ОРГАНИЗАТОРЫ

Ассоциация РусКрипто

АИС

ПРОГРАММА КОНФЕРЕНЦИИ

20-23 марта 2018 г.

www.ruscrypto.ru

КЛЮЧЕВОЕ СЛОВО

В ЗАЩИТЕ ИНФОРМАЦИИ

СКАЧИВАЙТЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ РУСКРИПТО’2018

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

IOS

НА ПРОМО СТРАНИЦУ

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

Благодарим спонсоров и партнеров за оказанную поддержку!

Золотой спонсор

КРИПТОПРО
ключевое слово в защите информации

Серебряные спонсоры

Компания АКТИВ

infotecs

Бронзовый спонсор

ФАКТОР-ТС

Научный партнер

НЕОБИТ

Спортивный партнер

SPORT PROJECT RUS

Партнеры конференции

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Check Point SOFTWARE TECHNOLOGIES LTD.

КОД БЕЗОПАСНОСТИ

ОПКИТ

TREND MICRO

ФГУП "НПП "Гамма"

РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ

АБИСС

АЗИ

Информационная поддержка

Единый портал Электронной подписи

ICT ONLINE
ИНФОКОММУНИКАЦИИ ОНЛАЙН

BITCRYPTO NEWS

КРИПТО валюты.рф

БИТ

Системный администратор

Б.О

NBJ

Аналитический банковский журнал

BIS JOURNAL

20 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 – 22:00	Вечерняя программа

21 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'2018» **Пленарное заседание** *Место: Зал «Шишка»* *Подробнее: 6 стр.*	
12:00 – 12:30	Кофе-брейк	
12:30 – 14:00	**Круглый стол «Российская криптография в российском сегменте Интернет»** *Место: Зал «Шишка»* *Подробнее: 6 стр.*	**Секция «Разработка защищенного программного обеспечения»** *Место: Зал «Еловый»* Ведущие: · Гамаюнов Д.Ю., ВМК МГУ · Елисеев И.Ю., АИС *Подробнее: 6-7 стр.*
14:00 – 15:00	Обед	
15:00 – 17:00	**Секция «Безопасность решений на базе технологий блокчейн. Применение российской криптографии в технологиях цепной записи данных и распределенных реестров»** *Место: Зал «Шишка»* Ведущие: · Качалин А.И., Сбербанк · Маршалко Г.Б., ТК26 *Подробнее: 7-8 стр.*	**Секция «Цифровая криминалистика»** *Место: Зал «Еловый»* Ведущие: · Яковлев А.Н., Следственный комитет РФ · Чиликов А.А., МГТУ им. Н.Э. Баумана *Подробнее: 8-9 стр.*
17:00 – 17:30	Кофе-брейк	

17:30 – 19:30	**Секция «Криптография и криптоанализ», 1 часть** *Место: Зал «Шишка»* Ведущие: · Матюхин Д.В., ФСБ России · Попов В.О., КриптоПро, Ассоциация «РусКрипто» · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Подробнее: 9-10 стр.*	**Секция «Информационная безопасность и криптография в кредитно-финансовой сфере** *Место: Зал «Еловый»* Ведущие: · Простов В.М., ФСБ России · Янсон И.А., Сбербанк *Подробнее: 10 стр.*
20:00 – 23:00	Торжественное открытие XX юбилейной конференции «РусКрипто'2018», фуршет	

22 МАРТА, ЧЕТВЕРГ. ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

08:00 – 10:00	Завтрак		
10:00 – 12:00	**Дискуссионная панель «Классический антивирус умер: что делать и чем заменить?»** *Место: Зал «Шишка»* Ведущие: · Ромашев А., Информзащита · Слободенюк Д., ARinteg *Подробнее: 11 стр.*	**Секция «Криптография и криптоанализ», 2 часть** *Место: Зал «Еловый»* Ведущие: · Матюхин Д.В.,ФСБ России · Попов В.О., КриптоПро, Ассоциация «РусКрипто» · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Подробнее: 11-12 стр.*	**Мастер-класс «Быстрее, глубже, точнее. Новые методы и приемы в арсенале интернет-разведки.»** *Место: Зал «Сосновый»* Ведущий: Масалович А.И., Академия Информационных систем *Подробнее: 12 стр.*
12:00 – 12:30	Кофе-брейк		
12:30 – 14:00	**Секция «Технологии электронной подписи и PKI»** *Место: Зал «Шишка»* Ведущие: · Маслов Ю.Г, РОСЭУ, КриптоПро · Малинин Ю.В., РОСЭУ Академия Информационных Систем *Подробнее: 12-13 стр.*	**Секция «Криптография и криптоанализ», 3 часть** *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.*	**Мастер-класс «Принцип Парето в информационной безопасности»** *Место: Зал «Сосновый»* Ведущий: Лукацкий А.В. *Подробнее: 13-14 стр.*
14:00 – 15:00	Обед		

15:00 – 16:30	**Секция «Криптография в системах IoT и M2M»** *Место: Зал «Шишка»* Ведущий: Горелов Д.Л., Компания Актив, Ассоциация «РусКрипто» *Подробнее: 14-15 стр.*	**Секция «Криптография и криптоанализ», 4 часть** *Место: Зал «Еловый»* Ведущие: · Матюхин Д.В., ФСБ России · Попов В.О., КриптоПро, Ассоциация «РусКрипто» · Жуков А.Е., МГТУ им. Баумана, Ассоциация «РусКрипто» *Подробнее: 15-16 стр.*	**Секция «Обеспечение киберустойчивости цифровой экономики и цифрового производства»** *Место: Зал «Сосновый»* Ведущий: Зегжда П.Д., СПбПУ ИБКС *Подробнее: 16-18 стр.*
16:30 – 17:00	Кофе-брейк		
17:00 – 19:30	**Круглый стол «Роль российского экспертного сообщества в разработке международных стандартов и рекомендаций в области криптографии и защиты информации»** *Место: Зал «Шишка»* *Подробнее: 18 стр.*	**Секция «Перспективные исследования в области кибербезопасности»** *Место: Зал «Еловый»* Ведущий: Котенко И.В., СПИИРАН *Подробнее: 19-21 стр.*	
19:30 – 20:30	Ужин		
20:00	**Интеллектуальная командная игра «Где логика?»** *Место: Киноконцертный зал*		

23 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

Есть ли жизнь после ГОСТ 28147-89?
Матюхин Дмитрий Викторович, ФСБ России

Вопросы обеспечения криптографической безопасности в актуальных системах
Баранов Александр Павлович, д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России

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

Российские криптоалгоритмы в международных протокольных решениях: история, задачи, перспективы
Смышляев Станислав Витальевич, к.ф.-м.н., директор по информационной безопасности, КриптоПро

12:30 – 14:00 Круглый стол «Российская криптография в российском сегменте Интернет»

Правительством утвержден план мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика». Он предусматривает разработку дорожной карты по переводу российского сегмента Интернет на отечественную криптографию. Цель круглого стола — открытый диалог заинтересованных сторон, общественное обсуждение и информирование широкого круга специалистов о возможных путях и этапах решения этой сложной задачи.

Эксперты круглого стола:

- **Устинов Игорь Геннадьевич,** Криптоком
- **Смышляев Станислав Витальевич,** КриптоПро
- **Горелов Дмитрий Львович,** компания Актив
- **Гусев Дмитрий Михайлович,** ИнфоТеКС
- **Темников Валерий Александрович,** Технический центр Интернет
- **Гилязов Руслан Раджабович,** лаборатория информационной безопасности МГУ имени М.В. Ломоносова
- **Ковалев Андрей,** Яндекс
- **Малинкин Дмитрий Викторович,** Спутник

12:30 – 14:00 Секция «Разработка защищенного программного обеспечения»

Ведущие:

- **Гамаюнов Денис Юрьевич,** ВМК МГУ
- **Елисеев Игорь Юрьевич,** Академия Информационных Систем

Практики разработки защищенного ПО призваны минимизировать возможность попадания критичных ошибок в продукционную среду, где они могли бы быть использованы для реализации компьютерных атак. Все понимают необходимость применения таких практик, но ошибок, на первый взгляд, не становится меньше, причем часть из них относится к разряду критичных. Что мешает разработчикам адаптировать в полной мере потенциал практик Secure SDLC? Каких результатов добились организации, уже внедрившие эти практики? Где и как готовить специалистов по разработке защищенного ПО?

Участники дискуссии:

- **Крайнов Сергей Олегович,** Сбербанк
- **Лебедев Виктор Олегович,** Банк России
- **Петухов Андрей,** SolidLab
- **Колесов Юрий,** 1С Битрикс

Вопросы реализации нормативных требований Банка России при разработке и эксплуатации прикладного программного обеспечения, используемого для осуществления денежных переводов

Лебедев Виктор Олегович, главный инженер Управления методологии и стандартизации информационной безопасности, Банк России

AppSec from scratch: тернистый путь

Колесов Юрий, 1С Битрикс

15:00 – 17:00 Секция «Безопасность решений на базе технологий блокчейн. Применение российской криптографии в технологиях цепной записи данных и распределенных реестров»

Ведущие:

- **Качалин Алексей Игоревич,** исполнительный директор Центра Киберзащиты, Сбербанк
- **Маршалко Григорий Борисович,** эксперт ТК26, руководитель рабочей группы «Безопасность технологий цепной записи данных и распределенных реестров»

Цель секции – рассказать о технологиях блокчейн без лозунгов и популизма. О безопасности, о моделях угроз и векторах развития. Докладчики расскажут о проектах, которые используют технологии цепной записи данных и распределенных реестров, об их реальной применимости, о достоинствах и недостатках перед классическими подходами. Значимая часть секции будет посвящена применению российских криптографических стандартов. Программа секции состоит из блока докладов и открытой дискуссии.

Использование технологии децентрализованного ведения реестров

Трифонов Михаил Игоревич, проектный менеджер, департамент по развитию технологии блокчейн, Внешэкономбанк

К вопросу построения безопасных протоколов функционирования блокчейн-систем

Маршалко Григорий Борисович, эксперт ТК26, руководитель рабочей группы «Безопасность технологий цепной записи данных и распределенных реестров»
Лавриков Иван Викторович, эксперт ТК26
Гуселев Антон Михайлович, эксперт ТК26

Как не надо работать с деньгами: ограничения смарт-контрактов и странные решения разработчиков Ethereum

Маланов Алексей, эксперт, Лаборатория Касперского

О построении среды для конструирования гарантированно надежных смарт-контрактов
Шишкин Евгений, ведущий исследователь, Центр научных исследований и перспективных разработок ОАО «ИнфоТеКС»

О разрешительных принципах регулирования блокчейн и криптовалют в Республике Беларусь и подходах к созданию блокчейн платформ
Комисаренко Владимир Владимирович, заместитель директора по проектам в сфере защиты информации компании LWO

Безопасное приземление технологии блокчейн в инфраструктуру корпоративной информационной системы
Качалин Алексей Игоревич, исполнительный директор Центра Киберзащиты, Сбербанк

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

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

Необходимость развития методов цифровой криминалистики обусловлена повсеместным проникновением информационных технологий в повседневную жизнь. Задачи, стоящие перед экспертами-криминалистами, постоянно усложняются и требуют совершенствования профессиональных навыков и применяемых инструментов. В рамках секции ведущие эксперты-практики и разработчики криминалистического инструментария поделятся своим опытом в решении сложных технических задач, а также расскажут о правовых и иных практических аспектах цифровой криминалистики.

Обнаружение криминалистических артефактов функционирования ПО Metasploit в слепках оперативной памяти
Скулкин Олег Владимирович, GCFA, MCFE, ACE, специалист по компьютерной криминалистике GroupIB

Преодоление парольной защиты и получение доступа к защищенным данным для некоторых моделей мобильных устройств Samsung в сложных случаях
Чиликов Алексей Анатольевич, к.ф.-м.н., МГТУ им. Баумана, Passware

Современные подходы к извлечению данных из Android-устройств
Карондеев Андрей, Oxygen

Использование принципов реверс-инжиниринга при автоматизации восстановления видеоданных с поврежденной логической структурой
Абрамец Алексей Сергеевич, старший эксперт отдела компьютерно-технических и инженерно-технических исследований управления организации экспертно-криминалистической деятельности Главного управления криминалистики, Следственный комитет РФ

Возможности анализа информации из социальных сетей
Турсунбаев Ерлан Хажмаханович, Евсеева Юлия Викторовна, старшие эксперты отдела компьютерно-технических и инженерно-технических исследований управления организации экспертно-криминалистической деятельности Главного управления криминалистики, Следственный комитет РФ

Современный компьютеризированный автомобиль как объект цифровых исследований
Бережной Игорь Анатольевич, старший эксперт отдела компьютерно-технических и инженерно-технических исследований управления организации экспертно-криминалистической деятельности Главного управления криминалистики, Следственный комитет РФ

Практические применения цифровой криминалистики
Яковлев Алексей Николаевич, заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований управления организации экспертно-криминалистической деятельности Главного управления криминалистики, Следственный комитет РФ

Компьютерно-техническая экспертиза в арбитражных спорах
Земцов Анатолий Павлович, директор Ассоциации производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ»

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

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

О свойствах W-марковских подстановок
Пудовкина Марина Александровна, д.ф.-м.н., профессор МГТУ им. Н.Э. Баумана

Рассматривается свойства преобразований слоев раундовой функции, обеспечивающих W-марковость XSL-алгоритмов блочного шифрования. Особенность W-марковских преобразований состоит в наличии определенной структурированности их матриц вероятностей переходов разностей. Описано множество подстановок, свойство W-марковость которых характеризуется свойствами орграфа, задаваемого матрицей вероятностей переходов разностей. Приведены условия на s-боксы и линейные преобразования, при выполнении которых имеет место W-марковость XSL-алгоритма.

О подходах к синтезу схем подписи, основанных на итеративном использовании функций хэширования
Гуселев Антон Михайлович, Лавриков Иван Викторович, ТК26

Описаны существующие сегодня подходы к созданию схем подписи, основанные на итеративном использовании функций хэширования, и, в частности, древовидные структуры, использованные при создании схем XMSS и LMS, которые в настоящее время находятся в процессе утверждения в качестве рекомендаций IETF. Рассмотрены альтернативные подходы к созданию схем подписи, основанных на итеративном использовании функций хэширования. Предложены возможные варианты подобных схем подписи, указаны их некоторые особенности по сравнению существующими схемами. Показано сведение криптографических свойств предлагаемых решений к свойствам используемых функций хэширования (в классической модели).

О возможности применения одного алгоритма дискретного логарифмирования
Гребнев Сергей Владимирович, МИЭМ НИУ ВШЭ
Изучаются свойства одного алгоритма дискретного логарифмирования в группе точек эллиптической кривой, предложенного А.Ю. Нестеренко на конференции CTCrypt 2016. Показано, что для практически важных случаев его средняя трудоемкость не меньше, чем у метода Полларда

Об асимметрично выполняемых симметричных криптосистемах (шифрах)
Варфоломеев Алексей Александрович, к.ф.-м.н., доцент, МИФИ

Рассматриваются классические симметричные и асимметричные криптосистемы (шифры), но обладающие свойством существенной асимметричности выполняемых работ законными участниками взаимодействия, например, при зашифровании открытого текста и при расшифровании соответствующего шифрованного

текста. Обсуждаются вопросы преобразования классических криптосистем в асимметрично выполняемые. При этом приходится учитывать различные определения понятия «ключ», в том числе из известного российского словаря криптографических терминов. Данные криптосистемы (шифры) существенно повышают сложность восстановления злоумышленником открытого текста при различных нормативных ограничениях на размер криптографического ключа.

Совершенные шифры. Один новый совершенный шифр
Бабаш Александр Владимирович, д.ф.-м.н., профессор, Высшая школа экономики
Баранова Елена Константиновна, доцент, Высшая школа экономики

Существующие совершенные шифры не являются совершенными по нападению на ключ. Шифр Виженера является подшифром шифра случайного гаммирования. Поэтому шифр случайного гаммирования следует отнести к практическим шифрам. Его следует дешифровывать. Приводится ранее неизвестный автору еще один совершенный шифр. Он также не является совершенным по нападению на ключ.

О ключевом расписании на основе модифицированного аддитивного генератора
Коренева Алиса Михайловна, системный аналитик, Код Безопасности
Задорожный Дмитрий Игоревич, руководитель службы сертификации, ИБ и криптографии, Код Безопасности
Фомичёв Владимир Михайлович, д.ф.-м.н., научный консультант, Код Безопасности

Представлен новый класс «гибких» алгоритмов ключевого расписания блочных шифров на основе модифицированного аддитивного генератора, позволяющий генерировать раундовые ключи заданного размера из основного ключа различной длины. Данный класс алгоритмов допускает быструю программную реализацию с использованием современных вычислительных средств и обеспечивает совершенную зависимость раундовых ключей от основного ключа, то есть зависимость каждого бита раундовых ключей от всех битов основного ключа.

17:30 – 19:30 Секция «Информационная безопасность и криптография в кредитно-финансовой сфере»

Ведущие:
- **Простов Владимир Михайлович,** ФСБ России
- **Янсон Иван Андреевич,** Сбербанк

Секция состоит из блока докладов и обсуждения проблем и задач, которые сейчас актуальны для банковской сферы. У участников будет возможность задать вопросы ведущим экспертам и регуляторам отрасли, в открытом диалоге обсудить наиболее злободневные темы.

О вопросе внедрения российских криптографических средств в национальной платежной системе
Простов Владимир Михайлович, ФСБ России

Стандартизированные решения по использованию российских криптоалгоритмов в платежных системах: вопросы безопасности
Елистратов Андрей Алексеевич, эксперт ТК26
Алексеев Евгений Константинович, к.ф.-м.н., эксперт ТК26

Практика применения средств электронной подписи
Янсон Иван Андреевич, Сбербанк

Криптографические средства на рабочих местах клиентов ДБО
Мещеряков Кирилл Олегович, компания Актив

Открытая дискуссия

ВТОРОЙ ДЕНЬ РАБОТЫ КОНФЕРЕНЦИИ

10:00 – 12:00 Дискуссионная панель «Классический антивирус умер: что делать и чем заменить?»

Ведущие:

- **Ромашев Анатолий,** начальник отдела безопасности прикладных систем, Информзащита
- **Слободенюк Дмитрий**, ARinteg

Киберпреступники непрерывно совершенствуют методы атак и техники применения вредоносного кода, что привело к значительной потере эффективности классических антивирусов. Привычные методы не работают, это показали громкие эпидемии 2017 года. Еще более бесполезны классические антивирусы против целенаправленных и сложных многовекторных атак. Клиенты по-прежнему тратят миллионы на защиту от вчерашних угроз, в то время как многие разработчики шагнули далеко за рамки «классики» и предлагают совершенно новые подходы. Об этих подходах и стоящих за ними технологиях пойдет речь.

Эксперты:

- **Кондрашин Михаил**, технический директор, Trend Micro в СНГ, Грузии и Японии
- **Челушкин Константин**, технический консультант, Symantec в России
- **Фишман Антон**, директор проектного направления, Group-IB
- **Маланов Алексей,** эксперт, Лаборатория Касперского

10:00 – 12:00 Секция «Криптография и криптоанализ». 2 часть

Принципы построения отечественных криптонаборов для TLS 1.2

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

Смышляева Екатерина Сергеевна, инженер-аналитик, КриптоПро

Доклад посвящен отечественным криптонаборам для протокола TLS 1.2, разработанным в рамках деятельности РГ 2.1 по сопутствующим криптографическим алгоритмам и протоколам ТК 26. Основные особенности режима работы TLS 1.2, определяемого данными криптонаборами, описываются с точки зрения устойчивости к известным методам проведения атак.

О реализации защищённого взаимодействия контрольных и измерительных устройств

Нестеренко Алексей Юрьевич, к.ф.-м.н, МИЭМ НИУ ВШЭ

В докладе будет рассмотрен вариант протокола выработки общего ключа для сетей, в которых нет гарантированной доставки сообщений.

Протокол SIKE и его устойчивость к классическим и квантовым атакам

Тараскин Олег Геннадьевич, зам. директора проекта Рутокен по науке, компания Актив

Протокол SIKE (Supersingular Isogeny Key Encapsulation) обладает экспоненциальной стойкостью к атакам с использованием как классических, так и квантовых алгоритмов. В основе его безопасности лежит задача нахождения изогений между суперсингулярными эллиптическими кривыми. SIKE был подан на конкурс NIST постквантовых алгоритмов, который начался в ноябре 2017. От своих конкурентов, которые основаны на решетках, multivariate и кодах, исправляющих ошибки он выгодно отличается по таким практическим характеристикам как длина ключа и возможность использовать постоянные пары. В докладе рассматриваются атаки на более старую версию — протокол SIDH, которые были учтены при конструировании SIKE.

Криптографические протоколы и возможность их использования для построения скрытых логических каналов

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

В настоящей работе рассматриваются особенности ряда стандартизированных криптографических протоколов и режимов шифрования, которые могут быть использованы злоумышленником для построения скрытых каналов. В частности, показано, что использование счетчиков, например, в качестве уникальной синхропосылки в режиме блочного шифрования и счетчика переданных пакетов в ряде криптографических протоколов, не является безопасным с точки зрения обеспечения защиты от скрытых логических каналов и может быть использовано нарушителем для нарушения безопасности информации.

Уязвимость ROCA и другие возможности внедрения закладок в алгоритм RSA

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

Доклад посвящён внедрению в алгоритм RSA различных видов криптографических лазеек, предоставляющих разработчикам и/или спецслужбам эксклюзивные возможности взлома криптосистемы.

О высокоскоростном асимметричном шифровании на публичном ключе на базе white-box-криптографии

Щелкунов Дмитрий Анатольевич, к.т.н., компания «Рекрипт»
Чиликов Алексей Анатольевич, к.ф.-м.н., Passware

Описывается разработанный авторами подход к созданию схемы высокоскоростного асимметричного шифрования на публичном ключе на базе механизмов white-box-криптографии

10:00 – 12:00 Мастер-класс «Быстрее, глубже, точнее. Новые методы и приемы в арсенале интернет-разведки.»

Ведущий: Масалович Андрей Игоревич, Академия Информационных Систем

Взрывной рост спроса на оперативно-значимую информацию о компаниях и персонах в последние годы привел к резкому расширению спектра методов и приемов интернет-разведки. «Прогулки по невидимому Интернету», которые ранее были уделом узкого круга профессионалов, сегодня стали доступны для широкого практического использования. Также появились методы анализа, использующие т.н. «Большие данные» (Big Data) для обогащения данных. Также существенно пополнился инструментарий анализа социальных сетей. Мастер-класс посвящен обзору новинок в арсенале интернет-разведке и их практическому применению.

12:30 – 14:00 Секция «Технологии электронной подписи и PKI»

Ведущие:

- **Маслов Юрий Геннадьевич,** эксперт Ассоциации РОСЭУ, коммерческий директоркомпании КриптоПро
- **Малинин Юрий Витальевич**, президент Ассоциации РОСЭУ, директор Академии Информационных Систем

Секция, посвященная вопросам развития инфраструктуры открытых ключей и электронной подписи в нашей стране: организационным, юридическим и техническим.
Программа секции состоит из блока докладов и открытой дискуссии посвященной злободневным вопросам российского рынка электронной подписи.

Об использовании токенов и смарт-карт в средствах электронной подписи
Агафьин Сергей Сергеевич, Бородин Георгий Олегович, КриптоПро

Актуальные вопросы применения и развития сервисов доверенной третьей стороны в Беларуси
Москалев Дмитрий Владимирович, «Национальный центр электронных услуг», г. Минск, Беларусь

Правовые аспекты признания электронных документов с иностранной ЭП контролирующими органами РФ
Крыжановская Алла Александровна, Толстых Наталия Иосифовна, ООО «Право высоких технологий»

Технологические аспекты признания трансграничных документов с иностранной электронной подписью российскими и иностранными контролирующими органами
Драло Мария Павловна, ООО «Газинформсервис»

Открытая дискуссия

12:30 – 14:00 Секция «Криптография и криптоанализ». 3 часть

AEAD режимы на основе полиномиальных хэш-функций: существующие решения, их криптографические свойства и возможные модификации
Кислякова Анастасия Сергеевна, ВМиК МГУ имени М.В. Ломоносова

В докладе предполагается осветить криптографические требования, предъявляемые к AEAD режимам шифрования блочных шифров, основные криптографические недостатки режима GCM. Рассматриваются криптографические свойства модификаций режима GCM, таких как белорусский стандарт AEAD режима, режим MGM. Автором предлагается собственная модификация режима GCM, полученная путем замены операции умножения в конечном поле на операцию умножения в кольце целых чисел по модулю 2^{128}, и описываются её криптографические свойства.

Multilinear Galois Mode. Об особенностях построения, функциональных возможностях и доказуемой стойкости
Ноздрунов Владислав Игоревич, ТК 26

В рамках деятельности технического комитета по стандартизации ТК 26 «Криптографическая защита информации» разработан режим работы блочного шифра, осуществляющий одновременно шифрование и аутентификацию, получивший название Multilinear Galois Mode (мультилинейный режим Галуа). В докладе вместе с описанием разработанного режима представлена идеология его построения и обоснование примененных синтезных решений. Также приводятся функциональные возможности MGM и оценки его безопасности в модели доказуемой стойкости.

О подходах к анализу схем аутентифицированного шифрования, построенных с использованием умножения в конечных полях
Бабуева Александра Алексеевна, специалист отдела специальных исследований и разработок, ИнфоТеКС
Науменко Антон Павлович, руководитель направления отдела специальных исследований и разработок, ИнфоТеКС

В представленной работе рассмотрены два режима аутентифицированного шифрования (AEAD-режима): «PD-режим» (представлен В. Ноздруновым на конференции CTCrypt'17) и режим «НЕФРИТ» (разработка ОАО «ИнфоТеКС», публикуется впервые). Для «PD-режима» авторами рассмотрены потенциально опасные события и оценена вероятность наступления некоторых из них. Для режима «НЕФРИТ» рассмотрены два класса атак, направленных на вскрытие ключевого материала и повторное навязывание ранее переданных сообщений.

Обзор алгоритмов аутентифицированного шифрования - финалистов конкурса CAESAR

Власова Виктория Владимировна, Лаборатория Касперского

В открытом международном криптографическом сообществе сложилась традиция проведения различных конкурсов среди разработчиков криптосистем с секретным ключом, а также функций хеширования, алгоритмов выработки имитовставки, электронно-цифровых подписей (конкурсы AES, CRYPTREC, NESSIE, eSTREAM, SHA3). В 2013 г. был объявлен конкурс CAESAR алгоритмов аутентифицированного шифрования. Обзорный доклад посвящен финалистам конкурса CAESAR. Описаны примитивы и подходы, используемые при их синтезе, а также методы анализа, применённые к участникам конкурса и его финалистам.

12:30 – 14:00 Мастер-класс «Принцип Парето в информационной безопасности»

Ведущий: Лукацкий Алексей Викторович, бизнес-консультант по безопасности, Cisco Systems

Нельзя абсолютно защитится от всех существующих и будущих угроз. Но можно попытаться сделать главное. Где те 20%, которые принесут 80% результата? Какие технологии и подходы должен знать и использовать современный безопасник? Алексей Лукацкий в ходе полуторачасового мастер-класса поделиться с участниками РусКрипто'2018 наиболее актуальной и свежей информацией, которая будет полезна любому специалисту в ИБ и ИТ.

15:00 – 16:30 Секция «Криптография в системах IoT и M2M»

Ведущий: Горелов Дмитрий Львович, компания Актив, Ассоциация «РусКрипто»

Некоторые подходы к криптографической защите коммуникаций в IoT и M2M

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

Первая часть доклада содержит рассмотрение и пример типизации промышленных протоколов передачи информации Индустриального интернета в части организации их защиты. Во второй части доклада автор поделится практическим опытом исследований криптографических способов защиты коммуникаций Индустриального Интернета вещей и M2M систем. Заключительная часть доклада посвящена наработкам РГ «Криптографические механизмы для M2M и индустриальных систем» подкомитета № 4 ТК 26, о криптографическом протоколе защищенного обмена для индустриальных систем CRISP и о том, что уже сегодня используется в продуктах компании ИнфоТеКС для защиты АСУ ТП и IoT.

Исследование различных характеристик шифра «Кузнечик» на российских процессорах и платформах IoT (Интернет Вещей)

Овчинников Андрей Игоревич, ФГУП «НПП «ГАММА»

В данной работе исследуется реализация блочного шифра ГОСТ Р 34.12–2015 на следующих популярных и перспективных платформах: российских процессорах Байкал и Эльбрус; одноплатных компьютерах на базе процессоров ARM (Allwinner, Rockchip и т.д.) для IoT, используя CPU и встроенную GPU; мультиклеточных процессорах (до 288 ячеек).

Практическое применение аппаратных криптографических средств в автономных телеметрических устройствах

Иванов Владимир Евгеньевич, директор по развитию, компания Актив

В докладе рассмотрены два конкретных примера реализации функций криптографической защиты коммуникаций с автономными телеметрическими устройствами. Описаны задачи и ограничения, стоящие перед разработчиками автономных устройств и способы их решения с использованием аппаратных криптографических средств.

Их нравы. Некоторые особенности применения криптографии в Intel ME 11

Скляров Дмитрий, руководитель отдела анализа приложений, Positive Technologies
Горячий Максим, старший специалист отдела исследований безопасности ОС и аппаратных решений, Positive Technologies

В докладе будут описаны свойства аппаратных криптографических средств, реализованных в Intel ME 11, а также «Best practices» построения безопасной вычислительной среды на базе доступных аппаратных решений.

15:00 – 16:30 Секция «Криптография и криптоанализ». 4 часть

О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС

Дмух Андрей Александрович, Трифонов Дмитрий Игоревич, Чухно Андрей Борисович, ТК26

В докладе указываются неточности, выявленные в работе Tomer Ashur, Achiya Bar -On, Orr Dunkelman. Cryptanalysis of GOST2 (опубликована eprint.iacr.org/2016/532), посвященной методу определения ключа алгоритма 2-ГОСТ с использованием неподвижных точек преобразования зашифрования. В докладе предложена модификация ключевой развертки алгоритма 2-ГОСТ, исключающая, в том числе, возможность применения метода определения ключа с использованием неподвижных точек преобразования зашифрования. Получены результаты, характеризующие сложность реализации на ПЛИС алгоритма 2-ГОСТ с модифицированной ключевой разверткой.

Метод параллельных защищенных вычислений систем линейных уравнений с трех диагональной матрицей на основе полностью гомоморфного шифрования для рациональных чисел

Кренделев Сергей Федорович, к.ф.-м.н., Лаборатория криптографии JetBrains, Новосибирский государственный университет
Вишневский Артем Константинович, к.т.н., Военная академия РВСН им. Петра Великого

В докладе предложен метод полностью гомоморфного шифрования, основанный на преобразованиях линейной алгебры, который позволяет выполнять защищенную обработку целых и рациональных чисел. Доказано, что шифрование устойчиво к методу взлома прямым перебором. Построена модель параллельных защищенных вычислений систем линейных уравнений с трех диагональной матрицей для метода прогонки. Ключевая особенность данного подхода заключается в применении модулярной арифметики к рациональным числам, что обеспечивается путем сопоставления рациональных чисел векторам с целочисленными коэффициентами, при этом достигается параллелизм вычислений по каждому модулю. Контроль ошибок вычислений обеспечивается введением избыточных модулей.

К вопросу о методах организации квантовых сетей
Жиляев Андрей Евгеньевич, исследователь, ИнфоТеКС
Николаева Анастасия Сергеевна, исследователь, ИнфоТеКС

В работе рассматриваются варианты построения сетей с использованием квантового распределения ключей. Проводится сравнение полносвязных сетей, построенных с применением различных аппаратных устройств. Также проводится анализ способов применения и управления полученными квантовыми ключами. Разбираются варианты создания ключевой пары между двумя любыми узлами сети, использующие различные каналы передачи ключевой информации. Рассматривается возможность применения каждого варианта в зависимости от ценности передаваемой информации и потребностей сети. Поставлена проблема использования одноразового блокнота при условии необходимости загрузки ключа одноразового блокнота в шифрующее оборудование

О некоторых актуальных направлениях исследований в области квантовой криптографии
Корольков Андрей Вячеславович, к.ф.-м.н., с.н.с., Московский технологический университет

В докладе будет представлен краткий обзор текущего состояния и актуальных направлений исследований в области отечественной квантовой криптографии.

15:00 16:30 Секция «Обеспечение киберустойчивости цифровой экономики и цифрового производства»

Современный уровень технологического развития мировой промышленности характеризуется переходом на цифровое производство, основу которого составляют «умные» устройства, сенсоры, исполнительные механизмы и интеллектуальные системы, автономно от человека реализующие технологические процессы. Какие угрозы кибербезопасности порождает глобальная цифровизация производства? Как от них защититься? Достаточно ли существующих средств защиты или необходимо разрабатывать новые? Как не потерять управление и обеспечить киберустойчивость цифрового производства и цифровой экономики? На эти и многие другие вопросы постараются ответить в своих докладах участники данной секции.

Ведущий: Зегжда Петр Дмитриевич, кафедра «Информационная безопасность компьютерных систем» СПбПУ, ООО«НеоБИТ»

Подходы к обеспечению киберустойчивости цифровой экономики и цифрового производства
Зегжда Петр Дмитриевич, Москвин Дмитрий Андреевич, кафедра ИБКС СПбПУ

Переход промышленности на ЦП сопряжен с рядом трудностей, связанных с применением оборудования десятков различных производителей, плохо налаженным информационным взаимодействием между различными сегментами, отсутствием единого подхода к обеспечению кибербезопасности и высокой зависимостью от персонала. Промышленные предприятия быстро оснащаются новейшими системами. Однако ввиду масштабности решаемых задач, вопросам кибербезопасности и киберустойчивости управления, уделяется недостаточно внимания. В докладе приводятся подходы к обеспечению кибербезопасности ЦП, которые должны позволить успешно противостоять многочисленным и разнообразным угрозам безопасности, действующим в современном киберпространстве, и главным образом тем, которые носят целенаправленный характер. При этом следует учитывать, что защищенной может считаться только та система, которая успешно и эффективно противостоит киберугрозам.

***Применение чесночной маршрутизации для обеспечения безопасного взаимодействия сегментов сети цифрового производства*[1]**

Дахнович Андрей Дмитриевич, кафедра ИБКС СПбПУ

В рамках доклада приводятся особенности обеспечения кибербезопасности в промышленных сетях нового поколения, анализируются основные угрозы и недостатки применения существующих средств защиты. Для обеспечения безопасного сетевого взаимодействия между различными сегментами цифрового производства предлагается применить механизм чесночной маршрутизации.

Применение технологии blockchain для обеспечения безопасности в распределенных системах хранения и обработки данных

Мясников Алексей Владимирович, ООО «НеоБИТ»

В рамках данного доклада рассматриваются архитектуры современных систем децентрализованного хранения и обработки данных, применение технологии blockchain в этих системах, существующие угрозы безопасности, методы обеспечения безопасности, позволяющие избежать данных угроз, перспективность создания, поддержания и разработки подобных распределённых систем и применимость их в рамках цифровой экономики.

Оценка робастности методов машинного обучения, применяемых в средствах защиты цифрового производства

Жуковский Евгений Владимирович, ООО «НеоБИТ»

В докладе будет представлена оценка эффективности методов машинного обучения на примере решения задачи обнаружения вредоносного программного обеспечения. Представлен анализ методов машинного обучения, используемых для обнаружения ВПО и приведены примеры построения моделей для решения данной задачи. Также будут указаны основные возможности по противодействию построенным моделям и предложены подходы к повышению устойчивости моделей к атакам.

***Метод контроля и поддержания связности узлов в крупномасштабных коммуникационных сетях беспилотного транспорта*[2]**

Бусыгин Алексей Геннадьевич, кафедра ИБКС СПбПУ.

В работе рассмотрена задача обеспечения связности узлов в самоорганизующихся сетях. Предложено использование системы хранения и распространения информации о топологии сети и данных аутентификации узлов с помощью технологии Блокчейн. Рассмотрена проблема неограниченного роста блокчейна, препятствующая внедрению предложенного метода в крупномасштабных децентрализованных сетях. Выполнен анализ и выявлены недостатки существующих решений данной проблемы. Введено понятие блокчейна с плавающим генезис-блоком и показаны его преимущества перед аналогами, делающие возможным его применение для решения проблемы постоянно растущего блокчейна в крупномасштабных децентрализованных сетях.

[1] При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы». Соглашение № 14.578.21.0231 от 26.09.2017, уникальный идентификатор соглашения RFMEFI57817X0231.

[2] При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение о предоставлении субсидии № 14.578.21.0224 от 03.10.2016, уникальный идентификатор соглашения RFMEFI57816X0224).

Применение мультифрактальных и вейвлет-эвристик для обнаружения аномалий в сверхвысоких объемах трафика сетевой инфраструктуры цифрового производства

Штыркина Анна Александровна, Лаврова Дарья Сергеевна, кафедра ИБКС СПбПУ [3]

В докладе предлагается подход к обнаружению аномалий в сверхвысоких объемах трафика сетевой инфраструктуры цифрового производства. В основе подхода лежит вычисление мультифрактальных и вейвлет-характеристик над временными рядами, сформированными из параметров сетевых пакетов. В докладе также описан метод сокращения размерности объема трафика на основе иерархически-зависимых окон агрегации, позволяющий значительно уменьшить объем обрабатываемых данных и повысить скорость их обработки.

17:00 – 19:30 Круглый стол «Роль российского экспертного сообщества в разработке международных стандартов и рекомендаций в области криптографии и защиты информации»

Направления международной стандартизации, которые сейчас охватываются российским экспертами. Степень их представительства в международных организациях. Заинтересованность участия в деятельности по разработке международных стандартов зарубежных представителей и иностранных компаний. Проблемы, возникающие при работе российских экспертов в международных организациях по стандартизации. Перспективные направления и задачи в области международной стандартизации, стоящие перед российским экспертным сообществом.

Эксперты круглого стола:

Матюхин Дмитрий Викторович, к.ф.-м.н., ФСБ России, зам. Председателя ТК 26 «Криптографическая защита информации», эксперт GOST_R в ISO/IEC JTC1/SC27 «IT Security techniques» и ISO /TC 307 «Blockchain and distributed ledger technologies»

Голованов Владимир Борисович, НПФ «Кристалл», эксперт ТК 22, ТК 26, ТК 122, ТК 362,эксперт GOST_R в ISO/IEC JTC1/SC27 «IT Security techniques»

Шишкин Василий Алексеевич, к.ф.-м.н., эксперт ТК 26 «Криптографическая защита информации», эксперт GOST_R и глава делегации РФ в ISO/IEC JTC1/SC27 «IT Security techniques»

Смышляев Станислав Витальевич, к.ф.-м.н., КРИПТОПРО, эксперт ТК 26 «Криптографическая защита информации», член экспертного совета Crypto Review Panel IETF

Шевченко Максим Александрович, «ИнфоТеКС»**,** эксперт ТК 26 «Криптографическая защита информации»**,** эксперт GOST_R в ISO/IEC JTC1/SC27 WG2 «Cryptography and security, mechanisms» и ISO /TC 307 «Blockchain and distributed ledger technologies» WG «Security and Privacy»

Сабанов Алексей Геннадиевич, к.т.н.**,** Аладдин Р.Д.**,** эксперт ТК122 «Стандарты финансовых операций», ТК 362 «Защита информации»**,** эксперт GOST_R в ISO/IEC JTC1/SC27 WG5 «Identity management and privacy technologies»

Аксененко Юрий Иванович, к.т.н., «Центр безопасности информации», эксперт ТК 362 «Защита информации»

Сидак Алексей Александрович, к.т.н., «Центр безопасности информации», эксперт ТК 362 «Защита информации», эксперт GOST_R в ISO/IEC JTC1/SC27 WG3 «Security evaluation, testing and specification» и ISO/IEC JTC1/SC27 WG4 «Security controls and services»

[3] При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП “Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы”. Соглашение № 14.578.21.0231 от 26.09.2017, уникальный идентификатор соглашения RFMEFI57817X0231.

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

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

Направления исследований в области Advanced Security Analytics

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

Рассматривается современное состояние исследований и разработок в области Advanced Security Analytics. Представляются модели, методики, методы и средства для использования технологий Advanced Security Analytics в перспективных компонентах SIEM-систем и SOC. Приводятся примеры разработанных компонентов, выделяются перспективные направления исследований и разработок.

Современные подходы к управлению рисками кибербезопасности

Минзов Анатолий Степанович, д.т.н., профессор, МЭИ

Анализируются различные концепции построения систем информационной безопасности на основе моделирования рисков. Представляются подходы к оценке показателей рисков и стратегии управления ими. Предлагаются механизмы выделения агрегатов рисков, связанных между собой по угрозам, уязвимостям, информационным активам и принимаемым контрмерам. На конкретном примере рассматривается методика моделирования рисков при различных стратегиях.

Методика разработки защищенных систем, содержащих встроенные устройства

Чечулин Андрей Алексеевич, к.т.н., СПбГУТ

Представляется подход, позволяющий повысить защищенность разрабатываемых систем, содержащих встроенные устройства, за счет выбора программно-аппаратных компонент и протоколов взаимодействия, удовлетворяющих требованиям безопасности. Предполагается, что данный подход может использоваться при производстве IoT-систем.

Системы защиты авторских прав, использующие неоднородную структуру защищаемой информации

Беззатеев Сергей Валентинович, д.т.н., профессор, ГУАП
Волошина Н.В., к.т.н., Университет ИТМО

Рассматриваются методы встраивания информации о владельце в медиафайлы, использующие их психо-визуальную и психо-акустическую неоднородность. Определяются различные варианты метрик, наиболее точно учитывающие такую неоднородность. Для выбранных метрик приведены кодовые конструкции, позволяющие построить эффективные системы встраивания. Для оценки эффективности используются величина внесенных искажений, учитывающая их значимость и объем встроенной информации.

Моделирование энергоатак на автономные IoT-устройства

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

Проводится анализ атакующих воздействий на автономно работающие устройства Интернета вещей. Представляются результаты экспериментов по моделированию атак типа denial-of-sleep на устройства беспроводных сетей на базе ОС Android и платформы Digi XBee.

Способы вычисления критериев схожести событий безопасности для процесса корреляции
Федорченко А.В., Университет ИТМО

Рассматриваются особенности событий безопасности как исходных данных для вычисления состояния защищенности условно-неопределенных инфраструктур. Описываются существующие способы оценки схожести объектов для ряда интеллектуальных методов анализа данных и возможность их применения для вычисления расстояний между событиями безопасности. Приводится подход вычисления критериев схожести между событиями для процесса корреляции, основанного на структурном и содержательном анализе исходных данных.

Обманные способы уклонения от сигнатурных правил сетевых систем обнаружения атак
Браницкий А.А., СПИИРАН

Представляются результаты экспериментального исследования нескольких сетевых систем обнаружения атак (СОА). Рассматривается несколько сценариев, представленных в виде последовательностей сетевых пакетов и позволяющих обойти сигнатурные правила этих СОА. Предлагаются рекомендации для предотвращения таких случаев.

Социальные механизмы обеспечения информационной безопасности в кибер-физических системах
Викснин Илья Игоревич, Университет ИТМО

Рассматривается построение модели обеспечения информационной безопасности (ИБ) кибер-физических систем (КФС) на основе социальных механизмов. Анализированы подходы к обеспечению ИБ в мультиагентных системах на основе социальных моделей. Предложенные модели были адаптированы для КФС, проанализирована их эффективность и разработана собственная модель на основе репутации и доверия. Разрабатываемая модель позволит повысить эффективность противодействия различным атакам на ИБ КФС.

Подход к внедрению робастного водяного знака в текстовые данные
Козачок Александр Васильевич, к.т.н., Академия ФСО России
Копылов Сергей Александрович, Академия ФСО России

Рассматриваются варианты стеганографического встраивания информации в текстовые данные. Обосновывается необходимость внедрения робастного водяного знака, устойчивого к преобразованию «печать-сканирование». Представляются численные оценки по емкости встраивания при различных параметрах текстовых документов, алгоритмы внедрения и извлечения робастного водяного знака, а также оценка точности извлечения внедренной информации и устойчивости к различным преобразованиям изображений.

Защита обрабатываемых данных от фишинговых атак
Щеглов К.А., ООО «НПП «ИТБ»
Щеглов А.Ю., д.т.н. профессор, ООО «НПП «ИТБ»

Рассматривается предлагаемая авторами технология анти-фишинговой защиты, основанная на контроле доступа к создаваемым файлам. Каждый файл при создании автоматически размечается, в его альтернативный поток помещаются учетные данные создавшего файл субъекта доступа, в данном случае процесса. Разграничительной политикой доступа определяется, какому субъекту к файлам, созданным каким субъектом, разрешает доступ, и какой доступ – чтение, запись, исполнении и т.д.

Инфраструктура для обнаружения источников сетевых вторжений с элементами технологии программно-конфигурируемых сетей

Сагатов Евгений Собирович, к.т.н., доцент, Самарский университет
Шкирдов Данила Андреевич, Самарский университет
Сухов Андрей Михайлович, д.т.н., профессор, Самарский университет
Салимов Арсен Серверович, Крымский федеральный университет

Рассматривается опыт создания инфраструктуры серверов-ловушек, территориально расположенных в России и США. На этих серверах были инсталлированы 10 наиболее популярных интернет протоколов и целый год собиралась статистика доступа к этим ресурсам. Так как информационное наполнение сервисов не проводилось, а IP-адреса не анонсировались и не вносились в DNS, то большинство запросов можно считать несанкционированными. Была собрана и обработана годовая статистика. На основе этой статистики были сформированы списки IP-адресов, которые участвовали в попытке неправомерного доступа, а также подробно представлена статистика осуществления вторжений. Были предложены подходы к ограничению несанкционированного доступа с помощью технологий программно-конфигурируемых сетей.

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. В течение 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:

- Единственный учебный центр, который проводит разноплановое обучение по направлению «Конкурентная разведка»;
- Всестороннее обучение для банков: НПС, СТО БР, 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.;
- 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

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

- первое в России сертифицированное СКЗИ, интегрированное с ОС Microsoft Windows – КриптоПро CSP;
- первое в России сертифицированное средство обеспечения деятельности удостоверяющих центров – КриптоПро УЦ;
- первые в России сертифицированные службы актуальных статусов сертификатов и штампов времени – КриптоПро OCSP и КриптоПро TSP;
- первые в России сертифицированные аппаратные криптографические модули – Атликс HSM и КриптоПро HSM;
- первые в истории сообщества Интернет стандарты, описывающие применение российских криптоалгоритмов – RFC 4357, RFC 4490, RFC 4491, RFC 7836, RFC 8133;
- первые стандартизированные параметры эллиптических кривых для российских алгоритмов электронной подписи, а также сопутствующие криптографические алгоритмы (HMAC, KDF, PRF, VKO) для российского стандарта функции хэширования;
- первый в России стандартизированный протокол для защиты взаимодействия с ключевыми носителями (SESPAKE) и реализующие его СКЗИ;
- первые утвержденные методические рекомендации по применению российских криптографических алгоритмов в протоколах TLS, IPsec, CMS;
- первое в России сертифицированное СКЗИ, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture) – КриптоПро JCP;
- первое в России «облачное» решение, получившее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» для централизованного применения (создания и проверки) электронной подписи, создания и хранения пользовательских ключей электронной подписи, – КриптоПро DSS.

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.

КриптоПро ведет непрерывную разработку в целях улучшения имеющихся программных продуктов и создания нового ПО, призванного оперативно решать новые задачи, возникающие в сфере защиты информации.

www.cryptopro.ru

Серебряный спонсор – 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 спонсор – 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 спонсор – Компания Фактор-ТС

Компания Фактор-ТСвыпускает программно-аппаратные комплексы для защиты информации уже 25 лет. 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. Dionis DPS включает в себя: криптографическую защиту (сертификат ФСБ, класс защищенности КС1, КС3), функции маршрутизатора, межсетевого экрана и сертифицированную ФСТЭК систему обнаружения и предотвращения вторжений IPS/IDS.

www.factor-ts.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 – ООО «Открытая Мобильная Платформа»

ООО «Открытая Мобильная Платформа» является разработчиком Sailfish Mobile OS RUS, первой отечественной операционной системы для мобильных устройств, и Sailfish Cloud RUS, сопутствующего облачного решения, предоставляющего средства для удаленного управления мобильными устройствами. Основной целью компании является создание продуктов, с помощью которых можно организовать надёжную и доверенную инфраструктуру для работы с мобильными устройствами. С 2016 года «Открытая Мобильная Платформа» активно и успешно сотрудничает с лидерами корпоративного рынка и государственными компаниями, создавая совместные решения и внедряя свои продукты. Также компания «Открытая Мобильная Платформа» взаимодействует с сообществом разработчиков и университетами, организовывает тренинги и учебные курсы.

www.omprussia.ru

Партнер – Check Point® Software Technologies Ltd.

Check Point® Software Technologies Ltd. является крупнейшим в мире вендором, специализирующимся исключительно на сетевой кибербезопасности. Предоставляет ведущие решения в области информационной безопасности и обеспечивает клиентам защиту от кибератак с непревзойденным уровнем обнаружения вредоносного ПО и других видов угроз. Check Point предлагает полноценную архитектуру защиты корпоративных сетей и мобильных устройств, а также возможность всестороннего и наглядного управления безопасностью. Check Point защищает более 100 тысяч организаций по всему миру. В Check Point мы создаем безопасное будущее.

www.checkpoint.com

Партнер – «Код Безопасности»

«Код Безопасности» - российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям российских, отраслевых и международных стандартов. Продукты «Кода Безопасности» применяются для защиты конфиденциальной информации, коммерческой тайны, персональных данных и сведений, составляющих государственную тайну. «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации. Сервисный центр компании готов предоставить профессиональную техническую поддержку партнерам и Заказчикам компании 24 часа и 7 дней в неделю.

www.securitycode.ru

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
- Построение SOC и подключение к системе ГосСОПКА
- Сертификационные и тематические исследования на соответствие требованиям по информационной безопасности ФСТЭК, ФСБ и МО России
- Специальные проверки и обеспечение кибербезопасности транспортных средств
- 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 – 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 – Trend Micro Incorporated

Trend Micro Incorporated, мировой лидер в области решений по кибербезопасности, видит свою миссию в том, чтобы сделать безопасным обмен цифровой информацией во всем мире. Наши инновационные решения для домашних пользователей, бизнеса и госструктур обеспечивают многоуровневую защиту центров обработки данных, облачных инфраструктур, сетей и конечных точек. Наши решения, оптимизированные для лидирующих инфраструктур, включая Amazon Web Services, Microsoft® и VMware® и др., позволяют организациям автоматизировать процесс защиты информации от современных угроз. Все наши продукты работают в тесной взаимосвязи между собой для обмена данными об угрозах и обеспечивают комплексную защиту с централизованным управлением, предоставляя более качественную защиту и быстрое реагирование.

Trendmicro.com.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 – АБИСС

Ассоциация пользователей стандартов по информационной безопасности «АБИСС», именуемая в дальнейшем "Ассоциация", является некоммерческой организацией, основанной на принципах добровольного объединения ее членов – субъектов предпринимательской деятельности, оказывающих услуги в области обеспечения информационной безопасности в организациях, созданной в целях разработки и установления стандартов и правил осуществления такой деятельности, а также в целях осуществления контроля за соблюдением членами Ассоциации требований указанных стандартов и правил. Ассоциация создана в 2006 году. Ассоциация «АБИСС» является официальным переводчиком стандарта PCI DSS 3.2

www.abiss.ru

РОССИЙСКИЙ
разработчик
и производитель

Входим в
ТОП-20
компаний в сфере
защиты информации

Более
20 лет
на рынке ИБ

Лучшие
ЭКСПЕРТЫ
отрасли

ПРОДУКТЫ
И РЕШЕНИЯ
для государственного,
коммерческого
и финансового сегментов

БОЛЕЕ 1000
реализованных
проектов

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

РУТОКЕН

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

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

Guardant

Средства защиты
и лицензирования
программного обеспечения.

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

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

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

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

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

Более 20 лет в сфере образования

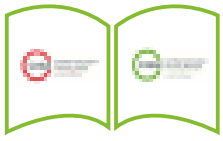
Программы повышения квалификации и профессиональной переподготовки, согласованные с ФУМО ИБ, ФСТЭК РФ, ФСБ РФ Банком России, в том числе, с выдачей диплома МГТУ им. Н.Э. Баумана

Более 300 курсов по направлению «Информационные технологии»

Обучение для банков: НПС, СТО БР, Стандарт PCI DSS, защита ДБО, расследование компьютерных преступлений, аудит безопасности, управление рисками и др.

Единственный учебный центр, который проводит комплексное обучение по направлению «Конкурентная разведка»

Обучение по защите АСУ ТП, управлению электронным документооборотом, экономической безопасности и пр.



Подготовка к международным сертификациям CISA, CISM, CGEIT и т.п.

Технологии дистанционного обучения, вебинары и онлайн-тестирования

Симуляционные деловые игры по управлению проектами, а также подготовка к сертификации PMI

АИС МЕРОПРИЯТИЯ

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.
Деловые мероприятия АИС проходят при поддержке и активном участии государственных ведомств и регуляторов, в числе которых аппарат Совета Безопасности РФ, Государственная Дума ФС РФ, Минкомсвязи России, МВД России, Министерство обороны РФ, Минэкономразвития РФ, ФСБ России, ФСТЭК России, а также ряда ассоциаций и общественных организаций Российской Федерации.

НАШИ КОНТАКТЫ: info@infosystem.ru +7 (495) 120-04-02 www.infosystems.ru www.vipforum.ru

КАЛЕНДАРЬ МЕРОПРИЯТИЙ

ИЮНЬ 2018

VI ВСЕРОССИЙСКАЯ ОТРАСЛЕВАЯ КОНФЕРЕНЦИЯ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И КВО ТЭК

www.vipforum.ru

Главная тема: Организационно-правовые и технические аспекты обеспечения безопасности АСУ ТП и станков с ЧПУ на промышленных предприятиях и объектах ТЭК, антитеррористическая защита объектов.

4-7 СЕНТЯБРЯ 2018

XVII ВСЕРОССИЙСКИЙ ФОРУМ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. РЕГУЛИРОВАНИЕ. ТЕХНОЛОГИИ. ПРАКТИКА.

ИНФОБЕРЕГ - 2018

www.vipforum.ru

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

23-26 ОКТЯБРЯ 2018

X МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ В СФЕРЕ ЭЛЕКТРОННОЙ ТОРГОВЛИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И PKI

www.pki.ineurasia.ru

Главная тема: В центре - дискуссии экспертов вокруг наиболее значимых вопросов развития электронной коммерции и электронных услуг в разрезе законодательных условий применения электронной подписи.

НОЯБРЬ 2018

VI НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И КОНКУРЕНТНАЯ РАЗВЕДКА

www.vipforum.ru

Главная тема: Самые актуальные и интересные доклады в области экономической безопасности, конкурентной разведки, информационного противоборства и аналитики. Лучшие практики и готовые решения по защите бизнеса.

ДЕКАБРЬ 2018

IX МЕЖДУНАРОДНЫЙ ФОРУМ «БОРЬБА С МОШЕННИЧЕСТВОМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ»

ANTIFRAUD RUSSIA - 2018

www.vipforum.ru

Главная тема: Организационные, юридические и технологические аспекты решения проблем борьбы с мошенничеством. Управление рисками, практика расследования инцидентов и привлечение к ответственности злоумышленников.

МАРТ 2019

XXI НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУСКРИПТО'2019

www.ruscrypto.ru

Главная тема: Использование криптографических средств и методов защиты информации, юридическое оформление электронного документооборота, обзоры основных достижений криптологии, криптографии.

www.ruscrypto.ru