ПРОГРАММА КОНФЕРЕНЦИИ

22-25 марта 2016 года

www.ruscrypto.ru

Спонсоры и партнеры конференции

Золотой спонсор

КРИПТО ПРО

Серебряные спонсоры

Компания Актив · BIFIT · Microsoft

Бронзовые спонсоры

GiS ГАЗИНФОРМСЕРВИС · Код безопасности · infotecs Решения по защите информации

Научный партнер

ФАКТОР-ТС

Партнеры конференции

s·terra · инсайд · НЕОБИТ · Ростех Информ · ISBC · Check Point SOFTWARE TECHNOLOGIES LTD. · АБИСС

Информационная поддержка

BANKIR.RU · BIS JOURNAL · Единый портал Электронной подписи · kartoteka.ru · NBJ · BISA · POSITIVE TECHNOLOGIES

Спортивные партнеры

I ♥ RUNNING ШКОЛА ПРАВИЛЬНОГО БЕГА · cep the intelligent sportswear · ZECURION

Таймлайн конференции

22 марта, вторник. День заезда

14:00	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

23 марта, среда. Первый день работы конференции

8:00 – 9:00	Завтрак	
9:00 – 10:00	Регистрация участников конференции	
10:00 – 11:30	Официальное открытие конференции. **Пленарное заседание** *Конференц-зал* *Подробнее на стр. 7*	
11:30 – 12:00	Кофе-брейк	
12:00 – 13:30	**Круглый стол «Электронная подпись: реальная практика применения и законодательное регулирование»** *Конференц-зал* Ведущие: · **Кузнецов А. Ю.,** Минкомсвязь России · **Маслов Ю. Г.**, КРИПТО-ПРО, РОСЭУ · **Баранов Н.В.,** СКБ Контур *Подробнее на стр. 7*	**Секция «Информационная безопасность и криптография в интернете вещей»** *Зал «Марс»* Ведущий: **Лукацкий А. В.**, Cisco *Подробнее на стр. 7*

Таймлайн конференции

13:30 – 14:30	Обед	
14:30 – 16:30	**Круглый стол «Импортозамещение в ИТ на предприятиях оборонно-промышленного комплекса»** *Конференц-зал* Ведущие: · **Литвинов О.А.**, Системы управления · **Губарев А.В.**, РТ-ИНФОРМ *Подробнее на стр. 8*	**Секция «Продукты и решения информационной безопасности для кредитно-финансовых организаций»** *Зал «Марс»* Ведущие: · **Гусев Д. М.,** ИнфоТеКС · **Горелов Д. Л.,** Актив, Ассоциация «РусКрипто» *Подробнее на стр. 8-9*
16:30 – 17:00	Кофе-брейк	
17:00 – 19:00	**Секция «Криптография и криптоанализ», I часть.** *Зал «Марс»* Ведущие: · **Матюхин Д. В.**, ФСБ РФ · **Попов В. О.**, КРИПТО-ПРО, Ассоциация «РусКрипто» · **Жуков А. Е.**, МГТУ им. Баумана, Ассоциация «РусКрипто» *Подробнее на стр. 10*	**Круглый стол «Средства криптографической защиты информации в системах дистанционного банковского обслуживания»** *Конференц-зал* Ведущие: · **Виноградов А. Ю.,** Златкомбанк · **Простов В. М.**, ТК 26 · **Левиев Д. О.,** НП ПСИБ *Подробнее на стр. 11*
19:30 – 20:30	Ужин	
20:30 – 22:00	Вечерняя программа	

24 марта, четверг. Второй день работы конференции

8:00 – 10:00	Завтрак		
10:00 – 12:10	**Секция «Вопросы разработки и применения криптографических требований и стандартов»** *Конференц-зал* Ведущий: **Кузьмин А. С.**, ТК 26 *Подробнее на стр. 12*	**Секция «Цифровая криминалистика и расследование инцидентов»** *Зал «Марс»* Ведущие: · **Чиликов А.А.,** МГТУ им. Н.Э. Баумана · **Яковлев А.Н.,** Следственный комитет РФ *Подробнее на стр. 13*	
12:10 – 12:30	Кофе-брейк		
12:30 – 14:00	**Секция «Электронный документооборот»** *Конференц-зал* Ведущие: · **Кузьмин А. С.**, ТК 26 · **Соловьев Н.Н.,** Гроссмейстер *Подробнее на стр. 14*	**Секция «Облака в безопасности»** *Зал «Марс»* Ведущие: · **Фатеев О. А.,** RCCPA · **Белявский А. К.**, Zecurion *Подробнее на стр. 15*	
14:00 – 15:00	Обед		
15:00 – 17:00	**Секция «Криптография и криптоанализ», II часть.** *Зал «Марс»* Ведущие: · **Кузьмин А. С.**, ТК26 · **Попов В. О.**, КРИПТО-ПРО, Ассоциация «РусКрипто» · **Жуков А. Е.**, МГТУ им. Баумана, Ассоциация «РусКрипто» *Подробнее на стр. 16*	**Секция «Информационная безопасность в России»** *Конференц-зал* Ведущая: **Старостина Е. В.,** Cyber Security, Advisory Services, EY *Подробнее на стр. 17*	**Секция «Интеллектуальные методы анализа нарушений кибербезопасности»** *Зал «Стеклянный»* Ведущий: **Зегжда П.Д.,** СПбПУ *Подробнее на стр. 18*

17:00 – 17:30	Кофе-брейк		
17:30 – 19:30	**Секция «Блокчейн и криптовалюты. Использование «пограничных» технологий в мирных целях»** *Конференц-зал* Ведущие: · **Комисаренко В. В.,** БЕЛТИМ СБ, Ассоциация «РусКрипто» · **Архипов А.С.**, QIWI *Подробнее на стр. 19*	**Секция «Перспективные исследования в области кибер-безопасности»** *Зал «Марс»* Ведущий: **Котенко И. В.,** СПИИРАН *Подробнее на стр. 20*	**Семинар «Защита информационных ресурсов от действий иностранных технических разведок. Конкурентная разведка vs ИТР»** *Зал «Стеклянный»* Ведущий: **Масалович А. И.,** АИС *Подробнее на стр. 21*
19:30 – 20:30	Ужин		
21:00 – 23:00	Вечерняя программа		

Первый день работы конференции

10:00 – 11:30	**Пленарное заседание** *Конференц-зал*

Официальное открытие конференции
Приветственное слово

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

Актуальные направления исследований в области информационной безопасности
Баранов Александр Павлович*, д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

Обзор поправок в закон N 63-ФЗ «Об электронной подписи», внесенных федеральным законом N 445-ФЗ от 30 декабря 2015 года
Кузнецов Александр Юрьевич, *заместитель директора правого департамента, Минкомсвязь России*

12:00 – 13:30	**Круглый стол «Электронная подпись: реальная практика применения и законодательное регулирование»** *Конференц-зал*

Ведущие:

- ***Кузнецов Александр Юрьевич,*** *заместитель директора правого департамента, Минкомсвязь России*
- ***Маслов Юрий Геннадьевич****, коммерческий директор, КРИПТО-ПРО, эксперт НП «РОСЭУ»*
- ***Баранов Никита Валерьевич,*** *руководитель группы проектов «Услуги Удостоверяющего центра», СКБ Контур*

12:00 – 13:30	**Секция «Информационная безопасность и криптография в интернете вещей»** *Зал «Марс»*

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

Эксперты открытой дискуссии:

- ***Бешков Андрей Юрьевич***, Microsoft
- ***Горелов Дмитрий Львович***, Ассоциация «РусКрипто», Актив
- ***Смирнов Николай Валерьевич****, ИнфоТеКС*
- ***Качалин Алексей Игоревич***, Positive Technologies

Криптография в IoT: обзор состояния в контексте противостояния
Лукацкий Алексей Викторович, *бизнес-консультант по безопасности, Cisco*
В докладе рассматривается текущее состояние применения различных криптографических стандартов и протоколов в консьюмерском и промышленном IoT, а также делается обзор сложностей применения традиционных криптографических подходов к IoT.

IoT в России – возможность или RuIoT, бессмысленный и беспощадный?
Смирнов Николай Валерьевич, *руководитель отдела, ИнфоТеКС*

В докладе рассматривается текущее состояние развития сегментов IoT в мире и в России, демонстрируется различие подходов к реализации сценариев IoT, включая особенности эксплуатации российской криптографии, поднимается проблематика существующих барьеров внедрения направления.

Безопасность IoT: чем выше ожидания - тем больше вопросов
Качалин Алексей Игоревич, *Руководитель Expert Security Center, Positive Technologies*

Информационная безопасность IoT очень давно. Сейчас одновременно происходит два процесса: увеличение многообразия устройств (и их совместное использование) и свойственное сегменту потребительской электроники ускорение разработки и повторное использование компонентов. Сложившаяся ситуация порождает широкие возможности для атакующего по целям и возможностям осуществления атак. В докладе будет представлен обзор трендов развития IoT в части разработки и использования и, как следствие – дополнительные проблемы информационной безопасности, о которых скоро предстоит беспокоиться в рабочей и личной жизни.

Обсуждение. Открытая дискуссия

14:30 – 16:30	**Круглый стол «Импортозамещение в ИТ на предприятиях оборонно-промышленного комплекса»** *Конференц-зал*

Ведущие:

- ***Литвинов Олег Анатольевич,*** *заместитель генерального директора по разработке и развитию информационных технологий, АО «Системы управления»*
- ***Губарев Андрей Васильевич,*** *директор по информационной безопасности, РТ-ИНФОРМ*

Эксперты круглого стола:

- ***Панченко Иван Евгеньевич****, Postgres Professional*
- ***Комиссаров Дмитрий Владимирович****, Новые облачные технологии*
- ***Тихонов Андрей Иванович****, Ассоциация Тайзен.ру*
- ***Рассомагин Александр Сергеевич,*** *РТ-ИНФОРМ*

Предложения по подходу и реализации стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации
Добродеев Александр Юрьевич, *советник генерального директора, Концерн Системпром*

Три грани санкционно-устойчивого программного обеспечения
Рубанов Владимир Васильевич, *управляющий директор, Росплатформа, вице-президент по технологиям, Virtuozzo*

14:30 – 16:30	**Секция «Продукты и решения информационной безопасности для кредитно-финансовых организаций»** *Зал «Марс»*

Ведущие:

- ***Гусев Дмитрий Михайлович,*** *заместитель генерального директора, ИнфоТеКС*
- ***Горелов Дмитрий Львович,*** *Ассоциация «РусКрипто», коммерческий директор, Актив*

Актуальные проблемы и методы решения двухфакторной аутентификации в финансовых сервисах для физических лиц

Юнусов Тимур Исламитдинович, *старший эксперт, руководитель отдела безопасности банковских систем, Positive Technologies*

В докладе будут описаны текущие проблемы основного механизма двухфакторной аутентификации в банковских продуктах для физлиц: одноразовых паролей через смс. Существует много способов реализовать этот механизм неправильно. И в большинстве проектов по аудиту безопасности банковских продуктов были выявлены те или иные недостатки, сводящие на нет все используемые механизмы двухфакторной аутентификации, начиная от атак на логику приложения и недостатки авторизации, заканчивая фишингом и атаками на клиентские устройства. Но даже если на стороне банка все условия выполнены, это не означает, что у клиента невозможно похитить деньги. Как не быть самым слабым в ряду? Какие уязвимости можно устранить с минимальными затратами? Существуют ли более эффективные методы двухфакторной аутентификации, при этом настолько же удобные?

Криптографическая платформа ViPNet HSM как основа для построения банковских PKI сервисов

Поташников Александр Викторович, *заместитель директора центра разработок по криптографии, ИнфоТеКС*

В докладе рассказывается про опыт ИнфоТеКС по разработке криптографического аппаратного модуля с реализацией электронных сервисов платежных карт, поддерживающего как зарубежные платежные системы Visa и MasterCard, так и отечественную карту МИР. Также в докладе рассматриваются открытые вопросы сертификации и стандартизации подобных продуктов с учетом российских требований к СКЗИ и зарубежных требований к HSM.

Обзор технологической платформы Рутокен для разработчиков систем информационной безопасности

Мещеряков Кирилл Олегович, *руководитель отдела по работе с технологическими партнерами, Актив*

Рассказ о продуктах и технологиях, ориентированных банковский сегмент. Архитектура, взаимосвязь и иерархия компонентов, возможности адаптации и ключевые особенности элементов платформы. Применимость при различных сценариях использования.

Практика внедрения и использования Трастскринов для радикального снижения рисков в ДБО

Шилов Станислав Олегович*, директор по продажам, БИФИТ*

Опыт эксплуатации в ДБО Трастскринов – аппаратных устройств, обеспечивающих неизвлекаемое хранение ключей ЭП и подпись с визуализацией. Рассмотрены вопросы противостояния актуальным угрозам хищения средств в ДБО и эффективности различных механизмов защиты. С учетом опыта практической эксплуатации предложены направления развития решений аналогичного класса.

Применение защищенной архитектуры «тонкого клиента» в банковских системах с высокими требованиями к уровню информационной безопасности

Любушкина Ирина Евгеньевна*, к. т. н., главный специалист, Фирма «АНКАД»*

Панасенко Сергей Петрович*, к. т. н., заместитель генерального директора по науке и системной интеграции, Фирма «АНКАД»*

17:00 – 19:00	**Секция «Криптография и криптоанализ» I часть.** *Зал «Марс»*

Ведущие:

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

О марковских алгоритмах блочного шифрования

Пудовкина Марина Александровна, *НИЯУ МИФИ*

Дана интерпретация широко известных результатов, посвященных марковским алгоритмам блочного шифрования, на языке укрупнений состояний цепи Маркова. Предложено обобщение марковского алгоритма блочного шифрования и описаны его свойства.

Совершенные шифры

Бабаш Александр Владимирович, *д.ф.-м.н., профессор кафедры «Информационная безопасность», НИУ ВШЭ*

Результаты задач: 1) по обобщению понятия совершенного шифра как функции от двух переменных f(i,k) на автоматную функцию A(i,k)=z, где I будет множеством водных слов длины n автомата, а K – множеством состояний автомата; 2) по поиску n и не константных функций Ф1 и Ф2, для которых выполняется условие Ф1(i)= Ф2(A(i,k)) при любых i∈I, k∈K.

Метод защиты неподвижных изображений с помощью обратимых геометрических преобразований

Мельников Дмитрий Анатольевич*, к.т.н., НИЯУ МИФИ*

Абрамов Антон Анатольевич*, аспирант, НИЯУ МИФИ*

В докладе рассматривается подход к защите изображений с использованием геометрического преобразования. Объясняются принципы на которых основывается подход. Исследуются свойства такого способа защиты и пути его реализации, оцениваются преимущества и недостатки каждого из путей. Показаны способы дальнейшего улучшения данного подхода.

Построение биодатчика случайных чисел и оптимизация его характеристик с помощью вычислительных экспериментов

Задорожный Дмитрий Игоревич, *руководитель службы, Код Безопасности*

В рамках доклада будут представлены макет и математическое описание биологического датчика случайных чисел (БиоДСЧ), основанного на скорости и точности реагирования руки пользователя на изменение изображения на экране персонального или планшетного компьютера.

Неразличимая обфускация

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

Предлагается метод защиты программного кода от несанкционированного доступа, основанный на применении процедуры неразличимой обфускации. Доказана его стойкость в модели со случайным оракулом. Работа посвящена модификации существующих подходов к осуществлению неразличимой обфускации с целью устранения ряда ограничений, обусловленных применяемыми механизмами, моделями и алгоритмами.

О способе сокращения перебора в атаке Дюжелла на шифрсистему RSA

Гинятуллин Роман Дамирович, *студент, НИЯУ МИФИ*

В работе рассматривается атака на шифрсистему RSA, предложенная Верхулом и ван Тилборгом и улучшенная Дюжелла. Экспериментально получены зависимости используемых коэффициентов от длины ключа. Предложены способы существенного сокращения перебора величин, влияющих на результат атаки. Например, при длине ключа в 1024 бит удалось сократить перебор ~ в 15 раз, что позволило существенно уменьшить время атаки.

17:00 – 19:00	**Круглый стол «Средства криптографической защиты информации в системах дистанционного банковского обслуживания»** *Конференц-зал*

Ведущие:

- ***Виноградов Александр Юрьевич,*** *начальник управления ИБ, Златкомбанк*
- ***Простов Владимир Михайлович****, ТК 26*
- ***Левиев Дмитрий Олегович,*** *председатель совета, НП ПСИБ*

В рамках секции ведущие обсудят на одной площадке с разработчиками СКЗИ, систем электронного документооборота и дистанционного банковского обслуживания, а также представителей финансовых организаций вопросы жизненного цикла СКЗИ и вопросы корректного использования СКЗИ в системах ДБО/СЭД. В рамках секции пройдет обсуждение ответственности поставщика решения перед банком и клиентами банка за правильность использования СКЗИ, разбора конфликтных ситуаций между разработчиком ДБО/СЭД и клиентом при окончании или продлении сертификата на СКЗИ. Ведущие поднимут тему перехода клиентов из банка в банк со своими СКЗИ и обсудят возможности и угрозы при аренде средств криптографической защиты.

Второй день работы конференции

10:00 –12:10	**Секция «Вопросы разработки и применения криптографических требований и стандартов»** *Конференц-зал*

Ведущий: ***Кузьмин Алексей Сергеевич,*** *д.ф.-м.н., профессор, председатель ТК 26*

Гражданская криптография
Кузьмин Алексей Сергеевич, *д.ф.-м.н., профессор, председатель ТК 26*

Все, что вы хотели знать о ТК 26, но боялись спросить
Сериков Игорь Анатольевич, *ТК 26*
Матюхин Дмитрий Викторович, *ФСБ России*

О проекте открытых требований к шифровальным (криптографическим) средствам защиты информации
Бондаренко Александр Иванович, *ФСБ России*
Нестеренко Алексей Юрьевич, *ФСБ России*

Перевод EMV-стандарта на отечественные криптографические алгоритмы
Простов Владимир Михайлович, *ТК 26*

Адаптация алгоритмов ГОСТ и Ciphersuites с использованием алгоритмов ГОСТ для протокола DTLS
Белявский Дмитрий Михайлович, *Технический центр Интернет*
В докладе описываются проблемы использования российских криптографических алгоритмов в протоколе DTLS (Datagram Transport Layer Security) и пути их решения.

Протоколы согласования ключей с аутентификацией на основе пароля: принципы обеспечения безопасности
Смышляев Станислав Витальевич, *к.ф.-м.н., начальник отдела защиты информации, КРИПТО-ПРО*
Алексеев Евгений Константинович, *к.ф.-м.н., ведущий инженер-аналитик, КРИПТО-ПРО*
В последние годы появилось немало работ, посвященных решению задачи выработки секрета с высокой энтропией (например, ключа ГОСТ 28147-89) под защитой слабого короткого пароля. В докладе рассматриваются подходы к обеспечению безопасности таких протоколов и ряд необходимых условий, нарушение которых влечет возможность восстановления высокоэнтропийного секрета путем перебора короткого пароля. Приводятся примеры нестойких протоколов с анализом ошибок синтеза, приводящих к уязвимостям.

Защита персональных данных. Какие СКЗИ выбрать?

Афанасьев Александр Александрович, *начальник отдела, Фактор-ТС*

В докладе сопоставляются требования руководящих документов ФСБ России и ФСТЭК России, регламентирующих защиту персональных данных. Оценивается возможность и корректность выбора оператором средств криптозащиты для ИСПДн. Сформулированы предложения по корректировке требований к СКЗИ в части пересмотра значимости (веса) некоторых угроз в отношении криптосредств.

10:00 –12:10	**Секция «Цифровая криминалистика и расследование инцидентов»** *Зал «Марс»*

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

Исследования цифровой информации: состояние, проблемы, решения

Яковлев Алексей Николаевич, *к.ю.н., Следственный комитет Российской Федерации*

Будет кратко представлено текущее состояние дел в области исследования компьютерных систем и технологий, включая формирование новых направлений исследования. Существенная часть доклада будет посвящена: планам федеральных регуляторов начать в 2016 году влиять на деятельность по исследованию компьютерных систем; решению Банком России схожих задач в области стандартизации сбора и анализа технических данных при расследовании некоторых видов инцидентов информационной безопасности; усилиям Минюста России по изменению федерального законодательства о судебно-экспертной деятельности в целом; иным факторам.

Криминалистический анализ данных Android приложений

Каррондеев Андрей Михайлович, *инженер-разработчик, Oxygen Software*

В данных мобильных приложений сосредоточено колоссальное количество информации. Эта информация крайне важна при проведении криминалистических расследований. Однако, чтобы ее извлечь и привести к виду, понятному следователю, приходится приложить немало усилий по деобфускации и декриптованию. В докладе на примерах демонстрируются основные этапы криминалистического анализа данных Android приложений.

Современная криминалистика или исследование «бестелесного» червя в сети предприятия

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

В случае заражения «бестелесным» червем оригинальный экземпляр вредоносной программы можно извлечь только из сетевого трафика в момент заражения. Алгоритм работы самого червя делает его удаление из сети практически невозможным. На примере этой новой угрозы будет рассмотрено исследование оперативной памяти и сетевого трафика, что прольет свет на возможные способы противодействия этой угрозе.

Инженерно-технические аспекты криминалистического анализа MacOS

Чиликов Алексей Анатольевич, *к.ф.-м. н., доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана,* ***Passware***

Анализ образов оперативной памяти и файлов гибернации может быть мощным инструментом в руках криминалиста, но его использование зачастую требует специальных знаний. Мы расскажем об особенностях шифрования файлов гибернации (sleepimage) в MacOS X, возможных путях его расшифрования и интерпретации извлеченных данных, взаимодействии sleepimage и системы полнодискового шифрования FileVault2.

Возможности извлечения юридически значимой информации из компьютеризированных систем автомобиля

Бережной Игорь Анатольевич, *Следственный комитет Российской Федерации*

Современные автомобили насыщены компьютеризированным оборудованием, которое фиксирует большое количество технических параметров движения автомобиля. В докладе будут раскрыты особенности исследования компьютеризированных систем автомобиля, в частности блоков управления подушками безопасности «EDR» (Event Data Recorder). Будут раскрыты наиболее значимые для расследований параметры работы систем автомобилей, приведены примеры использования результатов исследований для установления юридически значимых фактов.

12:30 –14:00	**Секция «Электронный документооборот»** *Конференц-зал*

Ведущие:

- ***Кузьмин Алексей Сергеевич,*** *д.ф.-м.н., профессор, председатель ТК 26*
- ***Соловьев Николай Николаевич,*** *советник генерального директора, Гроссмейстер*

Бумажный и электронный документ. Что общего? Возможна ли полная замена?

Соловьев Николай Николаевич, *советник генерального директора, Гроссмейстер*

Проблемы использования электронных документов и электронной подписи

Горностаев Владимир Павлович, *к.т.н., директор центра компетенции по защите информации, ИнтерТраст*

Применение сервисов безопасности для обеспечения юридической силы электронных документов

Сабанов Алексей Геннадьевич, *к.т.н., МГТУ им. Н.Э. Баумана, Аладдин Р.Д.*

Атрибутные сертификаты – завтрашний день или путь в никуда?

Петров Сергей Владимирович, *начальник отдела разработки средств защиты, Газинформсервис*

12:30 –14:00	**Секция «Облака в безопасности»** *Зал «Марс»*

Ведущие:

- ***Фатеев Олег Александрович,*** *эксперт, RCCPA*
- ***Белявский Александр Константинович****, коммерческий директор, Zecurion*

Безопасность из облаков

Бешков Андрей Юрьевич*, менеджер по развитию бизнеса гибридных облаков, Microsoft*

С переходом к гибридным облакам и мобилизацией пользователей привычные способы обеспечения безопасности довольно сильно поменялись, а некоторые вообще перестали быть действенными. В докладе будет проанализировано, как далеко зашла эта трансформация и как теперь можно применять облачные сервисы для контроля и защиты инфраструктур, приложений и данных.

Опыт выполнения требований 242-ФЗ российскими облачными операторами

Новицкая Оксана Витальевна, *директор по развитию, Облакотека*

С вступлением в силу нового закона 242-ФЗ перед облачными операторами встала задача обеспечить выполнение требований федерального закона в полной мере, соблюдая существующий режим обработки ПД и принимая необходимые меры для их защиты. В данном докладе будут рассмотрены основные требования закона и изменения, которые коснулись как операторов, так и заказчиков, способы реализации, а также варианты построения гибридных решений на базе облачных услуг.

Предоставление сервисов ИБ как облачных услуг SECaaS (SECurity as a Service)

Бражников Юрий Николаевич, *глава российского офиса, 5nine Software*

Новые угрозы в виртуальной среде. Проблемы СЗИ предыдущего поколения. Интеграция СЗИ на уровне ОС. Пример СЗИ для облака на базе Cloud OS. Интеграция СЗИ в клиентский портал и предоставление услуги SECaaS. Примеры реализации проектов.

Защита частного и гибридного облака

Харламов Павел Алексеевич, *IT менеджер, ActiveCloud*

Статистика и разновидности угроз возможных для облака. Защита данных в облаке, в том числе на уровне панели управления. Технические и организационные меры по обеспечению безопасности. Риски и решения по защите от DDoS атак. Решения для защиты документов и авторизации.

«Верхи не могут, низы не хотят», или «О том, как правильно в облаках SECaaS делать».

Феоктистов Константин Борисович, *главный архитектор проектов, Информзащита*

В процессе «поворачивания лицом в сторону облаков» большинство заказчиков в первую очередь вынуждены решать проблему обеспечения безопасности. Порой решение данной задачи с учетом существующих нормативных требований может быть достаточно существенной статьей расхода для потребителей облачных услуг. Как поставщику услуг защищенного облака предоставить услуги безопасности своим клиентам так, чтобы потом не было мучительно больно за безвозвратно потерянного клиента и неоправданные инвестиции.

Облачная безопасность не ограничивается конфиденциальностью

***Жбанков Антон Владимирович**, ведущий системный архитектор, Step Logic*

При разговоре про облачную безопасность большинство ограничивается вопросами конфиденциальности и разделения полномочий. Иногда ставят различные системы контроля доступа. В конечном итоге получается хорошо охраняемый вход в соломенную хижину, способную сложиться под порывом ветра. Как не забыть про целостность и доступность в облаках?

15:00 –17:00	**Секция «Криптография и криптоанализ» II часть.** *Зал «Марс»*

Ведущие:

- ***Кузьмин Алексей Сергеевич**, ТК 26*
- ***Попов Владимир Олегович**, Ассоциация «РусКрипто», КРИПТОПРО*
- ***Жуков Алексей Евгеньевич,** Ассоциация «РусКрипто», МГТУ им. Баумана*

Постквантовая криптография. Критический обзор и дополнения

***Кренделев Сергей Федорович,** к.ф.-м.н., доцент, Новосибирский государственный университет*

В докладе рассматриваются математические аспекты постквантовой криптографии. Делается критический обзор существующих решений и криптографических приложений. В качестве приложения к докладу рассматриваются новые подходы и реализации основных криптографических примитивов.

Методы обеспечения конфиденциальности пространственных данных в облаке у недоверенного провайдера, предоставляющие возможность выполнения пространственных запросов к этим данным

***Матерухин Андрей Викторович**, к.т.н., доцент кафедры ИИС, Московский государственный университет геодезии и картографии*

Доклад представляет собой обзор результатов современных исследований по тематике доклада. В докладе рассматриваются методы преобразования пространственных данных, основанные на иерархическом разбиении пространства; методы преобразования пространственных данных, основанные на использовании криптографических хэш-функций; схемы криптографической трансформации пространства, основанные на использовании B+ или R* деревьев; схемы, основанные на идеях предикативного шифрования.

Частичное маскирование шифра «Кузнечик»

***Жиляев Андрей Евгеньевич,** исследователь отдела научных исследований, ИнфоТеКС*
***Щербакова Анна Олеговна,** исследователь ЦНИПР, ИнфоТеКС*

В докладе рассматривается способ выбора необходимого количества раундов для частичного маскирования «Кузнечика», а также оцениваются трудозатраты такого маскирования.

О сложности перебора ключей в квантовой криптографии

***Молотков Сергей Николаевич,** д.ф.-м.н., член-корреспондент академии криптографии, профессор, МГУ им. М.В. Ломоносова*

Показана прямая связь между сложностью полного перебора ключей, который является одним из основных критериев секретности в классических системах, и следовым расстоянием, используемым в квантовой криптографии. Приведены границы на минимальное и максимальное число шагов перебора, за которые определяется истинный ключ.

Протокольные решения для безопасного формирования электронной подписи в облаке

***Смышляев Станислав Витальевич**, к.ф.-м.н., начальник отдела защиты информации, КРИПТО-ПРО*

***Алексеев Евгений Константинович**, к.ф.-м.н., ведущий инженер-аналитик, КРИПТО-ПРО*

Рассматриваются принципы построения системы формирования электронной подписи на сервере, в которой подтверждение операции осуществляется с помощью пользовательской SIM-карты и алгоритма выработки кода аутентификации сообщения. Рассказывается об основных элементах данной системы, приводятся модели нарушителя, в которых обеспечивается ее безопасность.

О возможных подходах к построению механизмов выработки производных ключей и механизмов выработки псевдослучайных последовательностей

***Лавриков Иван Викторович**, ТК 26*

***Рудской Владимир Игоревич**, ТК 26*

В докладе рассматривается ряд подходов к построению механизмов выработки производных ключей и псевдослучайных последовательностей. На основе анализа их криптографических и эксплуатационных характеристик даются предложения по наиболее перспективным механизмам с точки зрения национальной стандартизации.

15:00 –17:00	**Секция «Информационная безопасность в России»** *Конференц-зал*

Ведущая: ***Старостина Екатерина Вячеславовна**, менеджер, Cyber Security, Advisory Services, EY*

Инвестиции, тренды и технологии: основные данные глобального исследования в области ИБ для России

***Старостина Екатерина Вячеславовна**, менеджер, Cyber Security, Advisory Services, EY*

Доклад построен на глобальном исследовании 2015 года. Это результаты опроса 1755 представителей руководства, специалистов в ИТ и ИБ из крупнейших компаний, а также ведущих мировых экспертов по информационной безопасности, включая Россию. Будет представлена информация о рынке ИБ России и рассказано о бюджетировании и инвестициях, вопросах управления ИБ в России и мире. Будут подняты вопросы угроз и уязвимостей, рассказано о том, какие новые технологии и тренды приходят в Россию.

Взгляд на рынок ИБ России со стороны крупного корпоративного заказчика

***Волков Алексей Николаевич**, начальник отдела эксплуатации средств защиты информации управления по защите информации, Северсталь Менеджмент*

Рынок информационной безопасности в России - удивительная и самобытная субстанция. В отсутствие реальных драйверов роста все, чем могут завлекать продавцы, сосредоточено в рисках и возможностях. Но последних, увы, осталось совсем мало, а первые не так давно перекочевали из области «кибер» в область «гос». Покупатели, порядком устав от наблюдения законодательной чехарды, охладели к compliance и ждут, что им предложат взамен. Какие новые «фишки» предлагают вендоры, как их воспринимают заказчики и какое влияние это оказывает на развитие ИБ в реальном секторе экономики.

Видение использования криптографии в современных и перспективных продуктах

***Мамыкин Владимир Николаевич**, директор по информационной безопасности, Microsoft Россия*

Кибербезопасность, основные угрозы 2016 и новые технологии Intel

***Ларюшин Дмитрий Викторович**, Intel в России/СНГ*

В докладе будет озвучено видение Intel Security Group как будут меняться модели кибер-угроз и поведение организаторов кибер-атак, и как индустрия информационной безопасности будет отвечать на новые угрозы, на ближайшие 5 лет (горизонт 2020). Следствием этих оценок являются подходы Intel в реализации ключевых аппаратных и программных технологий в поле информационной безопасности и доверенного исполнения программных приложений в продуктах компании (AES-NI, TXT и SGX).

Перспективы решений Mobile ID в Российской Федерации

***Маркович Леонид Львович,** директор по маркетингу, А1 Системс*

История решений Mobile ID насчитывает уже более 10 лет. В последние 3 года в мире наблюдается значительный рост, как предложения, так и спроса на эти решения. Что скрывается за названием «Mobile ID»? Стоит ли ожидать появления таких решений в России? Какими они будут и каковы основные сферы их применения?

15:00 –17:00	**Секция «Интеллектуальные методы анализа нарушений кибербезопасности»** *Зал «Стеклянный»*

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

Подход к оценке безопасности киберфизических систем на основе фрактальных методов

***Зегжда Петр Дмитриевич,** профессор, д.т.н., СПбПУ ИБКС*

Применение методов машинного обучения для анализа безопасности приложений Android

***Павленко Евгений Юрьевич,** руководитель проекта, НеоБИТ*

Siem-система для выявления и анализа инцидентов безопасности в интернете вещей

***Лаврова Дарья Сергеевна,** аспирант, СПбПУ ИБКС*

Система распределенной аутентификации в интернете вещей на основе изогений эллиптических кривых

***Александрова Елена Борисовна,** профессор, к.т.н., СПбПУ ИБКС*

Обеспечение безопасности гетерогенных систем с применением гомоморфной модулярной криптографии

***Шенец Николай Николаевич,** старший преподаватель, СПбПУ ИБКС*

Оценка пропускной способности стеганографических каналов передачи информации и возможности их выявления методом статистического анализа
Бусыгин Алексей Геннадьевич, *НеоБИТ*

Автоматизация поиска уязвимостей с помощью обратной трассировки графа передачи управления
Демидов Роман Алексеевич, *аспирант, СПбПУ ИБКС*

17:30 – 19:30	**Секция «Блокчейн и криптовалюты. Использование «пограничных» технологий в мирных целях»** *Конферец-зал*

Ведущие:

- ***Комисаренко Владимир Владимирович,*** *Ассоциация «РусКрипто», директор по развитию, БЕЛТИМ СБ*
- ***Архипов Алексей Сергеевич****, директор по криптотехнологиям, QIWI*

Безопасность технологии блокчейн. Основные направления исследований и анализ научных публикаций

Комисаренко Владимир Владимирович*, Ассоциация «РусКрипто», директор по развитию, БЕЛТИМ СБ*
Роговой Александр, *эксперт по технологии блокчейн*
В докладе будут приведены основные угрозы на информационные системы, построенные по принципу блокчейн, определены подходы к оценке сложности атак. Отдельное внимание будет уделено направлениям исследований, результаты которых публикуются, в том числе по итогам международных конференций.

Проблемы производительности блокчейн
Архипов Алексей Сергеевич*, директор по криптотехнологиям, QIWI*
Увеличение производительности блокчейн, сложности и подводные камни. Оценка различных подходов повышения производительности, технологический прогноз.

О валютах и криптографии в криптовалютах
Дыгин Денис Михайлович, Лавриков Иван Викторович, Маршалко Григорий Борисович, *ТК 26*
В докладе с точки зрения функционального содержания анализируются протоколы, которые используются для реализации криптовалют. Проводится анализ задач, решаемых тем или иным протоколом и используемых для этого метода.

Блокчейн как облачная услуга - Blockchain as a Service (BaaS)
Фатеев Олег Александрович, *координатор, OpenStack Russia*
В докладе будет рассказано о возможности использования технологий блокчейн по модели облачной услуги на примере проекта Ethereum BlockChain as a Service. Основной акцент будет сделан на практический аспект, связанный с разработкой и развертыванием блокчейн-проектов в облачной инфраструктуре. Будут рассмотрены перспективы предоставления таких услуг на ресурсах российских облачных провайдеров.

Обсуждение. Открытая дискуссия.

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

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

Применение новых методов визуализации для отображения метрик безопасности компьютерной сети

Чечулин Андрей Алексеевич, *доцент кафедры Защищенных систем связи (ЗСС), СПбГУТ*

Представляется подход к применению диаграммы Вороного для визуализации метрик защищенности компьютерной сети. Данный подход позволяет объединить достоинства таких моделей визуализации, как карты деревьев и графов атак. В докладе представлены основные этапы построения визуализационной модели и описан программный прототип, реализующий данный подход.

Автоматическая классификация вредоносного программного обеспечения для платформы Android

Гамаюнов Денис Юрьевич, *к.ф.-м.н., с.н.с., лаборатория интеллектуальных систем кибербезопасности факультета ВМК, МГУ имени М. В. Ломоносова*

В работе предложен метод обнаружения вредоносного ПО на основе автоматические построения статических моделей анализируемого приложения и сравнения с моделями вредоносных приложений. Статические модели основаны на множестве привилегий и цепочках API-вызовов, используемых в приложении, из которых формируются основные последовательности. Результаты экспериментов показывают, что предложенный метод имеет лучшие показатели точности и полноты, чем ранее опубликованные полностью автоматические методы анализа, и может быть использован при построении инструментальных средств автоматизированной классификации ВПО для Android.

Методики корреляции событий безопасности для обнаружения целевых атак

Федорченко Андрей Владимирович, *лаборатория проблем компьютерной безопасности, СПИИРАН*

Рассматриваются исследования целевых атак с целью разработки методов их обнаружения. Предлагается определение теоретических свойств и практических особенностей атак данного класса. Основу методик составляют различные способы корреляции получаемых событий безопасности. Описываются программный стенд испытаний разработанных методик и результаты оценки их результативности.

Выбор и комбинирование элементов для построения комплексной системы кибер-физической безопасности

Десницкий Василий Алексеевич, *к.т.н., лаборатория проблем компьютерной безопасности, СПИИРАН*

Рассматривается подход к выбору и комбинированию различных элементов кибер-физической безопасности для построения комплексной системы безопасности. Для комбинирования элементов предлагается использовать модульный подход к построению архитектуры системы безопасности. Практические аспекты предлагаемого подхода будут продемонстрированы на примере процесса разработки системы контроля и управления доступом на базе интеллектуальных микроконтроллеров.

Распознавание стека прикладного программного обеспечения на серверной стороне веб-приложения

Самосадный Кирилл Алексеевич, *лаборатория безопасности информационных систем, факультет ВМК, МГУ имени М. В. Ломоносова*

Проблема определения стека прикладного программного обеспечения, на базе которого построен исследуемое веб-приложение, является одной из основных при анализе защищенности методом черного ящика. В данной работе предлагается решение этой проблемы на основе выделения набора признаков и автоматического обучения классификаторов на основе методов машинного обучения. Также решается связанная задача выявления всех веб-приложений, которые построены на том же наборе прикладного ПО, что и некоторый эталон.

Подход к моделированию компьютерных атак на основе стохастических сетей

Лаута Олег Сергеевич, *к.т.н., Военная академия связи*

Рассматривается подход к моделированию компьютерных атак в инфокоммуникационных сетях (ИКС), основанный на применении метода топологического преобразования стохастических сетей. Дается оценка вероятностно-временных характеристик ряда типовых компьютерных атак с помощью полученных рекуррентных математических выражений. На основе результатов оценки компьютерных атак предлагается методика оценки киберустойчивости ИКС.

Модели управления рисками информационной безопасности в мультисервисных системах связи на основе нечетких ситуационных сетей

Агеев Сергей Александрович*, к.т.н., Военная академия связи*

Приводятся результаты исследования математических моделей методов и алгоритмов управления рисками угроз информационной безопасности (ИБ) мультисервисных систем связи (МСС), функционирующих в режиме времени, близком к реальному. Решаемая задача сводится к иерархической совокупности многопараметрических и многокритериальных задач математического программирования. Для повышения оперативности выработки и принятия управленческих решений по минимизации угроз рисков ИБ МСС предлагается использовать модифицированный метод нечетких ситуационных сетей. Приводится анализ результатов математического моделирования рисков ИБ для различных вариантов построения МСС, показывающий высокую эффективность предложенных моделей.

Функция риска для многофакторной аутентификации в Интернете вещей

Беззатеев Сергей Валентинович, *д.т.н., заведующий кафедрой «Технологий защиты информации», ГУАП*

Предлагается адаптировать один из подходов, основанный на вероятностных методах, для решения задачи принятия решения об аутентификации пользователя на основе множества разнородных факторов, получаемых от носимых устройств. При этом использован аппарат оценки финансовых рисков для определения эффективности принимаемых решений и настройки параметров решающей функции. Применение описанного подхода позволяет существенно повысить универсальность, гибкость и надежность многофакторных систем аутентификации.

17:30 – 19:30	**Семинар «Защита информационных ресурсов от действий иностранных технических разведок. Конкурентная разведка vs ИТР»** *Зал «Стеклянный»*

Ведущий: ***Масалович Андрей Игоревич,*** *ведущий эксперт по конкурентной разведке, АИС*

Компания «КРИПТО-ПРО»

Компания КРИПТО-ПРО занимает лидирующее положение в сфере разработки средств криптографической защиты информации (СКЗИ) и развития Инфраструктуры Открытых Ключей (PKI) на территории РФ. Специалистами КРИПТО-ПРО 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;
- первый в России сертифицированный аппаратный криптографический модуль – Атликс HSM;
- первые в истории сообщества Интернет стандарты, описывающие применение российских криптоалгоритмов – RFC 4357, RFC 4490, RFC 4491;
- первое в России сертифицированное СКЗИ, разработанное в соответствии со спецификацией JCA (Java Cryptography Architecture) – КриптоПро JCP;
- первые в России стандарты по применению российских криптоалгоритмов в Ipsec.

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

Контактная информация:
www.cryptopro.ru
info@cryptopro.ru
+7 (495) 780-48-20

Компания «Актив»

Компания «Актив» - ведущий разработчик программно-аппаратных средств информационной безопасности и самый крупный производитель электронных ключей и идентификаторов в России. Компания основана в 1994 году и занимается производством аппаратных средств аутентификации Рутокен, а также средств защиты программного обеспечения от нелегального копирования Guardant.

Продукция линейки Рутокен предназначена для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и электронной цифровой подписи (ЭЦП). USB-токены Рутокен являются ключевыми носителями в государственных и коммерческих проектах, базирующихся на технологии ЭЦП и инфраструктуре открытых ключей (PKI). Все устройства имеют сертификаты ФСБ и ФСТЭК, подтверждающие соответствие требованиям к средствам криптографической защиты информации (СКЗИ) класса КС2 и требованиям к техническим средствам защиты информации класса НДВ3. Наличие сертификатов позволяет использовать идентификаторы Рутокен в системах, обрабатывающих конфиденциальную информацию, а также при работе с информацией, имеющей гриф «С» (гос.тайна).

Контактная информация:
www.aktiv-company.ru; www.rutoken.ru; www.guardant.ru
info@aktiv-company.ru
+7 (495) 925-77-90

Компания «ИнфоТеКС»

ОАО «ИнфоТеКС» является одной из ведущих ИТ-компаний отечественного рынка программных VPN решений и средств защиты информации в TCP/IP сетях.

Ключевой разработкой ИнфоТеКС является технология ViPNet. На сегодняшний день это самое масштабируемое отечественное решение для построения защищенных VPN-сетей. Торговая марка ViPNet объединяет целый ряд продуктов и сетевых решений для крупного, среднего и малого бизнеса, являясь одним из сильнейших и уважаемых брендов в России в сфере высоких технологий.

Компания совместно с партнерами предлагает полный спектр услуг по проектированию и внедрению систем информационной безопасности на объектах любого уровня сложности:

- проведение обследований ИС;
- разработка и согласование моделей угроз и технических заданий на системы защиты ИС;
- разработка технических проектов на системы защиты ИС;
- установка и настройка средств защиты информации;
- аттестация объектов информатизации;
- техническое сопровождение;
- обучение специалистов заказчика.

Продукты ИнфоТеКС регулярно проходят сертификацию в ФСБ и ФСТЭК России, а также в системе добровольной сертификации ГАЗПРОМСЕРТ.

В числе заказчиков ИнфоТеКС: предприятия госсектора, банки, телекоммуникационные компании, крупнейшие организации нефтегазодобывающей, перерабатывающей и металлургической отраслей.

ИнфоТеКС выполняет функции официальной секретарской компании Технического комитета по стандартизации №26 «Криптографическая защита информации».

Контактная информация:
www.infotecs.ru
soft@infotecs.ru
+7 (495) 737-6192

Компания «БИФИТ»

Компания «БИФИТ» основана в 1999 году в Москве.

Направления деятельности компании:

- разработка, внедрение и сопровождение решений ДБО для коммерческих банков;
- разработка, производство и поставка программных и аппаратных СКЗИ;
- внедрение промышленных решений Fraud-мониторинга;
- разработка и внедрение решений, предоставление услуг по защите от DDoS-атак.

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 более 750 тысяч корпоративных клиентов и более миллиона 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.

Контактная информация:
www.bifit.com
info@bifit.com
+7 (495) 797-88-89

Компания «Код Безопасности»

Компания «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» разрабатывает несколько линеек продуктов, объединенных единым архитектурным замыслом и ориентированных на обеспечение безопасности различных компонентов информационной системы. Такой подход позволяет нашим заказчикам поэтапно развивать свою систему обеспечения информационной безопасности, добавляя новые компоненты, расширяющие область действия уже внедренных средств защиты.

«Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации.

Контактная информация:
www.securitycode.ru
info@securitycode.ru
+7 (495) 982-30-20

Компания Check Point Software Technologies Ltd.

Check Point® Software Technologies Ltd. является крупнейшим в мире вендором, специализирующимся исключительно на интернет-безопасности.

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.

Контактная информация:
www.rus.checkpoint.com
+7 (495) 967-74-44

Компания «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» – один из ведущих российских разработчиков сертифицированных продуктов сетевой защиты информации.
Компания входит в тройку лидеров рынка VPN-продуктов, имеет все лицензии ФСТЭК России и ФСБ России, необходимые для разработки, производства и распространения криптографических средств защиты конфиденциальной информации.
Продукты С-Терра – программные и программно-аппаратные комплексы –сертифицированы на соответствие требованиям ФСБ России к криптографическим средствам различных классов защищенности (КС1, КС2, КС3), а также требованиям нормативных документов ФСТЭК России к средствам защиты от несанкционированного доступа (НСД).

Широкое применение в госструктурах различных уровней (в Совете Федерации России, Генпрокуратуре России, ФСБ России, МВД России, МЧС России, ФСКН России), в крупнейших финансовых, коммерческих и производственных организациях обусловлено высокой производительностью, масштабируемостью, надежностью и сетевой функциональностью разработок С-Терра.

Компания имеет опыт успешного решения ряда задач по защите информации в условиях экономических санкций, исполнения установок руководства страны, в том числе Указа Президента РФ №260 от 22.05.2015 г.

Контактная информация:
www.s-terra.ru
sales@s-terra.ru
+7 (499) 940-90-01

Компания «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 сетей передачи данных, телекоммуникационных узлов и других информационных систем в защищенном исполнении.

Компания «Фактор-ТС» - это комплексный подход к решению задач обеспечения информационной безопасности систем передачи информации в соответствии с требованиями российского законодательства.

Программно-аппаратные комплексы производства «Фактор-ТС» (маршрутизаторы, криптомаршрутизаторы, межсетевые экраны, клиентские средства защиты и др.) имеют сертификаты соответствия требованиям ФСТЭК, МО и ФСБ России по различным классам защиты.

Заказчиками ООО «Фактор-ТС» являются Министерство обороны РФ, ФСБ РФ, ВСИН РФ, ФСО РФ, МВД РФ, Банк России, ФНС РФ, предприятия ВПК, а также другие министерства и ведомства.

Контактная информация:
www.dionis-nx.factor-ts.ru
factor@factor-ts.ru
+7 (495) 644-31-30

Компания ISBC

Группа компаний ISBC является ведущим российским поставщиком оборудования и решений для построения систем информационной безопасности, контроля физического доступа, программ лояльности и других проектов с использованием смарт-карт с 2002 года.

На данный момент ISBC Group выступает эксклюзивным дистрибьютором продукции ведущих мировых вендоров оборудования и решений в сфере смарт-карт, RFID и NFC-технологий, а также является производителем смарт-карт.

ESMART® – зарегистрированный торговый знак Группы компаний ISBC.
Продукты и решения, выпускающиеся под брендом ESMART®, предназначены для использования в качестве безопасного хранилища ключевой информации, защиты электронной подписи, а также для обеспечения строгой двухфакторной аутентификации пользователей в ОС и информационных системах.

Контактная информация:
www.isbc.ru;
www.esmart.ru
+7(495)739-86-99

Компания Microsoft

Компания Microsoft — мировой лидер в области информационных технологий, поставляющий широкий диапазон устройств и сервисов, программного обеспечения и ИТ-услуг. Это одна из крупнейших в мире корпораций, работающая в более чем 190 странах мира.

Компания Microsoft действует в России с 1992 года. На сегодняшний день компания активно работает в 70 городах страны. Головной офис находится в Москве, региональные центры — в Санкт-Петербурге, Казани, Екатеринбурге, Ростове-на-Дону, Новосибирске.

Портфель продуктов и услуг Microsoft включает настольные и сетевые операционные системы, устройства (Xbox 360, Xbox One, Kinect, Surface и др.), серверные приложения, настольные бизнес-приложения и офисные приложения для конечных пользователей, облачные решения, интерактивные программы, сервисы и игры, средства для работы в Интернете, инструменты разработки и многое другое.

Облака и мобильность становятся главными приоритетами для Microsoft в соответствии со стратегией, объявленной Сатьей Наделлой, новым CEO корпорации. Microsoft предлагает клиентам и партнерам уникальный наиболее полный спектр «облачных» возможностей для создания и использования частного, публичного или гибридного облака.

Контактная информация:
https://www.microsoft.com/ru-ru/securitycertification/default.aspx

Компания «НеоБИТ»

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.

Основные виды деятельности:

- выполнение научно-исследовательских, проектно-конструкторских и проектно-технологических работ по созданию защищенных информационных систем, распределенных систем обработки и передачи данных;
- аудит состояния информационных систем и анализ безопасности распределенных систем обработки информации, в том числе работающих в сети Интернет;
- оперативное реагирование на возникающие угрозы безопасности систем и расследование компьютерных инцидентов;
- анализ уязвимости программного обеспечения, операционных систем, сетевых сервисов, баз данных и средств управления телекоммуникациями;
- разработка технологий контроля и управления доступом к информационным ресурсам на базе защищенных операционных систем;
- оказание услуг по внедрению и интеграции средств защиты информации.

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

Контактная информация:
www.neo-bit.ru
info@neo-bit.ru
+7(812)535-28-06, 535-88-67

Компания «РТ-ИНФОРМ»

ООО «РТ-ИНФОРМ» – инфраструктурное 100% дочернее общество Госкорпорации Ростех. В соответствии с решением Корпорации является единым центром компетенции при осуществлении торгово-закупочной деятельности холдинговых компаний и организаций Корпорации в сегменте информационных технологий, систем информационной безопасности и другого оборудования, приобретения, внедрения, сопровождения программного обеспечения для управления производственными предприятиями и холдинговыми структурами, оказания услуг в области информационных технологий.

Контактная информация:
www.rtinform.ru
info@rtinform.ru
+7 (499) 557-06-52

Компания «Инсайд РУС»

Компания «Инсайд РУС» занимается поставками и продвижением в России программных и аппаратных средств обеспечения информационной безопасности с 2011 года.

Портфолио компании включает в себя защищенные криптографические микроконтроллеры и программное обеспечение французской компании INSIDE Secure, криптографические микросхемы Atmel, а также собственную разработку – универсальный модуль безопасности с поддержкой отечественных алгоритмов криптографии «Инсайд РУС. ГОСТ».

Контактная информация:
www.inside-rus.ru
info@inside-rus.ru
+7 (812) 331-09-67

Компания «Газинформсервис»

Компания «Газинформсервис» — один из крупнейших в России системных интеграторов в области безопасности и разработчик уникальных программных продуктов, специализирующийся на создании систем информационной безопасности и систем обеспечения безопасности объектов для крупных корпораций энергетической и транспортной отраслей, органов государственной власти и местного самоуправления, а также учреждений финансового сектора и сектора здравоохранения.

Компания оказывает полный комплекс услуг в области информационной безопасности и обеспечения безопасности объектов: занимается проектированием, внедрением, сопровождением, подготовкой специалистов заказчика, а также участвует в разработке нормативной документации. Программные продукты собственной разработки неоднократно становились лауреатами престижной премии «За Укрепление Безопасности России». «Газинформсервис» предоставляет услуги испытательной лаборатории, проводит работы по аттестации и сертификации, а также оказывает консалтинговые услуги в области информационной безопасности и обеспечения безопасности объектов.

Богатый опыт создания и внедрения различных комплексов защиты для крупных объектов, высокая профессиональная оценка услуг и продукции компании со стороны Заказчиков, крепкие партнерские отношения с ведущими вендорами обеспечили нам стабильное положение на рынке.

Контактная информация:
www.gaz-is.ru
resp@gaz-is.ru
+7 (812) 677-20-50

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, входит в группу компаний «Стинс Коман». В течение 19 лет АИС предоставляет образовательные услуги по информационной безопасности, информационным технологиям, конкурентной разведке и системам управления.

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.

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

Контактная информация:
www.infosystems.ru; www.vipforum.ru
security@infosystem.ru
+7 (495) 120-04-02

Компания Актив

Компания «Актив» — ведущий разработчик программно-аппаратных средств информационной безопасности и самый крупный производитель электронных ключей и идентификаторов в России. Компания основана в 1994 году и занимается производством аппаратных средств аутентификации Рутокен, а также средств защиты программного обеспечения от нелегального копирования Guardant.

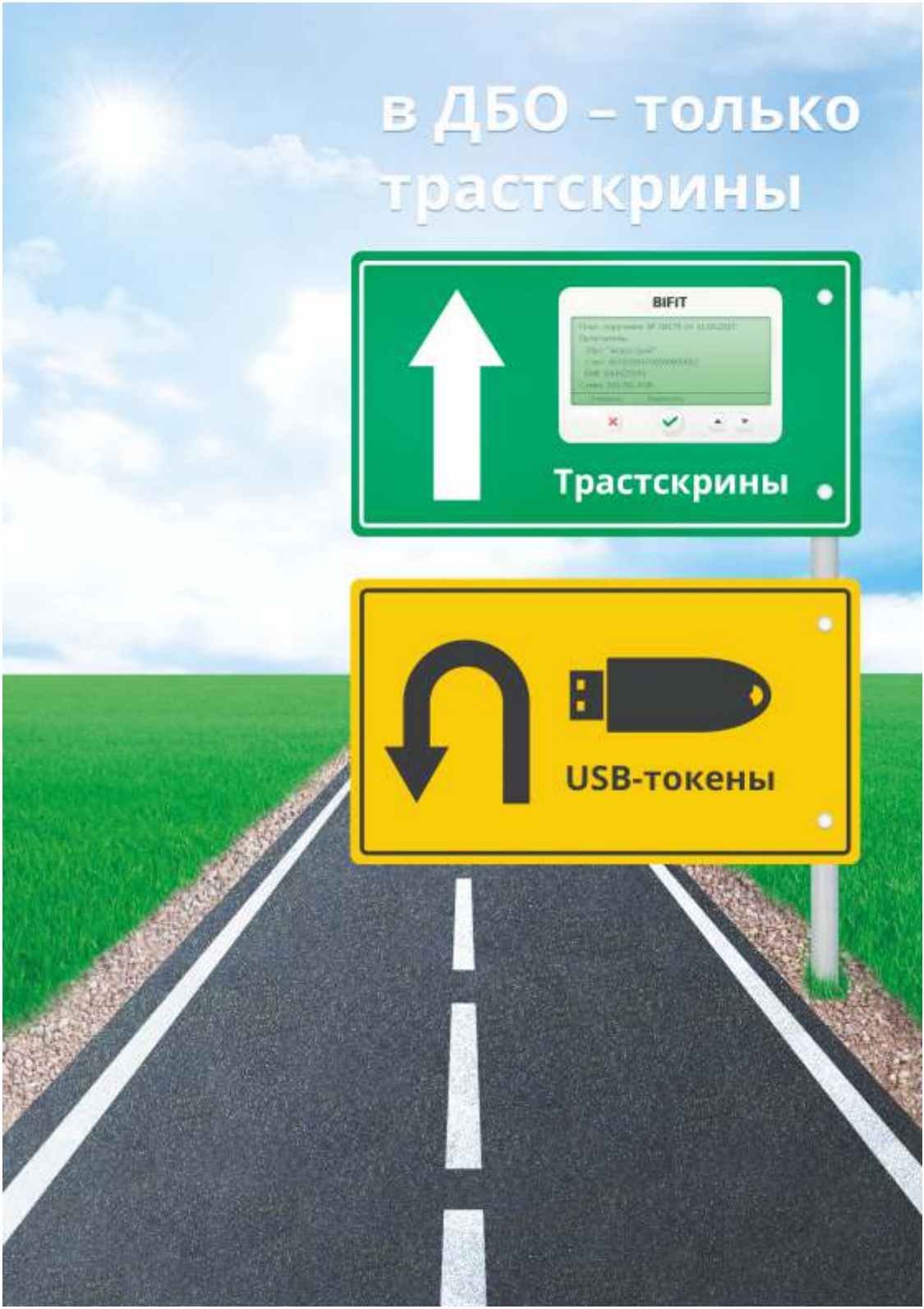
Продукция **Рутокен —** это персональные устройства доступа к информационным ресурсам, предназначенные для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и электронной подписи (ЭП). USB-токены Рутокен являются ключевыми носителями в коммерческих и государственных проектах, базирующихся на технологии ЭП и инфраструктуре открытых ключей (PKI).

Линейка продукции **Guardant** обеспечивает защиту ПО от компьютерного пиратства и включает в себя локальные ключи и их сетевые версии. В устройствах Guardant реализованы все современные возможности защиты программ при помощи электронных ключей.

- **Россия, Москва, Шарикоподшипниковская ул.,1**
- **+7 495 925-77-90**
- **www.rutoken.ru**
- **www.guardant.ru**

https://www.facebook.com/aktivsoft

https://twitter.com/rutoken


в ДБО – только трастскрины
BiFIT
Трастскрины
USB-токены

Код безопасности

SECRET NET STUDIO

Комплексное решение для защиты рабочих станций и серверов на 5 уровнях

- Защита от НСД
- Контроль устройств
- Межсетевой экран
- Обнаружение и предотвращение вторжений
- Антивирус
- Шифрование данных и трафика

www.securitycode.ru 8 (495) 982-30-20 buy@securitycode.ru

Защита информации – наш профиль!

ФАКТОР-ТС

«Фактор-ТС» предлагает решения в области обеспечения информационной безопасности на базе отечественной авторской разработки - технологии DioNIS.
Компания имеет лицензии и сертификаты соответствия ФСБ, ФСТЭК и МО России.

Изделия на базе технологии DioNIS:

- маршрутизаторы
- криптомаршрутизаторы
- межсетевые экраны
- почтовые серверы
- клиентские программы со средствами криптозащиты

«Фактор-ТС» – это:

- высокое качество продукции
- наличие производственных мощностей
- надежное обслуживание
- высокий научно-технический потенциал

Полный цикл работ при изготовлении изделий:

- разработка
- производство
- внедрение
- сопровождение

123290, г. Москва,
1-й Магистральный проезд, д.11, стр. 1
+7 (495) 644-31-30
factor@factor-ts.ru

ФАКТОР-ТС

Microsoft

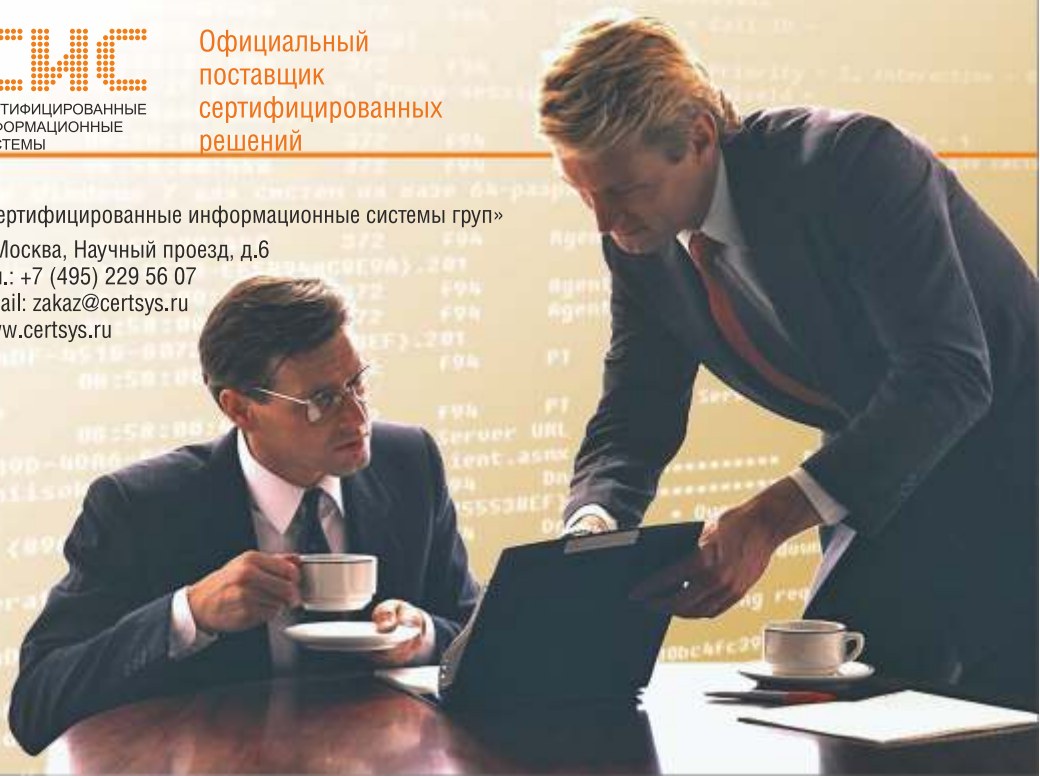
СЕРТИФИЦИРОВАННЫЕ ПРОДУКТЫ MICROSOFT

- Соответствие национальным требованиям в условиях импортозамещения
- Защита конфиденциальной информации и персональных данных
- Удобные настройка и контроль политик безопасности
- Снижение затрат на внедрение и поддержку
- Простой способ защитить информацию без использования наложенных средств

СИС
СЕРТИФИЦИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Официальный поставщик сертифицированных решений

«Сертифицированные информационные системы груп»
г. Москва, Научный проезд, д.6
Тел.: +7 (495) 229 56 07
Email: zakaz@certsys.ru
www.certsys.ru



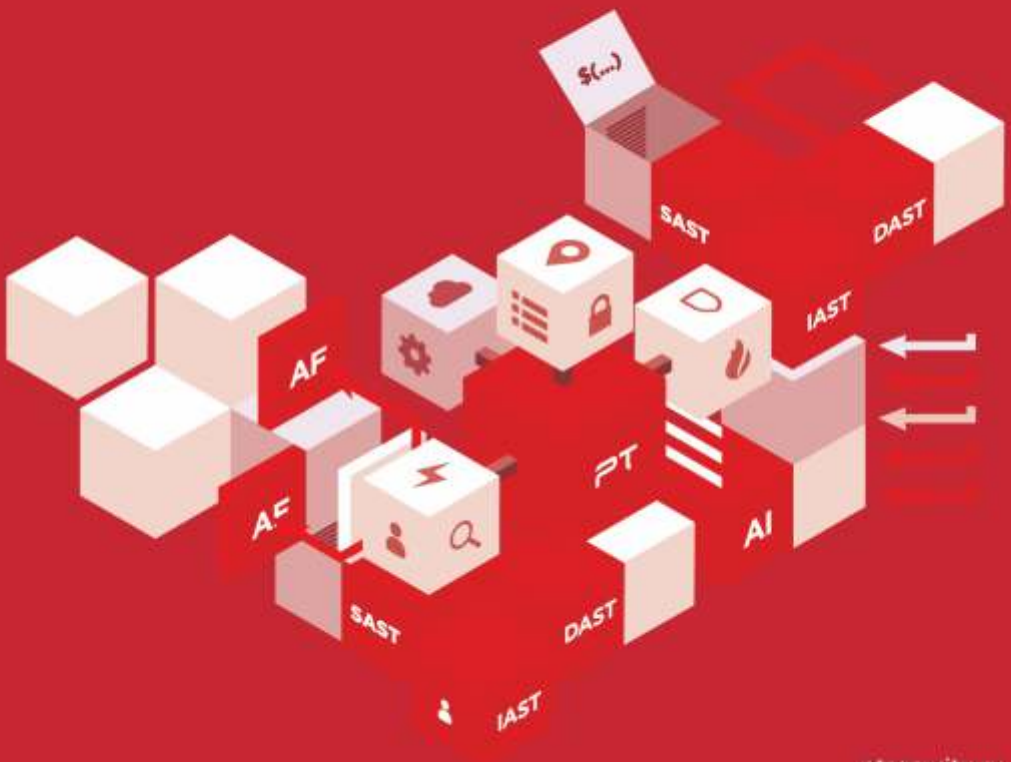
POSITIVE TECHNOLOGIES

Защита крупных информационных систем от кибер-угроз

Более 13 лет опыта и экспертных знаний по практической безопасности

Продукты и услуги обеспечивают:

- анализ защищенности и оценку соответствия стандартам;
- блокирование атак, включая ранее неизвестные (0-day);
- анализ безопасности кода приложений и построение безопасной разработки.
- мониторинг событий безопасности и предотвращение вторжений;
- расследование инцидентов и оценку защитных мер;



ptsecurity.ru

IV Международная научно-практическая конференция

«Управление информационной безопасностью в современном обществе»

31 мая - 2 июня 2016 года

г. Москва, ул. 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
- Презентация магистерской программы «Управление информационной безопасностью» НИУ «Высшая школа экономики»

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.

УСЛОВИЯ УЧАСТИЯ

Для представителей научного сообщества, органов государственной власти и управления, преподавателей, аспирантов и студентов	Бесплатно
Для разработчиков средств информационной безопасности, организаций, осуществляющих деятельность в области защиты информации, представителей бизнес-сообщества	По согласованию

В ПРОШЛОМ ГОДУ

2 дня общения с лучшими экспертами России, Европы, Северной и Южной Америки

Контакты: Пученкина Юлия, Кочукова Виктория
+7(495) 120-04-02, conf@infosystem.ru
www.vipforum.ru

Лица конференции

Соколов И.А.
Директор Института проблем информатики Российской академии наук (ИПИ РАН)

Шмид А. В.
д.т.н., профессор, Председатель Правления "ЗАО "ЕС-лизинг"

Зегжда П. Д.
Зав. кафедрой информационной безопасности компьютерных систем СПбГПУ Петра Великого, Заслуженный деятель науки, профессор, д.т.н.

Баранов А.П.
Заведующий кафедрой информационной безопасности НИУ ВШЭ, Председатель оргкомитета

Будзко В.И.
Заместитель директора Института проблем информатики Российской академии наук по научной работе

АИС
Академия Информационных Систем

«Академия
Информационных Систем»
Адрес: 111123, г. Москва,
ул. Плеханова, 4а, БЦ Юником
Тел. в г. Москве:
+7(495) 120-04-02
Тел. в г. Астане:
+7 7172-788-158
Сайт:
www.infosystems.ru
www.vipforum.ru

В течение 19 лет Академия Информационных Систем (АИС) предоставляет образовательные услуги по информационной и экономической безопасности, информационным технологиям и конкурентной разведке. Обучение своих кадров 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 многие другие.

Нам доверяют:

Северсталь · Ростелеком (Больше возможностей) · Гознак · Альфа-Банк · Сбербанк (Всегда рядом) · МТС

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

Более 300 курсов по направлению «Информационные технологии»

Всестороннее 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.

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

Большой выбор тренингов и семинаров по бизнес-образованию

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

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

Обучение по системе автоматизированного проектирования (САПР)

70 высококвалифицированных тренеров, обладающих большим практическим опытом и международными сертификациями

Технологии дистанционного обучения, вебинары и онлайн-тестирования

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

Для заметок

КАЛЕНДАРЬ МЕРОПРИЯТИЙ

Запланируй этот год с нами!

31 МАЯ – 2 ИЮНЯ 2016

IV Международная научно-практическая конференция «Управление информационной безопасностью в современном обществе»

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

www.vipforum.ru

7 ИЮНЯ 2016

IV Всероссийская отраслевая конференция «Безопасность критически важных объектов ТЭК»

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.

www.vipforum.ru

6-9 СЕНТЯБРЯ 2016

XV Всероссийская конференция «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ-2016»

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

www.vipforum.ru

ОКТЯБРЬ 2016

Ежегодный форум «Экономическая безопасность и конкурентная разведка 2016»

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.

www.vipforum.ru

19-21 ОКТЯБРЯ 2016

VIII Конференция «Электронная торговля. Информационная безопасность и PKI»

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

www.pki.ineurasia.ru

ДЕКАБРЬ 2016

VII Международный форум «Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia – 2016»

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

www.vipforum.ru

МАРТ 2017

XIX Научно-практическая международная конференция «РусКрипто'2017»

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

www.ruscrypto.ru

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'2016» указано в программе.

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

- 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.
- 24 марта в 08:00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 24 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»:

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

Внимание! Автобусы с табличкой «РусКрипто'2016» 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 – 22 марта с 16:00

Выезд – 25 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