводства, в такой сфере, как арбитражный процесс. Количество дел с «IT-элементом» в арбитражных судах все время возрастает, поэтому возрастает и важность таких методик – они постепенно становятся обязательными. Что подтверждается, в том числе, решениями Суда по интеллектуальной собственности РФ.

17:30 – 19:30 Секция «Криптография и информационная безопасность в банковской сфере»

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

Ведущие:
- **Простов Владимир Михайлович,** ФСБ России
- **Качалин Алексей Игоревич,** исполнительный директор Центра Киберзащиты, Сбербанк
- **Голованов Владимир Борисович,** ИнфоТеКС

Рекомендации по применению российской криптографии в банковской отрасли
Простов Владимир Михайлович, *ФСБ России*

Тема доклада уточняется
Качалин Алексей Игоревич, *исполнительный директор Центра Киберзащиты, Сбербанк*

Вопросы применения и эксплуатации новых технологий электронной подписи
Левиев Дмитрий Олегович, *НП ПСИБ, МГТУ им. Н.Э.Баумана*

Нормативно-техническое регулирование в области биометрии. Практическая значимость стандартов и новые направления в их разработке
Мамаев Василий Юрьевич, *заместитель директора некоммерческого партнерства «Русское биометрическое общество»*

Методы оценки доверия к результатам первичной идентификации
Сабанов Алексей Геннадьевич, *к.т.н, эксперт ISO, доцент МГТУ им.Баумана*

Противодействие онлайн-мошенничеству: интересные кейсы за 2018 год
Крылов Павел Владимирович, *руководитель направления по защите от онлайн-мошенничества, Group-IB*

17:30 – 19:30 Секция «Криптография и криптоанализ. Часть I»

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

Обзор результатов анализа шифра «Кузнечик»
Маршалко Григорий Борисович, *ТК 26*
Бондаренко Александр Иванович, *ТК 26*
Агафонова Анастасия Вячеславовна, *ТК 26*
В обзорном докладе планируется осветить некоторые опубликованные результаты криптографических исследований блочного шифра «Кузнечик», определённого национальным стандартом ГОСТ Р 34.12-2015 и межгосударственным стандартом ГОСТ 34.12-2018.

«КУЗНЕЧИК» - оптимизированные внедрения на ПЛИС и микроконтроллерах и их сопротивление анализу «DPA»

Delaunay Cédric, *ENSTA Bretagne/ ESIEA, (C + V) ^ O Lab, France*
Истомин Александр Александрович, *ФГУП «НПП «ГАММА»*
Filiol Eric, *ESIEA, (C + V) ^ O Lab, Laval, France*

Криптографические алгоритмы – это основной элемент безопасности. Если мы будем рассматривать работу алгоритма, реализованного аппаратно, то будет присутствовать определённый разрыв между математической моделью оцениваемой безопасности и фактической. Данная работа ориентирована на внедрение и анализ атак для аппаратных реализации на ПЛИС и микроконтроллерах двух основных блочных шифров: AES (Стандарт НИСТ) и «Кузнечик» (ГОСТ Р 34.12-2015).
После краткого обзора всех аппаратных атак на оба шифра, мы выберем рабочую модель атаки и меры противодействия на ПЛИС и микроконтроллеры, покажем реализацию атаки с использованием относительно дешёвого подхода анализа «DPA» (Дифференциальной атаки по энергопотреблению), чтобы увидеть, какой алгоритм чувствителен к ней, и насколько меры противодействия будут оказывать влияние на общий размер внедрения и производительность.

Логический криптоанализ функции хэширования ГОСТ Р 34.11-2012

Маршалко Григорий Борисович, *ТК 26*
Мхитарян Артем Гагикович, *КриптоПро, МГУ им. Ломоносова*

В данной работе рассмотрен подход к криптоанализу хэш-функций, базирующийся на современных эвристических методах решения задач о выполнимости КНФ или SAT-задач.

О параметрах генератора раундовых ключей алгоритма 2-ГОСТ

Коренева Алиса Михайловна, *к.ф.-м.н., ведущий системный аналитик ООО «Код Безопасности»*
Тулебаев Азат Ирикович, *программист,Код Безопасности*
Фомичёв Владимир Михайлович, *д.ф.-м.н., научный консультант, Код Безопасности, НИЯУ МИФИ, Финансовый университет при Правительстве РФ, ФИЦ ИУ РАН*

В 2014 году была представлена низкоресурсная реализация ГОСТ 28147-89 под названием 2-ГОСТ. Несмотря на достоинства, схема имела потенциал в части усиления криптографической стойкости, в том числе за счёт модификации ключевого расписания. На конференции РусКрипто'2018 предложен новый алгоритм генерации раундовых ключей для 2-ГОСТ на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32. Вместе с тем, параметры обратной связи регистра не были достаточно обоснованы. Доклад посвящен определению наилучших (или близких к наилучшим) трех точек съема функции обратной связи регистра сдвига и обоснованию предложенного решения.

Принципы построения отечественных криптонаборов для TLS 1.3

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

Доклад посвящен отечественным криптонаборам для протокола TLS 1.3, разрабатываемым в рамках деятельности РГ 2.1 по сопутствующим криптографическим алгоритмам и протоколам ТК 26. Основные особенности режима работы TLS 1.3, определяемого данными криптонаборами, описываются с точки зрения устойчивости к известным методам проведения атак, с позиций доказуемой стойкости, а также соответствия российским требованиям по информационной безопасности.

Криптографические механизмы защищенного взаимодействия

Нестеренко Алексей Юрьевич, *к.ф.-м.н., доцент кафедры «Компьютерная безопасность» МИЭМ НИУ ВШЭ*

Доклад будет посвящен рассмотрению методических рекомендаций «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств». Рекомендации содержат в себе описание протокола выработки общих ключей, транспортного протокола, а также механизмов выработки и преобразования ключевой информации, используемой для шифрования и имитозащиты передаваемой информации. Будут рассмотрены свойства безопасности, обеспечиваемые данными криптографическими механизмами, их эксплуатационные особенности и проведено сравнение с другими протоколами, разрабатываемыми в рамках деятельности ТК26. Будут отмечены как достоинства, так и недостатки разработанных рекомендаций.

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 12:00 Круглый стол «Переход на TLS с ГОСТ: дорожные карты и реальные перспективы»

За прошедший год произошло немало событий, связанных с использованием отечественной криптографии в российском сегменте Интернет: разработка дорожных карт по переходу на ГОСТ в национальном сегменте сети Интернет в рамках программы «Цифровая экономика» и Поручения Пр-1380, проектирование системы Национального Удостоверяющего Центра и сопутствующей инфраструктуры, появление пилотных зон на массовых web-ресурсах с одновременной поддержкой российских и зарубежных криптонаборов TLS. Кроме того, Росстандартом утвержден и введен с 1 февраля 2019 года в действие TLS 1.2 с новыми алгоритмами шифрования, в ТК 26 завершается разработка российских криптонаборов TLS 1.3.
Но все ли готово к переходу существенной части российского сегмента Интернет на отечественную криптографию на практике? Есть ли для этого удобные сертифицированные криптосредства для клиентской части, можно ли обеспечить удобным образом выдачу российских TLS-сертификатов, все ли теперь готово в части серверных решений для того плавного перехода на использование российских алгоритмов, о котором говорили участники круглого стола год назад?

Ведущий:
- **Горелов Дмитрий Львович,** Актив

Эксперты круглого стола:
- **Елистратов Андрей Алексеевич,** ТК 26
- **Смышляев Станислав Витальевич,** КриптоПро
- **Гусев Дмитрий Михайлович,** ИнфоТеКС
- **Устинов Игорь Геннадьевич,** Криптоком
- **Пьянченко Андрей Андреевич,** ФГБУ НИИ «Восход»
- **Кузьмичев Андрей Юрьевич,** RU-CENTER
- **Петлинский Павел Валентинович,** Rambler
- **Малинкин Дмитрий Викторович,** Спутник

10:00 – 12:00 Секция «Криптография и криптоанализ. Часть II»

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

BSEA – метод построения поточного шифра с закладкой (BSEA 1 - A Stream Cipher Backdooring Technique)

Eric Filiol, *ESIEA, (C + V) ^ O Lab, Laval, France*

Внедрение закладок в поточные шифры было активным направлением после Второй мировой войны вплоть до наступления эпохи блочных шифров в начале 90-х. В большинстве случаев алгоритмы были секретные или проприетарные. Версии с закладками, в первую очередь, создавались ради экспортных версий. К настоящему времени нет технической информации о том, как именно строились закладки в поточных шифрах. В настоящем докладе мы представим краткий обзор возможных методов внедрения закладок в поточные шифры и представим BSEA-1 (Backdoored Stream Encryption Algorithm), чтобы проиллюстрировать один из наиболее распространенных методов, использовавшихся в 80-е и 90е. BSEA-1 использует ключ длины 120 бит.

Внедрение закладок в генератор ключей RSA

Маркелова Александра Викторовна, *к.ф.-м.н., МГТУ им. Баумана, НТЦ Альфа-Проект*

В докладе описывается класс асимметричных закладок в генераторе RSA-ключей и оценивается возможность реализации предложенных алгоритмов на малоресурсных платформах.

О решении систем уравнений одного класса статистическими методами

Ошкин Игорь Борисович, *к.ф.-м.н., начальник отдела, КриптоПро*
Попов Владимир Олегович, *к.ф.-м.н., директор по научной работе, КриптоПро*

Приводится обзор публикаций по теме Side-Channel Attacks. На их основе формулируется математическая постановка задачи для класса систем уравнений. Приводятся параметры решения этих систем статистическими методами.

О подстановочных гомоморфизмах *-марковских XSL-алгоритмов блочного шифрования с неабелевой группой наложения ключа

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

Описываются свойства *w-марковских алгоритмов блочного шифрования и преобразований для неабелевой группы наложения ключа (X,*). Получены ограничения на строение группы, порождённой множеством частичных раундовых функций, вытекающие из условия сохранения каждой такой функцией нетривиального разбиения W. Указана связь между существованием подстановочного гомоморфизма и *w-марковостью алгоритма.

О подходах к обеспечению достаточного уровня стойкости в части конфиденциальности при малоэнтропийных предварительно распределенных секретах

Варфоломеев Александр Алексеевич, *к.ф.-м.н., доцент, МГТУ, МИФИ, РУДН*

Обсуждение проблемы обеспечения достаточного уровня стойкости в части конфиденциальности передаваемой информации при использовании общих секретов длины 56 бит или менее. Данная проблема является актуальной при анализе криптографических протоколов – например, одним из важных путей развития протоколов TLS и IPsec является внедрение аутентификации с использованием пароля на основе одного из протоколов семейства PAKE (Password Authenticated Key Exchange), а использование PSK (pre-shared key) длины 118 бит является де-факто стандартом для ряда приложений IPsec. Обеспечение должного уровня конфиденциальности передаваемых данных обеспечивается за счет выработки общих ключей достаточной длины с аутентификацией субъектов под защитой малоэнтропийных секретов, с обоснованием стойкости получающихся схем в актуальных моделях нарушителя. В докладе проводится обзор существующих механизмов для решения данной задачи, а также развивается начатое в докладе автора на конференции РусКрипто 2018 обсуждение альтернативного подхода с помощью концепции асимметрично выполнимых криптосистем, теперь применительно к асимметричной криптосистеме Эль-Гамаля. Кроме того, предлагается метод преобразования классического шифра в асимметрично выполнимый.

Влияние теории квантовых вычислений на развитие современной криптографии

Денисенко Денис Витальевич, *МГТУ им. Баумана*
Никитенкова Марина Викторовна, *ТК 26*
Поляков Михаил Вадимович, *МГТУ им. Баумана*
Рудской Владимир Игоревич, *ТК 26*

Обзор применения квантовых алгоритмов (Гровера, Саймона, комбинации Гровера и Саймона, HHL) в задачах криптографического анализа: восстановление ключа по парам блоков открытого и шифрованного текстов; квантовый метод согласования; квантовый метод связанных ключей; квантовый линейный и разностный метод (поиск разностных соотношений, восстановление ключа); поиск коллизий и второго прообраза криптографических хэш-функций; решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, МРКС. Оценки необходимого количества логических кубитов и квантовых вентилей для реализации алгоритмов блочного шифрования в виде квантовых схем на примере Simplified-DES, ГОСТ Р 34.12-2015. Обзор современных достижений в области создания квантовых компьютеров. Основные выводы из отчета Quantum Computing: Progress and Prospects, 2018.

Тенденции развития постквантовой криптографии

Гребнев Сергей Владимирович, *ТК 26*

В обзорном докладе планируется осветить основные тенденции постквантовой криптографии и связанные с этим вопросы: обзор основных угроз классическим криптосистемам с открытым ключом, обусловленных развитием квантовых вычислений; обзор основных синтезных методов постквантовой криптографии; стандартизация постквантовых схем, в том числе в работе IETF, опыт внедрения постквантовой криптографии в практические решения (ISARA и др.); конкурс NIST, его участники, итоги 1 этапа, проблемы, вопросы и сомнения.

10:00 – 12:00 Мастер-класс «Кибербразведка и методы OSINT в цифровом мире»

В цифровом мире меняются как подходы работы с информацией, так и сами источники данных. Теперь данные для анализа и принятия решений можно получать не только из сайтов, поисковых систем и баз данных, но и от миллиардов «умных» устройств IoT, огромного количества портативных гаджетов и мобильных приложений, из соцсетей, мессенджеров и «даркнета».Как собирать нужные данные и отфильтровывать их от «цифрового шума»? Как превратить «сырые» данные в полезную информацию, содержащую ценные сведения о людях, событиях или компаниях? Как эффективно использовать автоматизированные системы анализа данных? Об этом пойдет речь на мастер-классе Андрея Масаловича.

Ведущий:
Масалович Андрей Игоревич - к.ф-м.н., ведущий эксперт по конкурентной разведке Академии Информационных Систем, президент Консорциума Инфорус, лауреат стипендии РАН «Выдающийся ученый России». Подполковник ФАПСИ в отставке.

10:00 – 12:00 Дни Вузов. Часть I. Секция «Проблемы профессионального образования в области информационной безопасности»

Ведущие:
- **Белов Евгений Борисович,** Заместитель председателя Совета и президиума Совета ФУМО ИБ
- **Лось Владимир Павлович,** д.в.н., профессор, Президент Ассоциации защиты информации
- **Баранов Александр Павлович,** д.ф-м.н., заведующий кафедрой «Информационная безопасность», НИУ ВШЭ

Проблемы профессионального образования в области информационной безопасности
Белов Евгений Борисович, *Заместитель председателя Совета и президиума Совета ФУМО ИБ*

Проблемы кадрового обеспечения отрасли информационной безопасности
Лось Владимир Павлович, *д.в.н., профессор, Президент Ассоциации защиты информации, директор Центра исследования проблем кадрового обеспечения отрасли информационной безопасности ФГБОУ ВО «МИРЭА — Российский технологический университет»*

Новые вызовы безопасности и компетенции специалистов. Интеграция науки, образования, бизнеса
Зегжда Петр Дмитриевич, *д.т.н., проф. кафедры «Информационная безопасность компьютерных систем», Санкт-Петербургский политехнический университет Петра Великого, научный руководитель ООО «НеоБИТ»*

Автономность российского сегмента сети интернет как система технических требований
Сухов Андрей Михайлович, *Профессор кафедры суперкомпьютеров и общей информатики, д.т.н. Самарский университет*

О разработке примерной программы профессиональной переподготовки по информационной безопасности
Шапошников Виталий Анатольевич, *к.ф.-м.н., доцент, Заместитель начальника УМО Академии Информационных Систем*

Сотрудничество «Кода безопасности» с вузами: работодатель, технологический и образовательный партнер
Царькова Оксана Владимировна, *канд. пед. наук, Начальник отдела разработки учебной документации Компании «Код Безопасности»*

Опыт сотрудничества компании ИнфоТеКС с образовательными учреждениями
Чефранова Анна Олеговна, *д-р пед. наук, Исполнительный директор Компании «ИнфоТеКС»*

12:30 – 14:00 Секция «Информационная безопасность и современный маркетинг»

Секция, посвященная технологическому маркетингу для руководителей и маркетологов ИТ-компаний и заказчиков. Как доносить информацию, как ее дозировать, как привлекать внимание? Как создавать, публиковать и распространять информацию о сложных технических продуктах, чтоб ее читали и ей доверяли. Многие продукты информационной безопасности требуют глубоких технических знаний в узкой области. Где золотая середина между большим докладом на технической конференции для нескольких десятков специалистов и рекламной агиткой, и нужна ли эта золотая середина?

Ведущие:

- **Хайретдинов Рустэм,** Attack Killer
- **Шабанов Илья,** Anti-Malware.ru
- **Горелов Дмитрий,** Актив, Ассоциация РусКрипто

12:30 – 14:00 Секция «Высокоскоростные средства шифрования»

С каждым годом увеличивается ширина каналов связи и растут объемы передаваемой информации. Обеспечение информационной безопасности частных и государственных центров обработки данных требует средств высокоскоростного шифрования. Какие продукты, поддерживающие российскую криптографию, могут предложить разработчики, какие новые решения и подходы?

Ведущий:

- **Поташников Александр Викторович,** Заместитель директора Центра разработок ОАО «ИнфоТеКС»

Аппаратная криптографическая защита данных в высокоскоростных сетях Ethernet

Иванов Александр Геннадьевич, *Ассоциация «РусКрипто», Российская Корпорация Средств Связи*

В докладе обсуждаются особенности требований к средствам защиты данных на сетевом (Ethernet – Layer 2), транспортном (IP - Layer 3) и прикладном (Layers 4-7) уровнях. В кратком обзоре представленных на рынке сетевых криптографических средств защиты информации зарубежных и отечественных производителей производится сравнение технических характеристик оборудования, приводятся примеры внедрения на территории Российской Федерации и рассматриваются перспективы развития.

Высокоскоростной шифратор

Кобзев В.Н., Колыбельников Александр Иванович, *Код Безопасности*

В докладе приводится описание программно-аппаратных решений, позволивших реализовать шифратор с пропускной способностью до 20Гб/сек, архитектурных особенностей и достигнутых результатов производительности.

Некоторые особенности архитектуры высокоскоростных средств шифрования для обеспечения криптографической защиты центров обработки данных

Мареева Елена Владимировна, *Системы практической безопасности*

В докладе рассматриваются достоинства и недостатки существующих классов средств криптографической защиты данных, передаваемых между центрами обработки данных. Даётся определение нового класса устройств и его характеристик, исходя из требований криптографической защиты ЦОД. Рассматриваются архитектурные особенности устройств нового класса.

Способ снижения накладных расходов на передачу информации в канале между скоростными шифраторами

Калистру Илья Иванович, Бородин Михаил Алексеевич, *ИнфоТеКС*

В докладе представлен протокол аутентифицированного шифрования канального уровня, решающий задачи минимизации накладных расходов при передаче данных. Основным криптографическим механизмом является режим GCM с алгоритмом шифрования «Кузнечик». Для возможности применения на российском рынке также рассмотрен модифицированный вариант протокола с режимом «Нефрит». Проведено теоретическое и практическое сравнение упомянутых протоколов.

12:30 – 14:00 Мастер-класс «Как распознать психологические уловки социального инженера»

Социальная инженерия становится угрозой N1 при обеспечении личной и корпоративной безопасности. Атака методами социальной инженерии идет в обход аналитических инструментов разума. Она воздействует на эмоциональную сферу, привычно подавляемую у людей, занятых умственным трудом. Высокий интеллект не спасает, потому что методы социальной инженерии направлены на разрушение шаблонов разумного поведения, страхи и приспособительные рефлексы. Защититься от таких атак непросто, поскольку жертвы могут не подозревать, что ими манипулируют. Необходимо изучить психологическую природу и разновидности атак СИ, распознавать манипуляции и учиться правильно противодействовать им.
В ходе мастер-класса будут рассмотрены основные приемы социальной инженерии для выведывания личной информации, приемы выявления настораживающих признаков поведения, техники распознавания вербальных и невербальных признаков психологического воздействия при телефонном общении и проанализированы некоторые типичные психологические уловки собеседника.

Ведущая:

- **Ещенко Наталья Геннадьевна** - к.пс.н., автор и преподаватель курсов в АИС, специалист по психологической подготовке к экстремальным видам деятельности, член Профессиональной психотерапевтической лиги.

12:30 – 14:00 Дни Вузов. Часть II.

О почти совершенных нелинейных преобразованиях и разделяющем свойстве мультимножеств
Сорокин Михаил Артемович, *кафедра «Криптология и кибербезопасность», НИЯУ МИФИ*

Об одном способе противодействия MITM – атакам на основе протоколов, использующих общую память Отправителя и Получателя в модели секретной связи
Александров Алексей Викторович, Сорокин Илья Игоревич, *кафедра «Информатики и защиты информации», Владимирский Государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых*

Исследование алгоритмов развертывания ключа блочных шифрсистем, предназначенных для использования в средах с ограниченными ресурсами, с помощью методологии SAT
Слонкина Ирина Сергеевна, *кафедра «Криптология и кибербезопасность», НИЯУ МИФИ*

Прототип системы защиты программного обеспечения от анализа на основе применения технологии виртуализации исполняемого кода
Маркин Дмитрий Олегович, Вихарев Антон Николаевич, *Академия ФСО России*

Однонаправленные шлюзы передачи данных. Защита критической инфраструктуры
Совалов Роман Валерьевич, *Генеральный директор компании «Современная интеграция»*

Привратник – наложенное средство аутентификации в средах виртуализации
Совалов Роман Валерьевич, *Генеральный директор компании «Современная интеграция»*

15:00 – 16:30 Круглый стол «Импортозамещение нового поколения: разработка и внедрение отечественного ПО в гармонии с заказчиками»

Тема цифрового суверенитета красной строкой вошла в новую стратегию развития ИТ-отрасли; вышли новые директивы Правительства, форсирующие импортозамещение в госкомпаниях, а не только в госорганах. Государство все сильнее обозначает необходимость избавиться от технологической зависимости и санкционной уязвимости используемых в стране ИТ.
Что делать заказчикам и российским разработчикам в этих условиях, чтобы не спорить, а грести в одной лодке? Достаточно ли у нас в стране российских продуктов, чтобы решить задачу импортозамещения, по крайней мере, в критических областях и госсекторе? Какие сегменты ПО приоритетны для импортозамещения? Что необходимо предпринять, чтобы российских продуктов не только стало больше, но и их возможности удовлетворяли российских заказчиков? Как превратить разрозненные российские продукты в интегрированные стеки комплексных решений? Эти и другие вопросы превращения карты российских ИТ в полноценный отраслевой ландшафт мы обсудим на круглом столе.

Ведущий:
- **Рубанов Владимир Васильевич,** управляющий директор «Росплатформа»

К участию в дискуссии приглашены:
- **Массух Илья Иссович,** Директор Центра компетенции по импортозамещению в сфере ИКТ, Президент Фонда информационной демократии
- **Зубарев Николай Вадимович,** директор по направлению «Информационная безопасность» АНО «Цифровая Экономика»
- **Баранов Александр Павлович,** заместитель генерального директора АО «Главный научный инновационный внедренческий центр» (АО «ГНИВЦ» ФНС России)
- **Кравченко Константин,** советник генерального директора АО «Научно-производственная корпорация «Уралвагонзавод»
- **Маслов Юрий Геннадьевич,** коммерческий директор компании «КриптоПро»
- **Гусев Дмитрий Михайлович,** заместитель генерального директора компании «ИнфоТеКС»
- **Лашин Ренат,** исполнительный директор АРПП «Отечественный софт»
- **Макаров Валентин,** президент НП «РУССОФТ»
- **Комлев Николай Васильевич,** Ассоциация «АПКИТ»
- **Голов Андрей Викторович,** Генеральный директор, Код безопасности

15:00 – 16:30 Секция «Информационная безопасность и криптография в IoT и M2M»

Секция посвящена новому, быстрорастущему сегменту информационной безопасности. Классические подходы и привычные технологии информационной безопасности мало пригодны для интернета вещей. В докладах секции пойдет об адаптированных или заново разработанных решениях под задачи IoT и M2M.

Ведущий:
- **Иванов Владимир Евгеньевич,** директор по развитию, Актив

Особенности использования российской криптографии в протоколах обмена данными с приборами учёта IEC 62056 (DLMS/COSEM) и СПОДЭС

Костромин Игорь Сергеевич, *начальник отдела встраиваемого программного обеспечения ЦП ПО, ПКК МИЛАНДР*
Рассмотрены конкретные подходы к адаптации стандартов DLMS/COSEM (а так же СПОДЭС) к использованию российских криптографических алгоритмов в соответствии с действующими нормативными документами Российской Федерации, выработанные в рамках деятельности рабочей группы «криптографические механизмы для M2M и индустриальных систем» подкомитета № 4 ТК 26.

Аутентификация в IoT. Взгляд на традиционные схемы, поиск и устранение слабых мест

Лазарев Алексей Станиславович, *менеджер проектов, Актив*

Межмашинное взаимодействие, как один из столпов концепции интернета вещей, покидает свою колыбель - производственные площадки и приходит в новые отрасли. В новых условиях нет помещений, закрытых от посторонних взглядов. Каналы связи и устройства зачастую открыты для физического доступа. Это вынуждает нас уделять особое внимание защите оборудования и каналов связи от внешних атак, обеспечивать безопасность данных и проверку подлинности взаимодействующих объектов. Могут ли помочь старые отработанные приемы и алгоритмы там, где отсутствует главный участник процесса аутентификации – человек? Как адаптировать проверенные методы к новым реалиям?

Протокол защищенного обмена для индустриальных систем (CRISP 1.0)

Шемякина Ольга Викторовна, *ОАО «ИнфоТеКС»*

Доклад посвящен особенностям нового протокола CRISP – CRyptographic Industrial Security Protocol – разработанного для применения в индустриальных системах. Рассмотрены механизмы, позволяющие снижать требования к энергопотреблению, вычислительным ресурсам устройств, реализующих данный протокол, уменьшать время обработки пакета, снижать нагрузку на используемые каналы связи по сравнению с существующими протоколами. Приводится текущее состояние работ по стандартизации данного протокола, а также перспективы его развития и использования.

Применение российской криптографии и технологий M2M, IoT для решения проблем безопасности СКУД на объектах КИИ

Кожемякин Никита, *управляющий директор ГК ISBC*

Как защитить устройства IIoT/M2M в соответствии с законодательством РФ

Сорокина Марина, *руководитель направления развития продуктов ОАО «ИнфоТеКС»*

Презентация посвящена подходам защиты устройств IIoT и M2M систем. Будут рассмотрены основные вектора атак на такие устройства и обозначены возможные способы по их защите. Будет приведено сравнение вариантов реализаций обозначенных способов внутри устройств IIoT и M2M при использования встраиваемых средств защиты информации и при использовании концепции secure-by-design. Автор поделится практическим опытом по разработке продуктов компании ИнфоТеКС в соответствии с законодательством РФ для реализации в устройствах IIoT и M2M данных подходов к защите.

15:00 – 16:30 Секция «Кибербезопасность в цифровом мире»

Повсеместная доступность сети Интернет и универсальность сетевых протоколов связали в единую сеть все компьютерные системы производственной, энергетической, бытовой, финансовой и общественно-политической сферы и позволили осуществить транзитивное замыкание всех систем управления в единое киберпространство. Возникло понятие кибербезопасности (т.е. безопасности киберпространства), отражающее появление нового класса угроз, направленных не на несанкционированный доступ или искажение информации, а на получение контроля над физическими устройствами, в первую очередь в промышленности и энергетике, а также манипулирования людьми в социально-политических сферах. Какие новые угрозы порождает глобальная цифровизация? Достаточно ли существующих средств защиты или необходимо разрабатывать новые? На эти и многие другие вопросы постараются ответить в своих докладах участники данной секции.

Ведущий:

- **Зегжда Петр Дмитриевич,** д.т.н., проф. кафедры «Информационная безопасность компьютерных систем», Санкт-Петербургский политехнический университет Петра Великого, научный руководитель ООО «НеоБИТ»

Обеспечение кибербезопасности при цифровизации производства

Москвин Дмитрий Андреевич, *к.т.н., Санкт-Петербургский политехнический университет Петра Великого*

Переход к цифровому производству на промышленных предприятиях сопряжен со множеством трудностей не только технологического характера, но и с появлением новых угроз кибербезопасности. Поэтому требуется пересмотр модели угроз и переоценка эффективности применяемых средств защиты, которых оказывается недостаточно. Для обеспечения кибербезопасности цифрового производства требуются не просто дополнительные программно-технические средства, а разработка нового подхода. В качестве такого подхода авторами доклада предлагается использовать концепцию децентрализованных сетей и их технологий по обеспечению конфиденциальности, целостности и киберустойчивости функционирования.

Выявление вредоносного программного обеспечения в условиях наличия механизмов самозащиты на основе анализа его функциональных возможностей

Жуковский Евгений Владимирович, *Санкт-Петербургский политехнический университет Петра Великого.*

В докладе рассматриваются существующие подходы к выявлению вредоносного программного обеспечения и имеющиеся ограничения в их практическом применении. Предлагается подход, направленный на обнаружение в программном коде операций, приводящих к нарушению информационной безопасности системы в условиях наличия в коде механизмов уклонения от анализа. В качестве признаков, идентифицирующих попытки сокрытия вредоносного поведения программы, используются метрики, связанные с достижимостью потенциально опасных операций. Для обеспечения полноты анализа предлагается использовать динамическое символьное выполнение, позволяющее определить условия достижения требуемых участков программы. Для оптимизации процесса поиска путей исполнения программы, приводящих к выполнению вредоносных операций, применяются методы машинного обучения с подкреплением.

Сравнительный анализ подходов обеспечения безопасности устройств интернета вещей

Макаров Александр Сергеевич, *ООО «НеоБИТ»*

Каждый производитель систем умного дома и устройств интернета вещей предлагает свои узлы и протоколы для коммуникаций. Это значит, что нет четкой системы и общепринятых стандартов, а, следовательно, эта область мало изучена и имеет ряд проблем с безопасностью. Для решения вопросов безопасности применяют как программные, так и аппаратные средства. В докладе будут рассмотрены основные средства программного и аппаратного обеспечения безопасности, а также предложены методы повышения отказоустойчивости элементов умного дома.

Обеспечение безопасности динамических сетей Интернета вещей на основе децентрализованных моделей доверия

Бусыгин Алексей Геннадиевич, *ООО «НеоБИТ»*

Централизованные модели доверия в общем случае не применимы для Интернета вещей из-за его масштабов, открытой и децентрализованой архитектуры. В частности, для реализации динамических сетей (MANET, VANET и др.) Интернета вещей необходимы инструменты сравнения и выбора подходящей децентрализованной модели доверия. В статье рассматриваются децентрализованные модели доверия, применимые для данной предметной области, приводится их классификация и описание особенностей позволяющее подобрать подходящую модель для обеспечения защищённости различных типов динамических сетей Интернета вещей.

Оценка безопасности программного обеспечения с использованием сверточного представления журнала обращений к оперативной памяти

Самарин Николай Николаевич, *ФГУП «НИИ «Квант»*

Задача выявления потенциально опасного поведения программного обеспечения (ПО) по-прежнему занимает важнейшее место в теории защиты информации. При этом технологии и подходы, используемые вредоносным программным обеспечением (ВПО), для которого характерно отсутствие исходных кодов для анализа, не стоят на месте и прогрессируют наряду со средствами защиты. Это приводит к острой необходимости создания эффективных средств, опирающихся в первую очередь не на анализ исходного кода, а на выявление аномалий в поведении ПО.

15:00 – 16:00 Дни Вузов. Часть III.

Всё по закону! Особенности подключения к Единой биометрической системе

Александров Алексей, *директор по информационной безопасности ООО «АйДиСистемс»*

Шифрование на 2-м уровне эталонной сетевой модели в сетях Ethernet

Рожнов Михаил, *технический директор компании «CIS-Crypto»*

17:00 – 19:30 Секция «Жизненный цикл программного обеспечения информационной безопасности»

Секция посвящена вопросам реализации ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения» и «Требований по безопасности информации, устанавливающие доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденных приказом ФСТЭК России от 30.07.2018 № 131, на примере отечественных защищенных операционных систем и их программного обеспечения по направлениям: формальное моделирование и верификация политик управления доступом; системное программирование в контексте достижения безопасности и доверия к ПО; верификация и анализ кода; методы тестирования и выявления уязвимостей в программном коде на всех этапах жизненного цикла ПО; инструментальные средства, применяемые для достижения доверия к ПО; технические решения, используемые при разработке средств защиты информации.

Ведущие:

- **Девянин Петр Николаевич,** д.т.н., профессор, член-корреспондент Академии криптографии России, главный научный сотрудник НПО РусБИТех
- **Аветисян Арутюн Ишханович,** д.ф.м.н, член-корреспондент РАН, директор ИСП РАН

Сопоставление требований и практик применения ГОСТ Р ИСО/МЭК 15408 и КТ-178С

Хорошилов Алексей Владимирович, *к.ф.-м.н., ИСП РАН*

Рассматриваются требования и практики применения двух стандартов: ГОСТ Р ИСО/МЭК 15408-2013. «Критерии оценки безопасности информационных технологий», на котором основаны процессы сертификации программного обеспечения, критичного с точки зрения безопасности информации (security), и КТ-178С «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техник», на котором основаны процессы сертификации программного обеспечения, критичного с точки зрения безопасности жизни (safety). Выделяются общие подходы и отличия между ними, обсуждаются возможные варианты взаимного обогащения двух миров.

О результатах моделирования управления доступом в СУБД PostgreSQL в рамках МРОСЛ ДП-модели

Девянин Петр Николаевич, *член-корреспондент Академии криптографии России, д.т.н., профессор, АО «НПО РусБИТех»*

Мандатная сущностно-ролевая ДП-модель безопасности управления доступом и информационными потоками (МРОСЛ ДП-модель) в её иерархическом представлении была разработана и успешно внедрена как научная основа реализации механизмов мандатного управления доступом и мандатного контроля целостности в отечественной операционной системе специального назначения (ОССН) Astra Linux Special Edition. Вместе с тем использование включающей собственные развитые средства защиты СУБД PostgreSQL в составе ОССН потребовало разработки соответствующих четырёх уровней (ролевого управления, мандатного контроля целостности, мандатного управления доступом с контролем информационных потоков по памяти и по времени) иерархической МРОСЛ ДП-модели. Данная работа завершена и её результаты позволяют говорить об обеспечении соответствия таким важнейшим требованиям доверия как: разработка формальной модели безопасности и проведение анализа скрытых каналов (по памяти и по времени), включённым состав уровней доверия, начиная с третьего, в соответствии с «Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждёнными приказом ФСТЭК России от 30 июля 2018 г. № 131.

Спецификация модели управления доступом на языке TLA+ и ее верификация

Козачок Александр Васильевич, *к.т.н., Академия ФСО России*

Представлено описание модели управления доступом к разнокатегорийным электронным документам компьютерных систем, обеспечивающей выполнение требований мандатного контроля целостности и конфиденциальности без учета информационных потоков по времени. Отличительной чертой модели является учет особенностей жизненного цикла электронных документов и порядка работы с ними. Для задания модели управления доступом был выбран язык темпоральной логики действий Лэмпорта, поскольку его нотация представляется наиболее близкой к общепринятой математической, выразительные возможности и инструментальные средства позволяют описывать и верифицировать системы, заданные в виде конечных автоматов.

Перспективы реализации ролевого управления доступом в ОССН Astra Linux Special Edition

Тележников Владимир Юрьевич, *к.т.н., ФУМО ВО ИБ*

Предлагается подход к практической реализации в операционной системе специального назначения (ОССН) Astra Linux Special Edition ролевого управления доступом в условиях его совместного функционирования с мандатным управлением доступа. Оценивается возможность перехода от использования механизма привилегий к предоставлению полномочий через роли, затрагиваются вопросы организации администрирования ролей, а также рассматриваются особенности применения и реализации ролевого управления доступа при сетевом взаимодействии ОССН.

Скрытая отладка виртуальных машин

Довгалюк Павел Михайлович, *кандидат технических наук;* ***Абакумов Михаил Александрович; Полетаев Дмитрий Николаевич; Иванов Алексей Владимирович; Степанов Владислав Михайлович -*** *(НовГУ им. Я.Мудрого)*

Виртуальные машины используются при отладке или анализе программ, если требуется создание изолированной среды или отлаживаются компоненты операционной системы. При этом требуется ограничивать влияние изучаемого кода и инструментального друг на друга, что особенно важно при изучении вредоносного ПО. Скрытая отладка - это использование такого окружения, при котором отлаживаемая программа работает так же, как и на обычном компьютере. Во время скрытой отладки программа не может обнаружить в этой среде наличие отладочных функций. Рассматриваются способы для улучшения изоляции виртуальной машины и реализации скрытой отладки: внедрение сервиса для удаленной отладки в гипервизор вместо загрузки его в гостевую систему;отслеживание ввода-вывода виртуальной машин; отслеживание системных событий в гостевой ОС; запись и воспроизведение работы виртуальной машины.

Мандатные управления доступом и контроль целостности при разработке сетевых сервисов в среде ОССН Astra Linux Special Edition

Шишов Максим Николаевич, *РусБИТех-Астра*

Современная нормативная база ФСТЭК России, включающая требования к операционным системам (ОС), используемым в целях обеспечения защиты информации, накладывает жесткие ограничения на условия функционирования в среде таких ОС системного программного обеспечения, в том числе сетевых сервисов. В первую очередь для выполнения этих требований необходимо обеспечить корректное взаимодействие сетевых сервисов с механизмами защиты ОС, включая средства управления доступом. Это создает существенные трудности для разработчиков защищенных ОС семейства Linux, т. к. в этом случае сетевые сервисы создавались для работы с изначально дискреционным управлением доступом таких ОС, а, значит, в них не закладывались возможности для работы, например, с мандатным управлением доступом. По этой причине для применения в (ОССН) Astra Linux Special Edition популярные сетевые сервисы Apache2 и СУБД PostgreSQL были доработаны с целью обеспечения их корректного функционирования при использовании штатных для ОССН мандатных управления доступом и контроля целостности. Сутью этой доработки является исключение утечки конфиденциальных данных через используемые соответствующим сетевым сервисом общие ресурсы, такие как оперативная память и файловая система, за счет реализации технологии запуска для каждого пользователя сервиса отдельного процесса с мандатными атрибутами этого пользователя.

Абстрактная интерпретация бинарного кода как универсальная платформа анализа

Соловьев Михаил Александрович, *кандидат физико-математических наук;* ***Бакулин Максим Геннадьевич; Горбачев Михаил Сергеевич; Манушин Дмитрий Валерьевич; Падарян Вартан Андроникович, кандидат физико-математических наук; Панасенко Сергей Сергеевич*** *- (ИСП РАН)*

Рассматривается подход к анализу бинарного кода, основанный на трансляции машинных команд в промежуточное представление и проведении абстрактной интерпретации по этому представлению. Проводится обзор наиболее востребованных на практике задач в анализе бинарного кода и показывается, что все они могут быть сведены к задаче абстрактной интерпретации. Описываются разработанные компоненты универсальной платформы анализа бинарного кода: декодер машинных команд и промежуточное представление Pivot 2.

Подходы к внедрению мандатного управления доступом на этапе проектирования механизмов межпроцессного взаимодействия ОС семейства Linux

Буренин Павел Валерьевич, *к.т.н., ФУМО ВО ИБ*

Рассматриваются особенности внедрения мандатного управления доступом и мандатного контроля целостности на этапе проектирования механизмов межпроцессного взаимодействия ОС семейства Linux (детально на примере механизма D-Bus). Приводится анализ специфики проявления угроз безопасности информации, связанных с использованием таких механизмов. Исследуются подходы по обеспечению безопасности управления доступом при взаимодействии процессов ОС семейства Linux на основе мандатной сущностно-ролевой ДП-модели безопасности управления доступом и информационными потоками (МРОСЛ ДП-модели). Практические аспекты внедрения этих подходов анализируются в контексте применения в отечественной защищенной операционной системе специального назначения Astra Linux Special Edition.

Методика применения встроенных средств защиты ОССН Astra Linux Special Edition прикладным программным обеспечением

Борисов Андрей Львович, *НПО РусБИТех*

Разработчики прикладного ПО часто самостоятельно реализуют в нем функциональные возможности, связанные с защитой информации (идентификацию и аутентификацию, разграничение прав доступа и т. д.), что при его использовании в составе ведомственных или корпоративных автоматизированных систем (предназначенных для обработки, в том числе, информации ограниченного доступа) создаёт сложности как системного администрирования, так и при сертификации ПО таких систем.

Операционная система специального назначения (ОССН) Astra Linux Special Edition даёт возможность решения указанных проблем за счёт: применения встроенных средств защиты информации, обеспечивающих централизованную регистрацию информационных ресурсов, пользователей и управление разграничением доступа в рамках домена безопасности, однократной идентификации и аутентификации пользователя при входе в сеанс и последующего разграничения доступа в масштабах локальной сети, аудита событий безопасности. Такие результаты достигнуты благодаря применению рассматриваемой методики разработки прикладного ПО, включающей: исключение из прикладного ПО средств ведения учётных записей пользователей и разграничения прав доступа к информационным ресурсам с возложением этих функций на встроенные средства, включённые в сертифицированный дистрибутив ОССН, а также проектирование и разработку баз данных и программных модулей, взаимодействующих с этими средствами через API ОССН. Таким образом, прикладное ПО, разработанное в соответствии методикой, не требует самостоятельной сертификации по требованиям ФСТЭК, ФСБ и Минобороны России как СЗИ от НСД.

Формирование индикаторов достижения компетенций в области защищенных операционных систем на основе анализа требований образовательных и профессиональных стандартов

Цибуля Алексей Николаевич, *к.т.н., доцент, Академия ФСО России*

Представлены результаты анализа перечня трудовых функций и трудовых действий профессиональных стандартов, содержащихся в проектах ФГОС ВО (3++) для укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность» применительно к предметной области защищенных операционных систем. Приведены особенности формирования компетенций в данном направлении согласно международному стандарту «Национальная образовательная инициатива в области кибербезопасности. Структура трудовых ресурсов в области кибербезопасности». По результатам анализа сформулированы предложения по формированию индикаторов достижения соответствующих компетенций для дисциплин, а также программ профессиональной переподготовки и повышения квалификации. Представлены предложения по структуре лабораторных работ для привития практических навыков эксплуатации защищенных операционных систем.

Практики безопасной разработки программного обеспечения как важная составляющая соответствия требованиям безопасности информации

Смирнов Николай Валерьевич, *ОАО «ИнфоТеКС»*

Как известно, не существует компьютерных программ без ошибок. Есть мнение, что количество и вероятность возникновения таких ошибок разработчик может существенно редуцировать, внедрив практики и процессы безопасной разработки, выполнив рекомендации стандарта ГОСТ Р 56939-2016. Практика оказывается отличной от теоретических построений. О результатах внедрения практик безопасной разработки отдельно взятой компанией-вендором будет рассказано в докладе.

17:00 – 19:30 Секция «Перспективные исследования в области кибербезопасности»

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

Архитектуры и модели компонентов генерации и выбора контрмер для SIEM-систем следующего поколения

Котенко Игорь Витальевич, *д.т.н., профессор, СПИИРАН*

Рассматривается современное состояние исследований и разработок в области создания компонентов генерации и выбора контрмер для SIEM-систем. Представляется концептуальная модель основных процессов киберзащиты и место в ней процесса реагирования на инциденты. Формулируется постановка задачи генерации и выбора контрмер. Дается представление об архитектуре системы генерации и выбора контрмер. Рассматриваются модели, методики и средства генерации и выбора контрмер, в том числе на основе технологий Advanced Security Analytics. Сравниваются перспективные подходы к генерации и выбору контрмер. Для каждого из них анализируются используемые модели атак, модели защищаемой системы и модели возможных контрмер, а также методики формирования контрмер и оценки их результативности, степень автоматизации, используемые стандарты, показатели эффективности и др. Приводятся примеры разработанных компонентов, выделяются перспективные направления исследований и разработок.

Обеспечение доступности и анализ защищенности в беспроводных сетях кризисного управления

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

Рассматривается задача обеспечения доступности в беспроводных самоорганизующихся сетях кризисного управления и концепция системы обеспечения доступности с использованием средств сканирования сетей и БПЛА для восстановления связности сети. Предлагается модель сети кризисного управления, которая используется для оценки доступности узлов сети. Дается представление о разработанном программном прототипе, реализующем фрагмент сети кризисного управления и механизм обеспечения ее доступности. Прототип используется для проведения экспериментов и осуществления анализа защищенности сети.

Подход к автоматизации процесса защиты от нежелательной информации в сети Интернет

Чечулин Андрей Алексеевич, *к.т.н., СПИИРАН*
Виткова Лидия Андреевна, *СПбГУТ*

Рассматривается проблема защиты от нежелательной информации. Представляется алгоритм блокировки доменных имён, указателей страниц и сетевых адресов, который используется при контроле и надзоре за соблюдением требований законодательства Российской Федерации в сфере защиты от информации. Анализируются подходы к автоматизации анализа информационных объектов разных типов в сети Интернет и способы повышения эффективности противодействия распространению нежелательной информации.

Оценка опасности повседневных сетевых вторжений

Шкирдов Данила Андреевич, *Самарский университет*
Сагатов Евгений Собирович, *Самарский университет, доцент, к.т.н.*
Сухов Андрей Михайлович, *Самарский университет, профессор, д.т.н.*
Дмитренко Павел Сергеевич, *Крымский федеральный университет*

Приводятся полученные авторами данные об интенсивности ежедневных сетевых атак на основе информации с серверов ловушек. Для 10 наиболее популярных Интернет-сервисов составлены черные списки атакующих адресов, и приведены размеры этих списков. Рассчитаны параметры интенсивности запросов, для каждого из 10 сервисов найдены первые десять стран по количеству атакующих адресов. На примере DNS-сервиса подробно иллюстрируется процесс обработки данных из файлов журналов.

Динамический анализ потоков данных JavaScript-кода

Хашаев Артур Акрамович, *Лаборатория интеллектуальных систем кибербезопасности, Факультет ВМК МГУ*

Рассматривается задача динамического анализа потоков данных JavaScript-кода в контексте задачи автоматизированного поиска уязвимостей класса XSS в клиентской части современных веб-приложений. Обсуждаются возможные способы решения задачи распространения меток в памяти программы. Для решения этой задачи предложен и реализован метод, основанный на переписывании абстрактного синтаксического дерева. На основе предложенного метода продемонстрирован способ разметки объектов и значений в памяти программы с последующим распространением меток по ходу ее выполнения. Представлен путь эволюции реализованного инструментария в динамический анализатор, нацеленный на поиск уязвимостей в клиентской части веб-приложений.

Подход к синтаксическому определению сетевого трафика Интернета вещей для выявления аномалий

Гайфулина Диана Альбертовна, *Университет ИТМО*
Федорченко Андрей Владимирович, *Университет ИТМО*

Рассматривается подход к анализу трафика сетей Интернета вещей (IoT), позволяющий повысить качество процесса выявления сетевых аномалий. Представляется разработанная методика определения структуры сетевого трафика, содержащего нерегламентированные протоколы передачи данных. Предлагаемый подход позволяет преодолеть неопределенность протоколов прикладного уровня, что дает возможность проводить оценку защищенности сетей IoT и расследование инцидентов информационной безопасности.

Использование машинного обучения в IoT для детектирования вредоносной активности

Кушнеревич Алексей Геннадьевич, *СПИИРАН*

Проводится сравнение точности и быстродействия задач машинного обучения в случае локального и распределенного запуска для задач обеспечения кибербезопасности. В качестве прикладной задачи рассматривается обнаружение атак на сеть IoT и их классификация. Для распределенного режима используется платформа обработки больших данных Spark (ML) в паре с Hadoop (YARN).

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

Серебряный партнер – Компания «Актив»

Российский разработчик и поставщик систем и программно-аппаратных средств информационной безопасности, крупнейший в России производитель электронных идентификаторов Рутокен, а также программных продуктов и электронных ключей Guardant для защиты и лицензирования программного обеспечения. Продуктовая линейка Guardant – это стандарт де-факто на российском рынке защиты всех видов ПО. Рутокен – первая на рынке полностью отечественная линейка продуктов, контроль за производством которой происходит на всех этапах, силами производителя и на территории Российской Федерации. Ключевые носители Рутокен используются везде, где требуется безопасное хранение и использования паролей, цифровых сертификатов, ключей шифрования и ключей электронной подписи. Электронные идентификаторы Рутокен представлены во всех возможных форм-факторах: от стандартного USB-токена или смарт-карты до Bluetooth-устройств.

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

Серебряный партнер – ИнфоТеКС

ИнфоТеКС (ОАО «Информационные Технологии и Коммуникационные Системы») ведущий производитель программных и программно-аппаратных VPN-решений и средств криптографической защиты информации. Компания основана в 1991 году. Сегодня ИнфоТеКС занимает устойчивые позиции лидера Российского рынка информационной безопасности. Помимо разработки и продвижения средств защиты информации, компания обеспечивает их поддержку и обслуживание, ведет научно-исследовательскую и консалтинговую деятельность.

www.infotecs.ru

Бронзовый партнер – Компания Фактор-ТС

Компания «Фактор-ТС» выпускает программно-аппаратные комплексы для защиты информации уже 25 лет. Ключевые заказчики – государственные структуры. Новая разработка компании – Dionis DPS. Продукт, ориентированный на коммерческий сектор и государственные ведомства, работающие с персональными данными.

Dionis DPS – это единый центр управления безопасностью сети, сертифицированный ФСБ и ФСТЭК России. Dionis DPS гарантирует безопасность передачи конфиденциальной информации через незащищенные сети общего пользования.

Модельный ряд Dionis DPS ориентирован как на небольшие компании, так и на крупные организации с большими центрами обработки данных.

www.factor-ts.ru

Бронзовый партнер – АО «НПО РусБИТех»

АО «НПО РусБИТех» — научно-производственное объединение, осуществляющее лицензированную разработку, производство и внедрение автоматизированных систем, систем поддержки принятия решений, программных средств общего назначения, разработку и создание средств защиты информации. Приоритетным направлением является разработка сертифицированных ФСБ, ФСТЭК и Минобороны России семейства ОС Astra Linux, высокий уровень доверия к которым обеспечивается использованием широкого спектра методов формального моделирования и верификации политик управления доступом, выявления скрытых каналов, статического и динамического анализа программного кода с применением соответствующих инструментальных средств.

www.rusbitech.ru

Научный партнер – Компания «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

Партнер – Ассоциация Разработчиков Программных Продуктов «Отечественный софт»

Ассоциация Разработчиков Программных Продуктов «Отечественный софт» является крупнейшим объединением российских производителей программного обеспечения. Мы консолидируем игроков рынка для совместной работы над ключевыми вопросами развития ИТ-отрасли. Ассоциация учреждена в 2009 году российскими разработчиками, в настоящее время в АРПП «Отечественный софт» входит 157 компаний.

АРПП «Отечественный софт» — надёжная коммуникационная площадка, которая создаёт условия для партнерства, взаимодействия с государством и вносит вклад в развитие российской отрасли информационных технологий.

www.arppsoft.ru

Партнер – Академия ФСО России

Федеральное государственное казённое военное образовательное учреждение высшего образования Академия Федеральной службы охраны Российской Федерации осуществляет подготовку кадров для органов государственной охраны и других федеральных органов исполнительной власти. Научно-педагогический состав Академии ФСО России обладает высоким интеллектуальным потенциалом и большим опытом педагогической работы. Более 60 % профессорско-преподавательского состава имеют учёные степени (звания). Академия ФСО России поддерживает и развивает научное и научно-техническое сотрудничество с ведущими научными и образовательными центрами страны. На её базе проводятся всероссийские, ведомственные и региональные научные и научно-практические конференции, в работе которых принимают участие ученые и специалисты из многих регионов Российской Федерации.

www.academ.msk.rsnet.ru

Партнер – АПКИТ

Ассоциация предприятий компьютерных и информационных технологий АПКИТ образована в ноябре 2001 г. По составу участников это самое представительное некоммерческое объединение ИТ-отрасли в России.Членами АПКИТ являются крупнейшие отечественные (1С, ABBYY, Лаборатория Касперского, Консультант Плюс, Ланит, IBS, Мерлион и др.) и мировые компании в области разработки и внедрения программного обеспечения, дистрибуции, системной интеграции, сервисных услуг, производства компьютеров и оборудования, интернета, а также нишевые ассоциации.

АПКИТ сотрудничает с с Минкомсвязи, Минэкономразвития, Минтруда, Минобрнауки, Минпромторгом, МВД, ФНС, ФСБ, ФСТЭК, ФТС. В Национальном совете по профквалификациям при Президенте РФ ассоциация АПКИТ (как СПК-ИТ) отвечает за систему профквалификаций ИТ-отрасли.

www.apkit.ru

Партнер – Ассоциация банков России

Ассоциация банков России основана в 1990 году, сегодня она объединяет в своих рядах более 250 организаций. На банки-участники Ассоциации приходится более 80% всех активов банковской системы России. Стратегической задачей Ассоциации является создание условий для функционирования стабильной банковской системы. Законотворческая деятельность сосредоточена в комитетах Ассоциации, которые работают в режиме постоянных консультаций с обеими палатами Федерального Собрания РФ, Банком России и министерствами. Ассоциация банков России организует крупные ежегодные форумы и конференции, регулярно проводит совещания банкиров с участием представителей регулятора и профильных министерств по актуальным вопросам развития финансового рынка.

www.asros.ru/ru

Партнер – Ассоциация «РОСЭУ»

Ассоциация «РОСЭУ» была образована в начале 2010 года. Ее учредителями являются крупнейшие участники рынка электронных услуг в России. Одной из главных задач «РОСЭУ» является создание эффективной отраслевой площадки для диалога между участниками рынка, предоставляющими услуги в сегментах B2B, B2G и B2C. Ассоциация образована на принципах добровольного объединения его членов. Активное сотрудничество в рамках ассоциации способствует выработке единой позиции членов ассоциации, созданию условий для гармоничного развития рынка электронных услуг в интересах конечных потребителей, а также выстраиванию эффективных взаимоотношений между членами ассоциации и государством. Ассоциация «РОСЭУ» открыта для вступления новых членов, а также для взаимовыгодного сотрудничества с отраслевыми компаниями.

www.roseu.org

Партнер – ФГУП «НПП «Гамма»

ФГУП «НПП «Гамма» специализируется на оказании полного комплекса услуг в области информационной безопасности.

- Защита гостайны, ПДн; защита информации в КИИ, ГИС
- Проектирование и создание защищенных информационных систем
- Мониторинг объектов КИИ, подключение к ГосСОПКА
- Сертификационные и тематические исследования на соответствие требованиям по информационной безопасности ФСТЭК, ФСБ и МО России
- Аттестация объектов информатизации

ШИФРОВАНИЕ:

Тематические исследования шифровальной техники; Создание и сопровождение защищенных VPN-сетей и каналов связи; Защищенная IP-телефония, конференцсвязь

ПОСТАВКА:

Средства защиты информации; SIEM Visor

www.nppgamma.ru

Партнер – Ассоциация ФинТех

Ассоциация ФинТех (АФТ) — это уникальная площадка для конструктивного диалога Банка России с финансовыми и телекоммуникационными компаниями. В состав АФТ входят: Банк России, Сбербанк, Банк ВТБ, Альфа Банк, Газпромбанк, Банк Открытие, Национальная система платежных карт, КИВИ Банк, Банк АК БАРС, РНКО Платежный центр, Тинькофф Банк, Райффайзенбанк, Россельхозбанк; ассоциированные члены: СКБ-Банк, Совкомбанк, Промсвязьбанк, МТС, Московская Биржа, Ростелеком, ПАО «МегаФон», РОСБАНК, РЕГИОН Финансовые услуги, КБ Уральский Банк, ПАО Почта Банк и АКБ Абсолют Банк. На площадке АФТ разрабатываются концепции финансовых технологий и подходы к их внедрению.

www.fintechru.org

КОД БЕЗОПАСНОСТИ

Партнер секции – «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 РФ. Сервисный центр компании готов предоставить профессиональную техническую поддержку партнерам и Заказчикам компании 24 часа и 7 дней в неделю

www.securitycode.ru

CIS
Современные Информационные Системы

Партнер Дней Вузов – CIS

CIS – это журнал об информационных технологиях в России. Задача журнала CIS – показать общий ландшафт рынка ИТ-решений, то разнообразие платформ, идей и инструментов, которые могут быть использованы российскими ИТ-компаниями. ИТ-журнал CIS участвует и проводит промо-акции на всех крупных ИТ-выставках и мероприятия в Москве.

- Журнал выходит ежеквартально и распространяется как в бумажном, так и в электронном виде.
- Целевая аудитория это ИТ-директора и руководители крупных ИТ-компаний.
- География распространения: эл. версия журнала по России и странам СНГ, бумажная версия по Москве.
- Тираж от 5 000 экземпляров.
- График выхода журнала - 4 раза в год (раз в квартал).
- Условия распространения - бесплатно.
- Так же издание распространяется на мероприятиях партнёров.

www.cismag.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» 25

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

ViPNet®

Продукты торговой марки ViPNet – это:

- Комплексный подход к обеспечению ИБ
- Уникальные механизмы сетевой безопасности
- Прозрачная работа в современных сетях связи
- Неограниченная масштабируемость и высокая надежность
- Развитые прикладные сервисы
- Соответствие требованиям законодательства и регуляторов рынка

infotecs

Мы защищаем информацию, которую вы цените

Компания ИнфоТеКС – одна из ведущих ИТ-компаний отечественного рынка программных и программно-аппаратных VPN-решений и средств криптографической защиты информации.

Компания и ее специалисты являются членами профильных организаций и ассоциаций: АДЭ, АЗИ, ЕВРААС. ОАО «ИнфоТеКС» выполняет функции официальной секретарской компании Технического комитета по стандартизации №26 «Криптографическая защита информации».

Ключевой разработкой ИнфоТеКС является **технология ViPNet**, которая объединяет **более 50 программных и программно-аппаратных комплексов**, призванных решать задачи организации защищенных виртуальных частных сетей **(VPN)** и инфраструктуры открытых ключей **(PKI)**.

127287, Москва,
Старый Петровско-Разумовский проезд, 1/23
Тел.: (495) 737 6192,
Факс: (495) 737 7278
Бесплатный звонок по России 8800-250-260 (кроме звонков из Москвы)

www.infotecs.ru

ФАКТОР-ТС

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, а также в Государственной Думе, Банке России, в Министерстве экономического развития РФ (Росреестр, Росрезерв), в Министерстве труда и социальной защиты РФ, Федеральной таможенной службе, региональных подразделениях Федерального казначейства, администрациях целого ряда субъектов Российской Федерации, Сбербанке России и в других министерствах и ведомствах.

Москва, 1-й Магистральный проезд, д. 11, стр. 1
www.factor-ts.ru
factor@factor-ts.ru
+ 7 (495) 644-31-30

НЕОБИТ

Новые Безопасные
Информационные Технологии

СМОТРИ В БУДУЩЕЕ.
ИНВЕСТИРУЙ В ЗНАНИЯ.

АИС

АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Почему выбирают нас

Академия Информационных Систем (АИС) предоставляет образовательные услуги по информационной безопасности, информационным технологиям, конкурентной разведке и экономической безопасности.

Академия Информационных Систем зарекомендовала себя также как и организатор деловых мероприятий. Более чем за 20 лет команда АИС успешно провела более 250 успешных деловых событий.
Наши мероприятия проходят при поддержке и активном участии государственных ведомств и регуляторов, а также ряда ассоциаций и общественных организаций Российской Федерации.

Мы предлагаем:

- 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
- Многопрофильный экзаминационный центр
- Симуляционные деловые игры по управлению проектами, подготовка к сертификациям PMI
- Обучение по защите АСУ ТП, КИИ, ГосСОПКА
- Технологии дистанционного обучения, вебинары и онлайн-тестирование

Связаться с нами

info@infosystem.ru

+7 (495) 120-04-02

www.infosystems.ru , www.vipforum.ru

КАЛЕНДАРЬ МЕРОПРИЯТИЙ АИС

25 АПРЕЛЯ 2019 | Г. МОСКВА

Конференция по практическим аспектам борьбы с кибермошенничеством в финансовом секторе. AntiFraud Spring Russia

Главная тема: Актуальные проблемы правоприменения федеральных законов и нормативно-правовых актов Банка России в области противодействия фроду, обмен практическим опытом, а также новые инициативы по развитию цифровых финансовых технологий.

5-7 ИЮНЯ 2019 | Г. НИЖНИЙ НОВГОРОД

Конференция и семинар по защите конфиденциальной информации «Волга-Конфидент»

Главная тема: Конференция посвящена вопросам защиты конфиденциальной информации, адресована руководителям корпоративных служб безопасности, обеспечивающих защиту конфиденциальной информации, соответствие требованиям национального и международного законодательства.

ИЮНЬ 2019 | Г. МОСКВА

IX Научно-практическая конференция «Управление информационной безопасностью в современном обществе»

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

9-13 СЕНТЯБРЯ 2019 | Г. ЯЛТА

XVIII Всероссийский форум «Информационная безопасность. Регулирование. Технологии. Практика. ИнфоБЕРЕГ»

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

15-18 ОКТЯБРЯ 2019 | Г. ЯРОСЛАВЛЬ

XI Конференция «Цифровое государство: новые подходы к управлению и безопасности»

Главная тема: Конференция посвящена вопросам развития в Российской Федерации цифровой экономики, электронных услуг и услуг в области информационной безопасности, блокчейн-технологий.

3-5 ДЕКАБРЯ 2019 | Г. МОСКВА

Неделя безопасности АИС

Объединяет международный форум по борьбе с кибермошенничеством **Antifraud Russia**, ежегодную конференцию **«Экономическая безопасность и конкурентная разведка»** и серию образовательных семинаров по актуальным вопросам кибербезопасности и безопасности бизнеса.
Более 700 участников из 12 стран мира.

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

+7 (495) 120-04-02

conf@infosystem.ru

www.ruscrypto.ru
www.vipforum.ru