ОРГАНИЗАТОРЫ

Ассоциация РусКрипто

АИС

ПРОГРАММА КОНФЕРЕНЦИИ

21-24 марта 2017 г.

www.ruscrypto.ru

КЛЮЧЕВОЕ СЛОВО

В ЗАЩИТЕ ИНФОРМАЦИИ

СКАЧИВАЙТЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ РУСКРИПТО’2017

- **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**

Спонсоры и партнеры конференции

Золотой спонсор

КРИПТОПРО
ключевое слово в защите информации

Серебряные спонсоры

Компания АКТИВ

infotecs

BIFIT

Бронзовый спонсор

ФАКТОР-ТС

Научный партнер

НЕОБИТ

Партнеры конференции

ISBC
Группа компаний

АПКИТ

Код безопасности

НЕКОММЕРЧЕСКОЕ ПАРТНЕРСТВО
РОСЭУ
НАЦИОНАЛЬНЫЕ ЭЛЕКТРОННЫЕ УСЛУГИ

Check Point
SOFTWARE TECHNOLOGIES LTD.

НИИМЭ
НИИ МОЛЕКУЛЯРНОЙ ЭЛЕКТРОНИКИ

ФГУП
"НПП "Гамма"

АЗИ

Информационная поддержка

RUБЕЖ
Информационно-аналитический журнал

kartoteka.ru

POSITIVE TECHNOLOGIES

Деловая Трибуна

Единый портал
Электронной подписи

ГАРАНТ
ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

BIS JOURNAL
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

Таймлайн конференции

21 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

22 марта, среда. Первый день работы конференции

8:00 — 9:00	Завтрак	
9:00 — 9:50	Регистрация участников конференции	
10:00 — 11:30	Официальное открытие конференции **Пленарное заседание** *Конференц-зал «Шишка», 2 этаж* *Подробнее на стр. 7*	
11:30 — 12:00	Кофе-брейк	
12:00 — 14:00	**Круглый стол «Будущее электронной подписи и удостоверяющих центров в России»** *Конференц-зал «Шишка», 2 этаж* Ведущие: · **Маслов Ю.Г.**, РОСЭУ, КриптоПро · **Малинин Ю.В.,** АИС *Подробнее на стр. 7*	**Секция «Цифровая криминалистика»** *Конференц-зал «Еловый», 1 этаж* Ведущие: · **Чиликов А.А.**, МГТУ им. Н.Э. Баумана · **Яковлев А.Н.**, СК РФ *Подробнее на стр. 8*
14:00 — 15:00	Обед	

15:00 — 16:30	**Секция «Криптография и криптоанализ». Часть I** *Конференц-зал «Шишка», 2 этаж* Ведущие: · **Матюхин Д.В.**, ФСБ России · **Попов В.О.**, КриптоПро, РусКрипто · **Жуков А.Е.**, МГТУ им. Баумана, РусКрипто *Подробнее на стр. 10*	**Секция «Нестандартные применения криптографии»** *Конференц-зал «Еловый», 1 этаж* Ведущий: **Лукацкий А.В.**, Cisco Solutions *Подробнее на стр. 12*	**Секция «Час с экспертом»** *Конференц-зал «Сосновый», 1 этаж* Ведущий: **Кузнецов А.Ю.**, Минкомсвязь России *Подробнее на стр. 12*
16:30 — 17:00	Кофе-брейк		
17:00 — 19:00	**Секция «Криптография и криптоанализ». Часть II** *Конференц-зал «Шишка», 2 этаж* Ведущие: · **Матюхин Д.В.**, ФСБ России · **Попов В.О.**, КриптоПро, РусКрипто · **Жуков А.Е.**, МГТУ им. Баумана, РусКрипто *Подробнее на стр. 13*	**Секция «Криптография в кредитно-финансовой сфере»** *Конференц-зал «Еловый», 1 этаж* Ведущие: · **Простов В.М.**, ФСБ России · **Гусев Д.М.**, ИнфоТеКС *Подробнее на стр. 14*	**Секция «Цифровая (электронная) экономика»** *Конференц-зал «Сосновый», 1 этаж* Ведущий: **Димитров И.Д.**, омбудсмен по электронной торговле и предоставлению государственных и муниципальных услуг в электронной форме *Подробнее на стр. 16*
19:00	Ужин		
20:00 — 22:00	**Торжественное открытие конференции «РусКрипто»** *Киноконцертный зал (Ресторанный комплекс)*		

23 марта, четверг. Второй день работы конференции

8:00 — 10:00	Завтрак	
10:00 — 12:00	**Секция «Криптография и криптоанализ». Часть III** *Конференц-зал «Шишка», 2 этаж* Ведущие: · **Матюхин Д.В.**, ФСБ России · **Попов В.О.**, КриптоПро, РусКрипто · **Жуков А.Е.**, МГТУ им. Баумана, РусКрипто *Подробнее на стр. 16*	**Секция «Практика применения средств информационной безопасности»** *Конференц-зал «Еловый», 1 этаж* Ведущий: **Горелов Д.Л.**, Актив, РусКрипто *Подробнее на стр. 17*
12:00 — 12:30	Кофе-брейк	
12:30 — 14:00	**Секция «Информационная безопасность и криптография в средствах мгновенной передачи сообщений (мессенджерах)»** *Конференц-зал «Шишка», 2 этаж* Ведущие: · **Качалин А.**, Positive Technologies · **Смышляев С.**, КриптоПро · **Василенков А.**, ИнфоТеКС *Подробнее на стр. 19*	**Круглый стол «Безопасная дорога в облака»** *Конференц-зал «Еловый», 1 этаж* Ведущие: · **Баранов А.П.**, ГНИВЦ ФНС России · **Бражников Ю.Н.**, RCCPA, 5nine Software *Подробнее на стр. 20*
14:00 — 15:00	Обед	

15:00 — 16:30	**Круглый стол «Электронный документооборот»** *Конференц-зал «Шишка», 2 этаж* Ведущие: Эксперты: · **Миклашевич А.В.**, РОСЭУ · **Соловяненко Н.И.**, ИГП РАН, АИС · **Соловьев Н.Н.**, Гроссмейстер · **Курило А.П.**, Финансовый университет · **Казаков С.С.**, СКБ Контур *Подробнее на стр. 21*	**Секция «Технологии анализа, моделирования и трансформации программ для создания безопасного программного обеспечения»** *Конференц-зал «Еловый», 1 этаж* Ведущие: · **Девянин П.Н.**, ФУМО ВО ИБ · **Аветисян А.И.**, ИСП РАН *Подробнее на стр. 21*	**Секция «Информационная безопасность киберфизических систем и динамических сетей»** *Конференц-зал «Сосновый», 1 этаж* Ведущий: **Зегжда П.Д.**, СПбПУ ИБКС *Подробнее на стр. 23*
16:30 — 17:00	Кофе-брейк		
17:00 — 19:00	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал «Шишка», 2 этаж* Ведущий: **Котенко И.В.**, СПИИРАН *Подробнее на стр. 26*	**Мастер-класс «Электронное правосудие»** *Конференц-зал «Еловый», 1 этаж* Ведущий: **Соловяненко Н.И.**, ИГП РАН, АИС *Подробнее на стр. 28*	
19:00	Ужин		
20:00 — 22:00	**Интеллектуальная игра «Что? Где? Почему?»** *Киноконцертный зал (Ресторанный комплекс)*		

24 марта, пятница. День отъезда

9:00 — 11:00	Завтрак
12:00	Трансфер отель «Солнечный Park Hotel & SPA» — м. Речной вокзал

Первый день работы конференции

10:00–11:30	**Официальное открытие конференции. Пленарное заседание** *Конференц-зал «Шишка», 2 этаж*

Национальная и международная стандартизация в области криптографии
Качалин Игорь Федорович, *ФСБ России*
Матюхин Дмитрий Викторович*, ФСБ России*

Информационная безопасность больших данных в массовых системах
Баранов Александр Павлович*, д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

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

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

12:00–14:00	**Круглый стол «Будущее электронной подписи и удостоверяющих центров в России»** *Конференц-зал «Шишка», 2 этаж*

Ведущие:
- **Маслов Юрий Геннадьевич,** РОСЭУ, КриптоПро
- **Малинин Юрий Витальевич,** Академия Информационных Систем

Эксперты:
- **Кузнецов Александр Юрьевич, правовой департамент** Минкомсвязь России
- **Перевалов Иван Ярославович,** ФГБУ НИИ «Восход»
- **Лабуцкая Анастасия Сергеевна**, Опора России, СКБ Контур
- **Миклашевич Анатолий Вадимович,** Ассоциация РОСЭУ
- **Панов Валентин Николаевич**, Ассоциация Удостоверяющих центров
- **Соловяненко Нина Ивановна**, Институт государства и права РАН, эксперт АИС

За последнее десятилетие сформировалась целая отрасль в сфере информационных технологий связанная с электронной подписью. В стране действует несколько сотен коммерческих удостоверяющих центров. Подавляющее большинство каналов взаимодействия бизнеса и государства переведены на электронные рельсы и используют электронную подпись. С каждым днем появляется все больше электронных услуг для предприятий и граждан где электронная подпись обязательный и неотъемлемый компонент. Что нужно сделать, чтобы электронная подпись была благом, а не обузой пользователей? Куда движется рынок электронной подписи? Какие внешние и внутренние угрозы ждут электронную подпись в России?

Выступления в рамках круглого стола:

Перевод инфраструктуры открытых ключей Российской Федерации на применение криптографических стандартов нового поколения
Перевалов Иван Ярославович, *ФГБУ НИИ «Восход»*
В минувшем году Министерство связи и массовых коммуникаций РФ и ФГБУ НИИ «Восход» предприняло ряд шагов, направленных на осуществление плавного перехода отечественной инфраструктуры открытых ключей на применение криптографических стандартов ЭП и Хэш-функции 2012 года. Доклад посвящается результатам прошлого года, а также взгляду ФГБУ НИИ «Восход» на решение актуальных проблем в рамках перехода.

Поддержка ЭЦП в ОС из Реестра отечественного ПО
Державин Дмитрий Константинович*, Базальт СПО*
В докладе будут озвучены результаты исследовательской работы по оценке возможности применения в ОС, входящих в Реестр технологий ЭЦП, доступных физическим и юридическим лицам Российской Федерации на общих основаниях.

12:00–14:00	**Секция «Цифровая криминалистика»** *Конференц-зал «Еловый», 1 этаж*

Ведущие:
- **Чиликов Алексей Анатольевич,** к.ф.-м.н., доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана
- **Яковлев Алексей Николаевич,** к.ю.н., доцент, Следственный комитет Российской Федерации

Разработчики экспертного программного обеспечения и оборудования, как участники системы обеспечения информационной безопасности Российской Федерации
Земцов Анатолий Павлович, *генеральный директор Ассоциации «ЭКСПИТ»*
Российские компании-производители специализированного программного обеспечения и оборудования, используемого, в том числе, в сфере правоприменения, криминалистики и судебной экспертизы, являются полноправными участниками единой системы обеспечения информационной безопасности Российской Федерации. Для эффективного и скоординированного решения задач, стоящих перед указанными компаниями и отраслью в целом, была создана Ассоциация производителей программного обеспечения и оборудования для экспертных исследований в сфере высоких технологий «ЭКСПИТ». В докладе будет рассказано о целях и задачах Ассоциации.

Взгляды юристов на цифровую информацию как проблема разработчиков специализированного оборудования и программ

Яковлев Алексей Николаевич, *заместитель руководителя отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики Следственного комитета России; доцент кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы МГТУ им. Н.Э. Баумана*

Прошли времена беззаботного кодирования программ или изготовления оборудования для реализации задач цифровой криминалистики и компьютерно-технической экспертизы. Проблема юридической оценки предназначения оборудования и программ или особенностей их использования существует и крайне остра. При ее непонимании спектр негативных последствий может быть крайне широким — от существенного снижения спроса на продукцию до возбуждения уголовного дела по факту ее изготовления и распространения. В докладе будут кратко представлены заблуждения юристов об ограничениях и запретах на использование специализированного криминалистического и экспертного оборудования и программ, а также дан обзор международной корректной юридической практики.

Восстановление видеоданных из видеорегистратора, поврежденного вследствие криминальных событий

Абрамец Алексей Сергеевич, *старший эксперт отдела компьютерно-технических и инженерно-технических исследований Главного управления криминалистики Следственного комитета России*

Данные на электронном носителе видеорегистратора сегодня в буквальном смысле бесценны. Большое количество преступлений могут оказаться нераскрытыми, если «немой свидетель» произошедшего – видеорегистратор – не «расскажет» объективно о случившемся.

При бытовом использовании видеорегистратора его поломки случайны, незначительны и не имеют существенной значимости. Все меняется при криминальном событии – поломки умышленны, направлены на специальное и безвозвратное удаление видеоинформации, воспрепятствование возможности ее восстановления. В докладе на практических примерах будут раскрыты особенности умышленного повреждения видеорегистраторов, их фактическое влияние на возможность воспроизведения видеозаписей, подходы к восстановлению видеоданных в самом сложном случае – когда электронный носитель информации устройства содержит «сырой» поток данных.

Cobalt Strike в целевых логических атаках на банкоматы

Матвеева Веста Сергеевна, *главный специалист по компьютерной криминалистике, Group-IB*

2016 год в области киберпреступлений был примечателен серией целевых атак на банки в России, странах СНГ, Малайзии и странах Европы. Для этого использовался инструмент, находящийся в публичном доступе "Cobalt Strike". Интерес представляет сторона криминалистики и первичного реагирования, поскольку все компоненты "Cobalt Strike" выполняются только в оперативной памяти. По результатам участия в реагировании на инциденты с "Cobalt Strike" докладчиком будут рассказаны способы выявления зараженных и скомпрометированных машин в сети организации, а также будут даны рекомендации для предотвращения подобных инцидентов в финансовых организациях.

Особенности извлечения данных из мобильных устройств

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

Современные мобильные устройства предоставляют различные программные и аппаратные средства защиты данных, такие как: Screen Lock и Full-Disk Encryption. Несмотря на включенные средства защиты, в ряде случаев возможно извлечь данные из мобильных устройств. В докладе будут описаны различные методы обхода средств защиты данных для различных классов мобильных устройств.

«Волшебный источник»: новые методы поиска и применения данных из RAM для целей криминалистической экспертизы

Чиликов Алексей Анатольевич, *директор по науке Passware, доцент кафедры информационной безопасности МГТУ им. Н.Э. Баумана*

В последние годы стало ясно, что RAM является ценнейшим источником данных при криминалистическом анализе. Создано множество специализированных решений, предназначенных для извлечения и анализа данных из оперативной памяти. Однако не все сценарии анализа легко автоматизировать, и самый лучший инструмент — лишь орудие в руках человека. В рамках данного доклада будут рассмотрены некоторые продвинутые сценарии анализа RAM, позволяющие извлечь ценные артефакты.

15:00–16:30	**Секция «Криптография и криптоанализ», 1 часть** *Конференц-зал «Шишка», 2 этаж*

Ведущие:

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

О принципах разработки и модернизации шифровальных средств.
Бондаренко Александр Иванович, *эксперт ТК 26*
Нестеренко Алексей Юрьевич, *эксперт ТК 26*
В ноябре 2016 года решением заседания Технического комитета по стандартизации «Криптографическая защита информации» рекомендована к утверждению Росстандартом окончательная редакция проекта рекомендаций по стандартизации «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации», которые определяют основные положения по безопасности, необходимые для взаимодействия заказчика и разработчика средств криптографической защиты информации. В представленном докладе планируется раскрыть основные положения данных рекомендаций, а также их роль и взаимосвязь с действующей нормативно-методической базой ФСБ России.

О стойкости некоторых криптографических механизмов в национальной платежной системе «Мир»
Смышляев Станислав Витальевич, *к.ф.-м.н., КриптоПро*
В настоящее время для Российской национальной платежной системы «Мир» на основе российских криптографических стандартов разрабатывается ряд механизмов, обеспечивающих безопасность транзакций на различных уровнях взаимодействия. В докладе будет дан обзор данных алгоритмов и протоколов и будут представлены результаты их криптографического анализа.

Технологии цепной записи данных и распределенных реестров: криптографический скачок вперед, шаг назад или путь в никуда?
Гуселев Антон Михайлович, *эксперт ТК 26*
Лавриков Иван Викторович, *эксперт ТК 26*
Маршалко Григорий Борисович, *эксперт ТК 26*
Шишкин Василий Алексеевич, *эксперт ТК 26*
В докладе рассматривается возможный подход к формализации некоторых базовых понятий, используемых при описании технологии цепной записи данных и распределенных реестров (блокчейн). Указываются возможности по структуризации абстрактной системы, основанной на использовании рассматриваемых технологий, с точки зрения реализуемых функций и задействованных механизмов обеспечения безопасности, а также приводятся подходы к использованию современных криптографических решений для обеспечения безопасности подобных систем.
Криптография и Blockchain, обзор решений и перспективы развития

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

В докладе рассматривается ряд актуальных приложений технологии Blockchain (криптовалюты, распределенные реестры). Будет приведет необходимый для обеспечения безопасности технологии набор криптографических примитивов, алгоритмов и протоколов.

15:00–16:30	**Секция «Нестандартные применения криптографии»** *Конференц-зал «Еловый», 1 этаж*

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

Обнаружение вредоносного кода в зашифрованном TLS-трафике
***Иванов Руслан Витальевич**, эксперт*
В докладе будет рассмотрена работа группы исследователей, в результате которой доказана применимость методов статистического и поведенческого анализа для обнаружения и атрибуции вредоносного ПО, использующего TLS в качестве метода шифрования каналов взаимодействия.

Применение шифрования в качестве метода обезличивания персональных данных
***Лукацкий Алексей Викторович**, бизнес-консультант по безопасности, Cisco Solutions*
В докладе будет рассмотрено применение шифрования для обезличивания персональных данных как сценарий снижения обременений при выполнении требований законодательства по ПДн, а также для обхода ограничений на невозможность хранения ПДн россиян за границей.

Трояны-вымогатели и применяемые ими криптографические средства
***Синицын Федор Александрович**, эксперт, Лаборатория Касперского*
Одними из самых популярных типов вредоносного программного обеспечения являются трояны-вымогатели. В докладе будет рассказано о эволюции троянов-шифровальщиков, о криптографических схемах, применяемых троянами и методах расшифровки данных жертв без знания ключей злоумышленников.

15:00–16:30	**Секция «Час с экспертом»** *Конференц-зал «Сосновый», 1 этаж*

Ведущий: **Кузнецов Александр Юрьевич,** заместитель директора правового департамента, Минкомсвязь России

В рамках секции эксперт правового департамента Министерства связи и массовых коммуникаций Российской Федерации ответит на вопросы представителей

аккредитованных удостоверяющих центров и других игроков российского рынка электронной подписи.

17:00–19:00	**Секция «Криптография и криптоанализ», 2 часть** *Конференц-зал «Шишка», 2 этаж*

Ведущие:

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

О марковских свойствах усредненных разностных характеристик итерационных блочных шифров
Дрелихов Владимир Олегович, *Центр сертификационных исследований*
Никифоров Максим Сергеевич, *Центр сертификационных исследований*
В докладе исследуются марковские свойства разностных характеристик для некоторых вариантов итеративных блочных шифров. Показано, что усредненные по раундовым ключам разностные характеристики обладают марковскими свойствами.

О построении подобного AES блочного шифра с закладкой и о методах его вскрытия (One construction of a backdoored AES-like block cipher and how to break it)
Eric Filiol, Arnaud Bannier, *ESIEA, (C + V) ^ O Lab, Laval, France*
Доклад посвящен методам построения симметричных криптосистем, позволяющих внедрять в них математические закладки на этапе синтеза. Представлен модельный блочный шифр, содержащий закладку и близкий по структуре к AES.

О дифференциальных атаках Н. Куртуа на алгоритм шифрования ГОСТ 28147-89
Тришин Андрей Евгеньевич, *к.ф.-м.н., Центр сертификационных исследований*
Показывается, что указанные в названии доклада атаки не влияют на стойкость алгоритма ГОСТ 28147-89 и, в частности, алгоритма блочного шифрования «Магма» из стандарта ГОСТ Р 34.12-2015. Более того, оценивая характеристики предлагаемых атак в рамках Марковской модели, Н. Куртуа завышает возможности рассматриваемого варианта дифференциального метода применительно к алгоритму ГОСТ 28147-89.

Оценка сложности реализации алгоритма Гровера для перебора ключей блочного алгоритма шифрования «Кузнечик»
Маршалко Григорий Борисович, *эксперт ТК 26*
Рудской Владимир Игоревич, *эксперт ТК 26*
Шишкин Василий Алексеевич, *эксперт ТК 26*

В докладе рассматривается задача определения секретного ключа блочного алгоритма шифрования «Кузнечик» на квантовом компьютере с помощью алгоритма Гровера. В рамках одной из существующих в настоящее время методологий оценки параметров квантового компьютера, производится оценка параметров квантовой схемы, реализующей такой алгоритм.

Простой алгоритм обмена ключами и трех проходной алгоритм шифрования, на модулях над кольцами
Кренделев Сергей Федорович, *к.ф.-м.н., доцент, НГУ, JetBrains*
В работе рассматривается вариант объединения матричных колец и представлении матричных колец в модулях над целыми числами.

Метод полностью гомоморфного шифрования в кольце рациональных чисел
Вишневский Артем Константинович, *к.т.н., Военная академия РВСН им. Петра Великого*
Кренделев Сергей Федорович*, к.ф.-м.н., доцент, НГУ, JetBrains*
В работе построен базовый метод полностью гомоморфного шифрования, отличающийся от известных, возможностью реализации защищенных вычислений над множеством рациональных чисел.

17:00–19:00	**Секция «Криптография в кредитно-финансовой сфере»** *Конференц-зал «Еловый», 1 этаж*

Ведущие:
- **Простов Владимир Михайлович,** ФСБ России
- **Гусев Дмитрий Михайлович,** заместитель генерального директора, ИнфоТеКС

Российские криптографические алгоритмы в национальной платежной системе
Простов Владимир Михайлович, *ФСБ России*
Доклад посвящен технологическим и организационным вопросам внедрения российских криптографических стандартов в инфраструктуре национальной системы платежных карт.

Проблемы внедрения отечественных СКЗИ в платежных системах
Поташников Александр Викторович*, заместитель директора центра разработки, ИнфоТеКС*
Доклад о проблемах внедрения средств криптографической защиты информации отечественного производства в условиях противоречий требований регулятора и международных платежных систем. Перспективы появления отечественных

криптографических алгоритмов в национальной системе платежных карт, организационные и технические проблемы разработки и внедрения новых протоколов.

Особенности применения платежных HSM в процессинговых системах банков
Мареева Елена Владимировна, *заместитель директора по НТР, ООО «Системы практической Безопасности»*
В докладе рассматриваются особенности внедрения средств криптографической защиты информации типа HSM в процессинговые системы банков. Показывается высокий уровень кастомизации разных платежных систем в части взаимодействия с HSM, несмотря на общую декларацию соответствия стандартам Global Platform и сертификации по требованиям PCI DSS/PCI HSM. Объясняется необходимость разработки национальных требований и рекомендаций к платежным банковским системам и HSM, в частности с целью снижения издержек всех заинтересованных сторон в оценке и эксплуатации подобного рода систем.

Практика использования средств криптографической защиты информации и средств электронной подписи в системах дистанционного обслуживания
Горелов Дмитрий Львович*, ассоциация «РусКрипто», Актив*
Предприятия кредитно-финансовой сферы активно развивают дистанционные каналы взаимодействия с клиентами, и тем самым снижают издержки и повышают качество обслуживания. Где и как применяется криптография в системах дистанционного обслуживания, какие технологии востребованы и в каких направлениях идет развитие.

Варианты реализации дистанционной подписи в рамках эксперимента по Постановлению Правительства №1104 от 29.10.2016
Бродский Александр Владимирович, *управляющий директор Департамента безопасности, ПАО «Сбербанк»*
В докладе будут рассмотрены варианты реализации технологии электронной подписи, проработанные в рамках эксперимента по Постановлению Правительства №1104 от 29.10.2016. Возможность использования клиентами банка дистанционной электронной подписи является важной для развития сервиса удаленной регистрации предприятия и открытия банковского счета. Наличие такого сервиса позволит улучшить позицию России в рейтинге Всемирного банка по условиям ведения бизнеса «Doing Business».

О блокчейн платформе для электронных денег государства с применением отечественной криптографии

Комисаренко Владимир Владимирович, *директор по развитию, ЗАО «БЕЛТИМ СБ»*
Доклад посвящен вопросам создания системы электронных платежей с использованием электронных денег нового поколения, внедрение которой приведет к существенной (на порядок) экономии средств. При этом применяются идеи блокчейн и отслеживаются государственные интересы.

17:00–19:00	**Круглый стол «Цифровая (электронная) экономика»** *Конференц-зал «Сосновый», 1 этаж*

Ведущий: **Димитров Илия Димитров,** омбудсмен по электронной торговле и предоставлению государственных и муниципальных услуг в электронной форме

Второй день работы конференции

10:00–12:00	**Секция «Криптография и криптоанализ», 3 часть** *Конференц-зал «Шишка», 2 этаж*

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

Асимметричный SPN-шифр на базе white-box-криптографии и хаотических отображений
Щелкунов Дмитрий Анатольевич, *к.т.н., КФ МГТУ имени Н.Э. Баумана*
Рассматривается технология создания быстрого асимметричного SPN-шифра с помощью хаотических отображений и метода сокрытия линейной зависимости.

Об алгоритмической реализации *s*-боксов
Фомичев Владимир Михайлович, *д.ф-м.н., профессор, НИЯУ МИФИ, Код Безопасности*
Доклад посвящен методам построения нелинейных узлов замены блочных шифров (*s*-боксов). Авторы предлагают метод синтеза *s*-боксов на основе модифицированных аддитивных генераторов.
Оптимизация перспективных постквантовых алгоритмов на малоресурсных микроконтроллерах
Тараскин Олег Геннадьевич, *зам. директора проекта Рутокен по науке, Актив*
В докладе рассматриваются вопросы использования изогений на суперсингулярных эллиптических кривых для алгоритмов ЭЦП и обмена ключами, устойчивых к атакам с использованием квантовых компьютеров. Приводятся примеры их практической реализации на малоресурсных микропроцессорах.

О подходах к испытаниям высокоскоростных СКЗИ
Овчинников Андрей Игоревич, *ФГУП «НПП «ГАММА»*
В рамках доклада будет рассказано о возможности и целесообразности создания стенда на базе ПЛИС для функциональных испытаний различный аппаратных высокоскоростных СКЗИ. Также будет рассказано об опыте оптимизации алгоритма шифрования ГОСТ Р 34.12–2015 на ПЛИС.

Исследование применимости метода связанных ключей к 4-раундовой версии шифра «Кузнечик»
Гончаренко Кирилл Сергеевич*, факультет Вычислительной Математики и Кибернетики, МГУ им. Ломоносова*
Приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст был утвержден и введен в действие новый блочный шифр ГОСТ Р 34.12-2015, которому было присвоено название «Кузнечик», и который стал с 1 января 2016 г. государственным стандартом РФ для блочного шифрования. Данная работа посвящена криптоанализу модификации этого шифра с использованием метода связанных ключей. Описана атака на версию с 4 раундами шифрования и урезанного ключевого расписания, позволяющая полностью найти мастер-ключ за 2^{12} шифрований при стольких же связанных ключах.

О вычислительной сложности алгоритмов выработки производных ключей
Бородин Михаил Алексеевич, *ИнфоТеКС*
В работе рассмотрена вычислительная сложность ряда алгоритмов выработки производных ключей и преобразования существующих ключей.

10:00–12:00	**Секция «Практика применения средств информационной безопасности»** *Конференц-зал «Еловый», 1 этаж*

Ведущий: **Горелов Дмитрий Львович,** Ассоциация «РусКрипто», коммерческий директор, Актив

Организация защищенных каналов передачи данных в зарубежные представительства
Комаров Валерий Валерьевич, *эксперт*
Опыт прохождения процедур по временному вывозу сертифицированных СКЗИ, для организации защищенных каналов связи с зарубежными филиалами.

Практическая безопасность инфраструктуры PKI
Петров Сергей Владимирович, *руководитель экспертной группы, Positive Technologies*

В докладе рассматривается подход пассивного анализа PKI трафика, с целью предотвращения атак на сеть предприятия с внедренной PKI, фактически построение и применение узкоспециализированной IDS для PKI.

Облачная подпись, неизвлекаемые ключи или криптопровайдер – что лучше?
Смирнов Павел Владимирович, *к.т.н., КриптоПро*
Технологии применения электронной подписи эволюционируют. От криптопровайдера к самодостаточным токенам с неизвлекаемыми ключами и к облачной подписи. Однако, у каждой технологии есть свои достоинства и недостатки. В докладе проводится их сравнение и дается окончательный ответ на вопрос, что же лучше.

Практический подход к управлению рисками уязвимостей
Смирнов Алексей Анатольевич, *ассоциация «Открытая Сеть»*
В докладе приводится анализ текущей ситуации управления рисками: почему стоимость программных продуктов высока, а эффективность недостаточна, и предлагаются подходы к решению проблемы: как перестать воспринимать управление рисками как атрибут «бумажной» безопасности и сделать его практическим доступным инструментом, не требующим существенных финансовых и организационных затрат.

Intel DPDK в решениях для противодействия DDoS-атакам от 40 Гбит/с
Козлюк Дмитрий Александрович, *ведущий разработчик сетевых решений, «БИФИТ»*
Постоянно появляются новые киберугрозы, старые усиливаются. Спец. оборудование не поспевает за изменениями, а сервера и ОС общего назначения - за ростом объемов атак. Intel DPDK — открытый, полностью программный набор инструментов и библиотек для x86/x64, позволяющий достичь скорости аппаратных решений при гибкости программных. Доклад о нюансах и производительности DPDK в прикладных задачах: генерации, анализе, фильтрации сетевого трафика, криптографии, виртуализации.

Комплекс тестов, рекомендованных NIST, для подтверждения корректности функционирования PKI-решений
Камозин Алексей Васильевич*, инженер проектировщик, Газинформсервис*
PKI-функциональность может быть протестирована комплексом тестов, рекомендованных National Institute of Standards and Technology. Эти тесты позволяют подтвердить корректность функционирования средств электронной подписи при выполнении ими валидации сертификатов ключей проверки ЭП и цепочки сертификатов. В докладе содержится описание практического опыта проведения тестирования.

12:30–14:00	**Секция «Информационная безопасность и криптография в средствах мгновенной передачи сообщений (мессенджерах)»** *Конференц-зал «Шишка», 2 этаж*

Ведущие:

- **Качалин Алексей Игоревич,** Positive Technologies
- **Смышляев Станислав Витальевич,** КриптоПро
- **Василенков Александр Сергеевич,** ИнфоТеКС

Мессенджеры давно стали одним из основных каналов электронного взаимодействия. Они широко применяются в крупных корпорациях и государственных органах, во многих сферах вытесняя электронную почту. Изначально мессенджеры не проектировались как инструмент корпоративной коммуникации и о безопасности и криптографической защите информации разработчики думали по остаточному принципу. Насколько безопасны современные, массовые мессенджеры? Как, и на базе каких криптографических протоколов они защищают сообщения пользователей?

На волне импортозамещения появилось много проектов отечественных, доверенных, защищенных мессенджеров. Какие криптографические механизмы и стандарты рекомендуют специалисты для этих проектов? Открытый разговор и дискуссия специалистов в области реальной безопасности, криптографов и разработчиков отечественных мессенджеров. Международный опыт и российская специфика.

Что должно делать до, во время и после безопасного обмена сообщениями
Качалин Алексей Игоревич, *руководитель Expert Security Center, Positive Technologies*
Как в целом должна строиться практическая безопасность в средствах мгновенной передачи информации. О чем должны знать разработчики и пользователи мессенджеров.

О криптографических механизмах и протоколах существующих защищенных мессенджеров
Ахметзянова Лилия Руслановна, *МГУ имени М.В. Ломоносова*
Николаев Василий Дмитриевич, *МГУ имени М.В. Ломоносова*

В данном докладе рассматриваются различные аспекты защиты пользовательской информации в популярных мессенджерах и используемые в них криптографические механизмы. Также приводится обзор известных результатов по анализу безопасности применяемых в них криптографических протоколов.

Разработка защищенного мессенджера. Не так просто, как кажется. Опыт ИнфоТеКС

Василенков Александр Сергеевич, *менеджер продуктов, ИнфоТеКС*

Представитель компании-разработчика криптографических средств поделится с аудиторией опытом по разработке защищенного мессенджера и расскажет о потребностях клиентов при использовании продуктов этого класса.

Технологии безопасности мессенджеров для облачных сервисов и внутрикорпоративного развертывания

Сидоров Евгений Александрович, *технический директор, ООО «Киберника»*

В ходе доклада будет рассказано о механизмах безопасности, актуальных для любых типов мессенджеров.

12:30–14:00	**Круглый стол «Безопасная дорога в облака»** *Конференц-зал «Еловый», 1 этаж*

Ведущие:

- **Баранов Александр Павлович**, д.ф.-м.н., заместитель генерального директора ГНИВЦ ФНС России
- **Бражников Юрий Николаевич**, эксперт RCCPA, генеральный директор 5nine Software

Безопасная дорога в облака. Защищенные каналы доступа и инфраструктура ЦОД хостинг-провайдера. Практика адаптации к новой гибридной ИТ-инфраструктуре. Большинство предприятий и организаций рассматривают или планируют перенос ИС в облака хостинг провайдеров. Но для этого необходимо выполнение требований регулятора как по защите информации в облаке, так и организации безопасного доступа к ЦОД. Предлагается обсудить общую концепцию на конкретных примерах:

- Безопасность облака: СЗИ инфраструктуры и защищенный скоростной доступ
- Безопасность как сервис (SECaaS)
- Практическая реализация требований концепции на разных платформах виртуализации от конкретных хостинг провайдеров
- Скоростной шифрованный доступ к облаку – необходимость для выполнения требований регулятора, бизнес-запросов крупных корпоративных пользователей и государственных организаций.

Участники дискуссии:

- **Николаев Александр Викторович**, главный инженер компания «Тионикс»
- **Бялькин Руслан Николаевич**, директор департамента компания «РТК – ЦОД»

15:00–16:30	**Круглый стол «Электронный документооборот»** *Конференц-зал «Шишка», 2 этаж*

Ведущие:
Миклашевич Анатолий Вадимович, РОСЭУ
Соловяненко Нина Ивановна, ИГП РАН, эксперт АИС
Соловьев Николай Николаевич, компания Гроссмейстер
Курило Андрей Петрович, Финансовый университет
Казаков Сергей Сергеевич, СКБ Контур

15:00–16:30	**Секция «Технологии анализа, моделирования и трансформации программ для создания безопасного программного обеспечения»** *Конференц-зал «Еловый», 1 этаж*

Ведущие:

- **Девянин Петр Николаевич,** д.т.н., доцент, председатель учебно-методического совета (УМС) ФУМО ВО ИБ
- **Аветисян Арутюн Ишханович,** директор ИСП РАН, д.ф.м.н, член-корреспондент РАН

О проблеме представления формальной модели политики безопасности операционных систем

Девянин Петр Николаевич. *д.т.н., доцент, председатель учебно-методического совета (УМС) ФУМО ВО ИБ*

В связи с начавшимся процессом внедрения ФСТЭК России «Требований безопасности информации к операционным системам» в докладе анализируются пути выполнения требований функциональной компоненты ADV_SPM.1 «Формальная модель политики безопасности», в том числе по определению языка, глубины и детализации представления модели политики безопасности управления доступом и информационными потоками. При этом приводятся предложения по составу основных элементов модели, использованию для ее верификации инструментальных средств. Практическая возможность применения предлагаемых подходов рассматривается на примере представления описания и верификации МРОСЛ ДП-модели, как основы механизма управления доступом в ОССН Astra Linux Special Edition.

Система безопасного исполнения программного кода

Козачок Александр Васильевич, *к.т.н., Академия Федеральной службы охраны России (г. Орел).*

В настоящее время вопросу защиты информации при проектировании и эксплуатации объектов критической информационной инфраструктуры уделяется особое внимание. Одним из распространенных подходов к обеспечению безопасности информации, обрабатываемой на объектах, является создание изолированной программной среды. Безопасность среды обуславливается ее

неизменностью. Однако эволюционное развитие систем обработки информации порождает необходимость запуска в данной среде новых компонентов и программного обеспечения при условии выполнения требований по безопасности. Наиболее важным при этом является вопрос доверия к новому программному коду. Доклад посвящен разработке формального логического языка описания функциональных требований к программному коду, который позволит в дальнейшем предъявлять требования на этапе статического анализа и контролировать их выполнение в динамике.

Легковесный метод интроспекции виртуальных машин

Фурсова Наталья Игоревна, Довгалюк Павел Михайлович, Макаров Владимир Алексеевич, Васильев Иван Александрович*, кафедра информационных технологий и систем, Новгородский государственный университет имени Ярослава Мудрого*

Предлагается метод интроспекции виртуальных машин, ориентированный на использовании ABI. Главная отличительная особенность метода состоит в том, что он позволяет получать информацию о работе системе, опираясь на минимальные знания о ее внутреннем устройстве. Основное назначение метода — перехватывать системные функции, считывать параметры и возвращаемые значения. Предлагаемый подход затрагивает редко изменяющиеся части двоичного интерфейса приложений, такие как номера и параметры системных вызовов, соглашения о вызовах. Легковесность метода интроспекции обусловлена минимизацией знаний о системе и его высокой производительностью. Инфраструктура интроспекции базируется на симуляторе QEMU версии 2.8. На текущий момент в программном коде реализованы функции мониторинга файловых операций, процессов и вызовов API.

Проблемы и пути решения практических задач анализа зависимостей между инструкциями при автоматизации динамического анализа программного кода

Тихонов Андрей Юрьевич, *МГТУ им. Н. Э. Баумана*

Доклад посвящен проблемам анализа зависимостей между процессорными инструкциями и путям их решения. Рассмотрены разные виды зависимостей и проблемы, возникающие при попытке их учета в практических случаях анализа. Рассмотрены различные подходы к решению указанных проблем. В частности, на конкретном примере показано, что формальное применение обратного слайсинга приводит к разочаровывающим результатам в связи с подавляющим числом «лишних» инструкций и разобраны причины этого. Показано, что комбинация обратного и прямого слайсинга позволяет получить ожидаемые аналитиком корректные результаты без «лишних» инструкций.

ADV_SPM- Формальные модели политики безопасности на практике
Хорошилов Алексей Владимирович, *к.ф.-м.н., ВМК МГУ*
В докладе рассматривается семейство требований доверия к безопасности ADV_SPM «Моделирование политики безопасности», которое определяется стандартом ГОСТ Р 15408-3-2013 «Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности». Обсуждаются задачи, решаемые этим семейством, и вопросы, которые возникают при попытке интерпретировать его требования. Представляется практический опыт формализации политик безопасности при помощи языка формальных спецификаций Event-B и инструментов платформы Rodin.

О представлении результатов обратной инженерии бинарного кода
Падарян Вартан Андроникович, *к.ф.-м.н., ИСП РАН*
Доклад посвящен вопросу выбора удобного внутреннего представления, используемого при решении задач поиска дефектов и НДВ в бинарном коде программ. Рассматриваются ключевые свойства представлений, влияющие на возможности и ограничения дальнейшего анализа. В задаче поиска дефектов промежуточное представление связывает бинарную трансляцию с построением системы ограничений для SMT-решателя. В задаче поиска НДВ — представление на основе восставленных зависимостей по данным и управлению между машинными инструкциями, используется при построении аннотированной блок-схемы.

15:00–16:30	**Секция «Информационная безопасность киберфизических систем и динамических сетей»** *Конференц-зал «Сосновый», 1 этаж*

Ведущий: **Зегжда Петр Дмитриевич,** профессор, д.т.н., Заслуженный деятель науки РФ, СПбПУ ИБКС

Подходы к оценке безопасности киберфизических систем
Зегжда Петр Дмитриевич*, профессор, д.т.н., заслуженный деятель науки РФ, руководитель отделения «Кибербезопасность» Санкт-Петербургского политехнического университета Петра Великого*
Идеология 4-й промышленной революции привела к появлению нового класса объектов – киберфизические системы (КФС) для обозначения интегрированных комплексов, включающих информационные и исполнительные системы, системы управления и встроенные контролеры с обеспечением межмашинного взаимодействия. В докладе рассматриваются проблемы информационной безопасности киберфизических систем с учетом их архитектуры и комплексного характера последствий атак на информационный уровень и блок контроллеров.

Предлагается подход к моделированию киберфизических систем как многоагентных систем с использованием иерархических семантических графов. Предложен ряд показателей устойчивости КФС и их способности к саморегулированию (гомеостазу). Приведены примеры оценки показателей, определяющих безопасность КФС для Интернета вещей (IoT).

Безопасность протоколов мониторинга индустриальных объектов в концепции Интернета вещей

Беззатеев Сергей Валентинович*, НИУ Информационных технологий, механики и оптики, Санкт-Петербургский государственный университет аэрокосмического приборостроения*

Мониторинг состояния индустриальных объектов, использующий концепцию Интернета вещей, то есть совокупность киберфизических объектов, взаимосвязанных по различным каналам связи, требует решения задачи обеспечения безопасности такой системы. В данном случае под безопасностью понимается эффективное решение всей триады задач информационной безопасности. Анализ существующих протоколов обработки, хранения и передачи данных в совокупности с анализом надежности компонентов системы мониторинга, использующих эти протоколы, позволяет выбрать наиболее оптимальный вариант реализации таких систем с учетом повышенных требований к безопасности. В данной работе рассматривается вариант построения системы мониторинга индустриальных объектов, использующих для управления процессами подсистемы на базе концепции Интернета вещей, для решения задач безопасности в которой применяются специальные протоколы начальной инициализации и взаимной аутентификации ее элементов.

Адаптивное управление безопасностью информационных систем, построенных на базе программно-конфигурируемых сетей

Павленко Евгений Юрьевич, *аспирант, Санкт-Петербургский политехнический университет Петра Великого*

В докладе рассматривается возможность адаптивного управления безопасностью информационных систем на базе программно-конфигурируемых сетей для защиты от таргетированных атак. Проанализированы методы работы современного ВПО и по результатам анализа определены уровни обеспечения безопасности информационных систем. Разработана обобщенная многоуровневая модель взаимодействия компонентов информационных систем, связывающая события безопасности на различных уровнях обеспечения безопасности информационной системы. Разработан подход к управлению безопасностью, основанный на прогнозировании событий безопасности на различных уровнях безопасности и контроля их состояний.

Поиск уязвимостей в программных компонентах киберфизических систем с помощью методов глубокого обучения

Демидов Роман Алексеевич, *аналитик, НеоБИТ*

Автором предлагается алгоритмический подход к поиску уязвимостей в программных компонентах киберфизических систем на основе методов глубокого обучения. В рамках подхода осуществляется двухступенчатый процесс обучения многослойной нейронной сети на помеченных и непомеченных данных о структуре исполняемых файлов. Путем построения иерархии высокоуровневых абстракций из низкоуровневого кода в процессе обучения, в новых образцах кода возможно распознавание различных классов уязвимостей.

Анализ безопасности технологии NFC при решении прикладных задач

Мясников Алексей Владимирович, *аспирант, СПбПУ ИБКС*

Технология NFC позволяет передавать данные на коротком расстоянии посредством радиосигнала. Эта технология используется во множестве решений в различных сферах жизнедеятельности, в том числе в системах контроля доступа, системах бесконтактной оплаты банковскими картами, применяется для оплаты проезда в общественном транспорте и др. В докладе приведены результаты анализа технологии NFC на предмет защищенности при передаче конфиденциальных данных. Рассмотрены возможные атаки на канал передачи данных, а также предложены способы защиты от них.

Защита беспроводных клиентов от атак, основанных на использовании особенностей построения WiFi-сетей

Дахнович Андрей Дмитриевич, *аналитик, НеоБИТ*

В докладе представлены результаты анализа механизмов защиты WiFi-сетей от атак с использованием поддельных точек доступа. Данная атака является актуальной для большинства некорпоративных WiFi-сетей, т.к. от нее не существует универсальных и надежных механизмов защиты. В результате нарушитель получает возможность перехватывать данные клиента.

Авторами предложен метод защиты от рассмотренного класса атак на WiFi-сети, основанный на аутентификации точек доступа. В докладе приведена оценка применимости данного метода в сетях различного назначения. Проведены экспериментальные исследования, подтвердившие применимость и эффективность разработанного метода защиты.

17:00–19:00	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал «Шишка», 2 этаж*

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

Технологии больших данных для мониторинга компьютерной безопасности
Котенко Игорь Витальевич, *д.т.н., профессор, заведующий лабораторией проблем компьютерной безопасности, СПИИРАН*
Проводится анализ существующих подходов к использованию технологий больших данных для мониторинга компьютерной безопасности и управления инцидентами. Особенностью рассматриваемых решений является акцент на интеграции технологий больших данных и традиционных технологий управления информацией и событиями безопасности. Приводятся примеры разработанных систем мониторинга, основанных на технологиях больших данных, делаются сравнительные выводы об известных подходах в этой области.

Анализ атакующих воздействий по истощению энергоресурсов в системах Интернета вещей
Десницкий Василий Алексеевич*, к.т.н., доцент кафедры защищенных систем связи, СПбГУТ*
Предлагается модель нарушителя систем Интернета вещей, имеющего целью скомпрометировать устройства системы путем истощения их энергоресурсов. К основным путям таких атак относятся: принудительный вывод устройств из режима работы с низким энергопотреблением, увеличение трафика, создание помех, нештатное использование ПО. Анализируются количественные и качественные показатели данного вида атак.

Разработка и оценка программной платформы для параллельной распределенной обработки данных о событиях безопасности
Кушнеревич Алексей Геннадьевич*, ЛЭТИ*
Рассматривается архитектура и вопросы построения на платформе Hadoop компонентов разработанной программной системы, предназначенной для выполнения распределенной параллельной обработки больших массивов данных в интересах мониторинга и управления безопасностью компьютерной сети. В основу функционирования такой системы положена технология потоковой обработки данных Complex Event Processing. Собираемые данные о событиях безопасности, в разработанной программной платформе, подвергаются процедурам агрегации, нормализации, корреляции, визуализации и хранению с использованием распределенной файловой системы. Раскрываются основные вопросы реализации программной платформы. Обсуждаются результаты оценки ее функциональных показателей.

Графические модели для визуализации метрик безопасности компьютерной сети
Чечулин Андрей Алексеевич, *СПИИРАН*
Представляется подход к выбору наиболее эффективных по соотношению «информативность — понятность» графических моделей для визуализации различных метрик защищенности компьютерной сети. Для этого был проанализирован ряд графических моделей и определены их основные достоинства и недостатки. Кроме того, были рассмотрены основные метрики защищенности компьютерных сетей и были выбраны графические модели, позволяющие наиболее эффективно визуализировать эти метрики. Предполагается, что разработанный подход позволит повысить защищенность компьютерных сетей за счет повышения качества решений, принимаемых оператором системы безопасности.

Оценка киберустойчивости на основе метода топологического преобразования стохастических сетей
Лаута Олег Сергеевич, *Военная академия связи*
Предлагается метод оценки киберустойчивости компьютерных сетей, основанный на аналитическом моделировании компьютерных атак с помощью стохастических сетей и их последующем топологическом преобразовании. Приводятся примеры формирования стохастических сетей для типовых компьютерных атак. Рассматривается сущность метода топологического преобразования стохастических сетей, позволяющего получить первые моменты функций распределения времен реализации атак. Предлагаются показатели и аналитические выражения для оценки киберустойчивости. Обсуждаются результаты экспериментальной оценки предложенных моделей и метода. Формулируются предложения по поиску мер противодействия компьютерным атакам, приводящие к повышению киберустойчивости компьютерных сетей.

Армия умных ботов - инструмент достижения превосходства в киберпространстве
Масалович Андрей Игоревич*, руководитель направления конкурентной разведки, Академия Информационных Систем, президент консорциума «ИНФОРУС»*
В докладе рассматривается обширный набор реальных примеров: согласованное использование ботов позволяет за час подобрать пароли от миллиона почтовых ящиков, за полчаса взломать код верификации (cvv) кредитки, перехватить управление десятками аккаунтов в Facebook и т.д. Высокоорганизованные боты «информационного спецназа» обеспечивают практически мгновенную доставку ударного контента в места обитания целевой аудитории. Также будут приведены примеры использования армий умных ботов на «светлой стороне» — для борьбы с пиратами, мошенниками, вымогателями и экстремистами.

17:00–19:00	**Мастер-класс «Электронное правосудие. Практика использования электронного документооборота в арбитражном суде»** *Конференц-зал «Еловый», 1 этаж*

Ведущий: **Соловяненко Нина Ивановна**, Институт государства и права РАН, эксперт Академии Информационных Систем

Что такое электронное правосудие, из каких элементов оно состоит и какими нормативными актами регулируется? Какие информационные системы используется в электронном правосудии и какие задачи решаются с их помощью? Новые положения законодательства и иных нормативных актов о применении электронных документов в деятельности судов (вступили в силу с 1 января 2017г.).

Раскроется тема о подаче в арбитражный суд и регистрации документов в электронном виде, в том числе в форме электронного документа. Система «Мой арбитр». Поговорим о требованиях к электронным документам и электронным подписям, про основания отклонения документов и о вопросах, связанных с использованием документов в электронном виде, требующие особого внимания.

Не останутся без внимания темы об электронных доказательствах в арбитражном процессе и использование программного комплекса «Судебно-арбитражное делопроизводство» подсистема «Судопроизводство» (ПС СП) в целях делопроизводства и документооборота.

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
info@ruscrypto.ru

Академия Информационных Систем (АИС)

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
info@infosystem.ru
+7 (495) 120-04-02

Компания КриптоПро. С момента создания (2000 г.) компания КриптоПро занимает лидирующее положение в области разработки средств криптографической защиты информации и развития Инфраструктуры Открытых Ключей (PKI) на территории РФ. Компания внесла существенный вклад в адаптацию международных рекомендаций применительно к российским криптографическим алгоритмам. Продукты компании КриптоПро широко используются органами власти и коммерческими организациями всех отраслей. Они применяются в системах электронного документооборота, исполнения госзаказа, сдачи всех видов отчетности и т.п. Включают поддержку всех платформ, имеют версии для мобильных устройств, интегрированы с ведущими IT решениями.
www.cryptopro.ru

Компания «Актив» — крупнейший российский производитель аппаратных средств аутентификации и электронной подписи, разработчик и поставщик решений в сфере информационной безопасности. Направления деятельности: Guardant – средства защиты и лицензирования программного обеспечения. Рутокен – продукты и решения в области аутентификации, защиты информации и электронной подписи.
www.aktiv-company.ru; www.rutoken.ru; www.guardant.ru

Группа компаний «ИнфоТеКС» — один из первых разработчиков программных и программно-аппаратных VPN-решений с 1991 года. Основной разработкой компании является технология ViPNet — наиболее гибкое VPN-решение, которое позволяет осуществлять безопасную передачу данных в защищенной сети. Более миллиона пользователей технологии ViPNet уже убедились в качестве и надёжности продуктов «ИнфоТеКС», которые предназначены для решения самых сложных задач в сфере защиты данных. В состав ГК «ИнфоТеКС» также входят три дочерние компании: ОАО «ИнфоТеКС Интернет Траст», ЗАО «Перспективный мониторинг» и НОЧУ ДПО «Учебный центр «ИнфоТеКС».
www.infotecs.ru

Компания «БИФИТ» основана в 1999 году в Москве. Партнерами компании «БИФИТ» являются более 39% банков Российской Федерации. Система электронного банкинга «iBank 2» является одним из наиболее распространенных решений ДБО в России. Системой пользуются около миллиона корпоративных клиентов и более 1 200 тысяч частных клиентов. Компания «БИФИТ» имеет Лицензию ФСБ РФ на осуществление разработки, производства, распространения шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств. Компания «БИФИТ» активно ведет работы по созданию программных и аппаратных СКЗИ собственной разработки.
www.bifit.com/ru

Компания «Фактор-ТС», создана 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 сетей передачи данных, телекоммуникационных узлов и других информационных систем в защищенном исполнении.Технические решения компании позволяют замещать импортные аналоги в критически важных для безопасности страны сегментах национальной информационной структуры.
www.factor-ts.ru

Компания ООО «НеоБИТ» создана командой ведущих ученых и специалистов в области безопасности компьютерных систем и сети Интернет для продвижения на российский и мировой рынок собственных решений и передовых технологий защиты информационных систем от киберугроз.
Профиль компании – проектирование и разработка продуктов и решений, обеспечивающих безопасность информации, создание защищенных информационных систем, анализ защищенности ресурсов, доступных в сети Интернет.
www.neo-bit.ru ; www.необит.рф

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

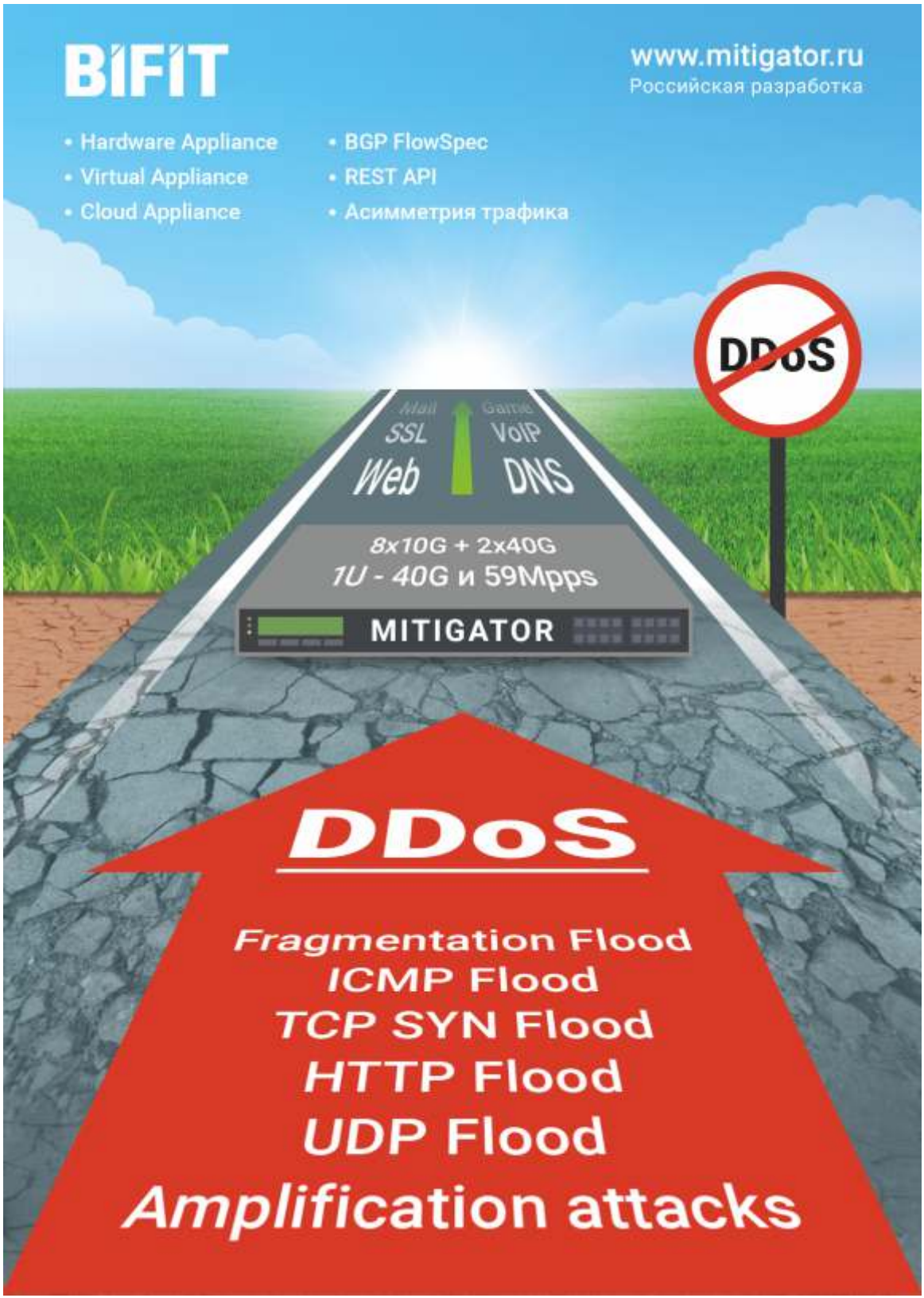
Компания ИнфоТеКС – одна из ведущих ИТ-компаний отечественного рынка программных и программно-аппаратных VPN-решений и средств криптографической защиты информации.

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


BIFIT
www.mitigator.ru
Российская разработка
• Hardware Appliance
• Virtual Appliance
• Cloud Appliance
• BGP FlowSpec
• REST API
• Асимметрия трафика
DDoS
Mail
SSL
Web
Game
VoIP
DNS
8x10G + 2x40G
1U - 40G и 59Mpps
MITIGATOR
DDoS
Fragmentation Flood
ICMP Flood
TCP SYN Flood
HTTP Flood
UDP Flood
Amplification attacks

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

- проектирование и создание защищенных информационных систем специального назначения
- разработка технологий контроля и управления доступом к информационным ресурсам на базе защищенных операционных систем
- аудит состояния информационных систем и анализ безопасности распределенных систем обработки информации
- разработка телекоммуникационных систем для передачи конфиденциальной и закрытой информации
- анализ эффективности антивирусных средств и разработка систем антивирусной защиты
- выполнение научно-исследовательских и опытно-конструкторских работ
- разработка аппаратных средств защиты данных
- анализ уязвимостей программного обеспечения, в том числе операционных систем, сетевых сервисов, баз данных и средств управления телекоммуникациями

195220 РОССИЯ, САНКТ-ПЕТЕРБУРГ,
УЛ. ГЖАТСКАЯ Д.21 ЛИТЕРА «Г»
ТЕЛ./ФАКС: 535-28-06, 535-88-67
NEOBIT.RU / НЕОБИТ.РФ
INFO@NEOBIT.RU

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

ОБ АКАДЕМИИ

В течение 20 лет Академия Информационных Систем (АИС) предоставляет образовательные услуги по информационной и экономической безопасности, информационным технологиям и конкурентной разведке. Обучение своих сотрудников нам доверяют Пенсионный Фонд РФ, ФСС РФ, ФСКН России, ФСО России, ФССП России, ФСБ России, МВД России, Сбербанк, Газпромбанк, Альфа-банк, Северсталь, Лукойл, Роснефть, Ростех, МТС, МГТС, Мегафон, Ростелеком, и другие.

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

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.

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

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

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

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

V Международная научно-практическая конференция

«Управление информационной безопасностью в современном обществе»

30 мая - 1 июня 2017 г.

Москва, Кирпичная, 33

НИУ ВШЭ

ОСНОВНЫЕ ТЕМЫ

- Теория и методология информационной безопасности;
- Проблемы управления отраслью информационной безопасности в государственном и частном секторах;
- Состояние и решение основных научно-технических задач обеспечения информационной безопасности;
- Проблемы развития и обеспечения информационной безопасности при массовом применении IT –технологий при разработке и реализации функциональных систем.

ДЛЯ КОГО

- Руководителей и специалистов:
- Федеральных органов исполнительной власти РФ;
- Администрации субъектов РФ, в том числе краев и областей;
- Ученые, аспиранты, преподаватели, студенты;
- Компаний-разработчиков средств информационной безопасности,
- а также организаций, осуществляющих свою деятельность в области защиты информации.

В ПРОШЛОМ ГОДУ

<50 докладов
<100 участников
2 дня общения с лучшими экспертами России, Европы, Северной и Южной Америки

Контакты: Елин Владимир Михайлович
velin@hse.ru
+7(926) 774-41-46,
confinfo@hse.ru
+7(495) 772-95-90, доб. 55134

КАЛЕНДАРЬ МЕРОПРИЯТИЙ

5 АПРЕЛЯ 2017

ИТ-ФЕСТИВАЛЬ
ИМПОРТОЗАМЕЩЕНИЕ - 2017
www.infosystems.ru

Главная тема: Поддержка заказчиков из государственного и промышленного секторов в контексте реализации или программ по импортозамещению в ИКТ, обсуждение практических вопросов, обмен опытом выполненных проектов.

30 МАЯ 1 ИЮНЯ 2017

V МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СОВРЕМЕННОМ ОБЩЕСТВЕ
www.vipforum.ru

Главная тема: Проблема обеспечения информационно й безопасности систем со значительным количеством пользователей, включая информационную безопасность самих пользователей.

22 ИЮНЯ 2017

V ВСЕРОССИЙСКАЯ ОТРАСЛЕВАЯ КОНФЕРЕНЦИЯ
БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ТЭК
www.vipforum.ru

Главная тема: Правовые аспекты обеспечения безопасности АСУ ТП критически важных объектов ТЭК, защита АСУ ТП от деструктивного воздействия и вопросы реализации требований №256 - ФЗ и его подзаконных актов.

5-9 СЕНТЯБРЯ 2017

XVI ВСЕРОССИЙСКИЙ ФОРУМ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. РЕГУЛИРОВАНИЕ. ТЕХНОЛОГИИ. ПРАКТИКА»
ИНФОБЕРЕГ - 2017
www.vipforum.ru

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

18-20 ОКТЯБРЯ 2017

IX 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 2017

V НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ И КОНКУРЕНТНАЯ РАЗВЕДКА
www.vipforum.ru

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

1 ДЕКАБРЯ 2017

VII МЕЖДУНАРОДНЫЙ ФОРУМ «БОРЬБА С МОШЕННИЧЕСТВОМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ»
ANTIFRAUD RUSSIA - 2017
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.

Общие правила для участников:

- Пропуск на территорию отеля в период проведения конференции осуществляется строго по спискам зарегистрированных участников.
- Питание на территории отеля организовано по системе «все включено» с 08:00 до 23:00. Время завтраков, обедов и ужинов для участников «РусКрипто'2017» указано в программе.

Трансфер в дни работы конференции (для участников, не проживающих на территории отеля):

- 22 марта в 08:00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 22 марта в 19:50 вечера трансфер отель «Солнечный Park Hotel & SPA» – м. Речной вокзал.
- 23 марта в 08:00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 23 марта в 19:50 вечера трансфер отель «Солнечный Park Hotel & SPA» – м. Речной вокзал.

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

Организованный выезд из отеля «Солнечный Park Hotel & SPA»:

24 марта (пятница) в 12:00 автобусом до станции метро «Речной вокзал». Подача автобусов в 11:45 у ворот отеля.

Внимание! Автобусы с табличкой «РусКрипто'2017» отправятся ровно в 12:00.

Просьба заранее сдать номера и не опаздывать.

Отель «Солнечный Park Hotel & SPA»:

Московская область, Солнечногорский район, Ленинградское шоссе, 74 км

Телефон: +7 (925) 922-42-00

Расчетный час:

Заезд – 21 марта с 16:00

Выезд – 24 марта до 12:00

Контакты организаторов:

Кочукова Виктория – т. 8 (925) 884-44-08
Ульянова Светлана – т. 8 (985) 134-80-40
Пученкина Юлия – т. 8 (926) 257-33-90

www.ruscrypto.ru