Тайм-лайн конференции

27 марта, среда. День заезда

16.30	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»
18:00 – 20:00	Заезд и регистрация участников, проживающих в отеле. Ужин
20:00 – 22:00	Организационный сбор участников РусКрипто (*Конференц-зал*)

28 марта, четверг. Первый день работы конференции

7:30	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»	
8:00 – 8:20	Зарядка (*сбор у ресторанного комплекса*)	
8:00 – 9:00	Завтрак	
9:00 – 09:30	Регистрация участников конференции	
9:30 – 11:00	**Пленарное заседание** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр.4*	
11:00 – 11:30	Кофе-брейк	
11:30 – 12:30	**Секция «Квалифицированная электронная подпись: организационные, технические и юридические вопросы»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 4*	**Секция «Криптография и криптоанализ»** *Конференц-зал «Марс» (Конференц-комплекс)*
12:30 – 13:30	**Круглый стол «Вопросы и ответы»** *Конференц-зал (Ресторанный комплекс)*	*Подробнее на стр. 5*
13:30 – 14:30	Обед	
14:30 – 16:30	**Секция «Российский и международный опыт построения систем обнаружения и предупреждения компьютерных атак. Путь от частных инициатив и бизнес проектов к построению глобальных систем»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 7*	**Секция «Криптография и криптоанализ»** *Продолжение работы секции*

16:30 – 17:00	Кофе-брейк	
17:00 – 19:00	**Секция «Анализ кода и технологии защиты: динамический и статический анализ, виртуализация кода, исследование на недекларированные возможности»** *Конференц-зал «Юпитер» (Конференц-комплекс)* *Подробнее на стр. 8*	**Секция «Криптография и криптоанализ»** *Продолжение работы секции*
19:30	Трансфер отель «Солнечный Park Hotel & SPA»– м. Речной вокзал. Подача автобуса в 19.15 у ворот отеля.	
20:00 – 23:00	Банкет в честь открытия конференции «РусКрипто'2013» *Конференц-зал (Ресторанный комплекс)*	

29 марта, пятница. Второй день работы конференции

7:30	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»	
8:00 – 8:20	Зарядка (*сбор у ресторанного комплекса*)	
8:00 – 10:00	Завтрак	
10:00 – 11:30	**Секция «Информационная безопасность финансово-кредитных организаций»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 10*	**Секция «Криптография и аппаратные платформы»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр. 11*
11:30 – 12:00	Кофе-брейк	
12:00 – 13:30	**Секция «Информационная безопасность финансово-кредитных организаций»** *Продолжение работы секции*	**Секция «PKI в России, в СНГ, в мире»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр. 12*
13:30 – 14:30	Обед	
14:30 – 16:10	**Секция «Криптография в проекте Универсальная Электронная Карта»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 13*	**Секция «Современные технологии на службе средств защиты и вредоносного программного обеспечения – «искусство войны» в сети Интернет»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр.14*

Тайм-лайн конференции

16:10 – 16:30	Кофе-брейк	
16:30 – 19:00	**Секция «Продукты и технологии информационной безопасности»** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 15*	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал «Марс» (Конференц-комплекс)* *Подробнее на стр. 16*
19:30	Трансфер отель «Солнечный Park Hotel & SPA»– м. Речной вокзал. Подача автобуса в 19.15 у ворот отеля.	
19:30 – 20:30	Ужин	
20:30 – 23:00	**Тематический вечер «Джентльменский клуб»** *Развлекательный комплекс*	

30 марта, суббота. День отъезда

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

Первый день работы конференции

9:30 – 11:00	**Пленарное заседание** *Конференц-зал (Ресторанный комплекс)*

Официальное открытие конференции

Приветственное слово
***Кузьмин Алексей Сергеевич**, сопредседатель программного комитета конференции, ФСБ России*

Дайджест новостей мировой и российской криптографии
***Жуков Алексей Евгеньевич**, сопредседатель программного комитета конференции, МГТУ им. Баумана*

Актуальные задачи защиты информации в компьютерных системах, обрабатывающих конфиденциальную информацию
***Баранов Александр Павлович**, ФГУП ГНИВЦ ФНС России, Высшая Школа Экономики*

11:30 – 12:30	**Секция «Квалифицированная электронная подпись: организационные, технические и юридические вопросы»** *Конференц-зал (Ресторанный комплекс)*

***Ведущий:** Загорский Игорь Иванович, заместитель директора Департамента развития электронного правительства, Минкомсвязь России*

Условия применения квалифицированной электронной подписи: технологические и организационные аспекты
***Маслов Юрий Геннадьевич**, коммерческий директор, КРИПТО-ПРО*
Условия признания действительной квалифицированной электронной подписи. Детализация условий использования средств электронной подписи для создания и проверки квалифицированной электронной подписи в системах документооборота, требования к содержанию квалифицированного сертификата ключа проверки электронной подписи и определению его статуса. Сценарии отказа подписанта от своей электронной подписи, считающейся в системе в качестве квалифицированной.

Расширенный справочник аккредитованных удостоверяющих центров
***Миклашевич Анатолий Вадимович**, исполнительный директор, РОСЭУ*
Аккредитованные в Минкомсвязи УЦ указаны в реестре, расположенном на сайте регулятора. Однако, для простого потребителя квалифицированной электронной подписи этот реестр мало что дает. Как же найти предложения по изготовлению квалифицированной электронной подписи на своей территории, как сравнить по критериям аккредитованные УЦ и в конце концов определиться - у кого приобрести квалифицированную электронную подпись?

Подводные камни аккредитации Удостоверяющего центра в Минкомсвязи
***Волков Алексей Николаевич**, эксперт в области ИБ, член RISSPA, АРСИБ, Датум*
Аккредитация удостоверяющего центра по требованиям 63-ФЗ в Минкомсвязи РФ необходима для признания сертификата ключа проверки электронной подписи, выдаваемого УЦ, квалифицированным, и является главным шагом в светлое будущее электронного юридически значимого документооборота безо всяких дополнительных условий и соглашений. Процедура, на первый взгляд, хорошо описана, проста и понятна - но, как показывает практика, далеко не все желающие проходят ее с первого (а то и со второго) раза. С какими трудностями может столкнуться заявитель, как их предвидеть и преодолеть. В докладе речь пойдет о светлом настоящем и туманном будущем аккредитованных УЦ в РФ.

Границы применимости организационных мер при эксплуатации СКЗИ или где начинается работа хакеров

***Смирнов Николай Валерьевич**, начальник отдела научных исследований и развития продуктов, Инфотекс*

Доклад является приглашением к диалогу на тему поиска точки целесообразности в части использования регламентов как компоненты средств криптографической защиты информации и средств электронной подписи, в частности. Где находится грань, за которой обеспечить доверие к квалифицированной ЭП и СКЗИ соблюдением регламента уже нельзя? С какого момента отказ от использования технических средств защиты становится уязвимостью? Где границы необходимого и достаточного, каков правильный путь производителей средств СКЗИ и ЭП?

11:30 – 19:00 Секция «Криптография и криптоанализ»

Конференц-зал «Марс» (Конференц-комплекс)

Ведущие:

- *Кузьмин Алексей Сергеевич, ФСБ России;*
- *Попов Владимир Олегович, Ассоциация «РусКрипто», КРИПТО-ПРО;*
- *Жуков Алексей Евгеньевич, Ассоциация «РусКрипто», МГТУ им. Баумана*

Принципы синтеза перспективного алгоритма блочного шифрования с длиной блока 128 бит

***Шишкин Василий Алексеевич**, к.ф.-м.н., ФСБ России*

Ряд соображений указывает на необходимость дополнения стандарта ГОСТ 28147-89 новым алгоритмом блочного шифрования. В докладе предполагается раскрыть краткое описание перспективного алгоритма блочного шифрования, синтезные решения, вопросы программной реализации.

О криптографических свойствах итеративных симметричных блочных шифров, построенных на основе обобщения раундовой функции Фейстеля

***Коренева Алиса Михайловна**, Ведущий специалист отдела ИБ, Pointlane*

Работа посвящена исследованию итеративных алгоритмов блочного шифрования – обобщений шифров Фейстеля, основанных на регистрах сдвига произвольной длины над множеством двоичных r-мерных векторов.

Biclique cryptanalysis: новый метод или вариации на тему полного перебора ключей?

***Рудской Владимир Игоревич**, ФСБ России*

После опубликования в 2011 году известной работы А. Богданова, Д. Ховратовича и К. Рехбергера по анализу алгоритма AES появились работы, в которых метод биклик применяется к различным блочным шифрам. При этом во всех работах оценки трудоемкости атак сопоставимы с трудоемкостью полного перебора. В докладе будет проведен анализ метода биклик и его сравнение с универсальными методами.

Изоморфизмы шифров как инструмент криптоанализа с приложениями к AES

***Ростовцев Александр Григорьевич**, Санкт-Петербургский государственный политехнический университет*

Предлагается метод виртуальных изоморфизмов шифров для усиления атак. Показано, что стойкость AES к дифференциальным/линейным атакам равна примерно квадратному корню из общепринятых оценок.

Системы разреженных булевых уравнений и алгебраические атаки

***Ростовцев Александр Григорьевич**, Мизюкин Алексей Вадимович, Санкт-Петербургский государственный политехнический университет*

Для ускорения алгебраических атак предлагается вместо булевых функций и подстановок рассматривать алгебро-геометричесие объекты: идеалы и многообразия. Идеал подстановки задается цепочкой вложенных идеалов, состоящих из 1, 2, 3, … слагаемых.

Об одном режиме шифрования с возможностью аутентификации

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

В предлагаемом докладе будет предложено криптографическое решение, которое позволит совместить в одном алгоритме как процесс зашифрования информации, так и процесс вычисления кода аутентификации. Будут рассмотрены вопросы стойкости решения, а также приведены результаты сравнительного анализа быстродействия.

О геометрических свойствах обобщенных алгоритмов шифрования Фейстеля

*Пудовкина Марина Александровна, ассоциация РусКрипто, **Токтарёв Александр**, Национальный исследовательский ядерный университет (МИФИ)*

Рассматриваются различные обобщения алгоритмов шифрования Фейстеля. Каждому обобщенному алгоритму шифрования Фейстеля ставится в соответствие ориентированный помеченный граф. Через характеристики этого графа приведены оценки наибольшего числа раундов, для которых существуют невозможные разности.

Шифрование, сохраняющее порядок

***Кренделев Сергей Федорович**, к. ф.-м. н., доцент, НГУ, лаборатории НГУ-Parallels*

С целью создания защищенной базы данных необходимо построить вариант шифрования, сохраняющего отношение порядка. В работе приводятся несколько методов шифрования, адаптированных под конкретные данные.

Детерминированные генераторы псевдослучайных чисел на основе блочных шифров и функций хэширования: принципы синтеза и методы анализа

***Маршалко Григорий Борисович**, ФСБ России*

На основе анализа научных публикаций, а также нормативных документов NIST, ISO и BSI формулируются общие принципы синтеза генераторов, основанных на блочных шифрах и функциях хэширования. Проводится обзор классических подходов к анализу генераторов подобных типов.

Один способ формирования случайной последовательности хорошего качества

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

В настоящей работе рассматриваются алгоритмы формирования последовательности случайных бит хорошего качества с использованием недетерминированного генератора случайных чисел. Предлагается использовать в качестве алгоритма блока преобразования исходной случайной последовательности линейные коды. Показано, что в данном случае можно улучшить характеристики получаемой последовательности случайных чисел.

О подходах к построению ДСЧ в программных СКЗИ

***Смышляев Станислав Витальевич**, к.ф.-м.н., ведущий инженер-аналитик, КРИПТО-ПРО*

Обзор существующих методов построения программно-аппаратных ДСЧ в среде, в которой отсутствуют соответствующие специализированные аппаратные средства. Предлагается подход, базирующийся на неустранимой нестабильности доступных с уровня пользователя источников времени вычислительной системы. Также в докладе рассматривается метод построения программных ПДСЧ на основе случайных автоматов.

Критерий Лемпеля-Зива - новая надежда

***Костевич Андрей Леонидович**, к.ф.-м.н., АВЕСТ, Шилкин Антон, НИИ ППМИ БГУ*

В последнее время для тестирования бинарных последовательностей в задачах криптографии предпринимаются попытки использовать статистические критерии, основанные на универсальных алгоритмах сжатия. Например, критерии Маурера и Лемпеля-Зива. Однако сложность записи алгоритмов сжатия приводит к проблемам с теоретическим обоснованием данных критериев. Поэтому критерий Лемпеля-Зива был исключен из последней редакции стандарта SP 800-22. В докладе предлагается подход к построению критериев на основе универсальных предикторов и приводятся теоретические результаты для критерия Лемпеля-Зива, обосновывающие его применение.

Неравномерные распределения ключей, схемы парольной защиты и цепи Маркова

***Чиликов Алексей Анатольевич**, к.ф.-м.н., ведущий инженер-аналитик, МГТУ им. Баумана*

Принято рассматривать ключи как элементы большого множества, выбираемые равновероятно. Однако это требование труднодостижимо на практике, а в ряде случаев не является однозначно необходимым для стойкости. Классическим примером использования неравновероятных ключей являются парольные схемы. Они хорошо изучены на практике, но теоретическая база в этой области не полна. Марковские цепи являются мощным инструментом для исследований таких схем. В докладе будет сформулировано несколько теоретических результатов в этой области.

Дешифрование шифра перестановки

***Бабаш Александр Владимирович**, д.ф.-м.н., профессор, МЭСИ*

В работе предложен метод дешифрования шифра перестановки, трудоемкость которого при небольших степенях используемых ключевых подстановок меньше трудоемкости тотального метода опробования.

О сложности двумерной задачи дискретного логарифмирования в группе точек эллиптической кривой с эффективным автоморфизмом порядка 6

***Николаев Максим Владимирович**, факультет ВМК, МГУ имени М.В. Ломоносова*

Двумерная задача дискретного логарифмирования является обобщением классической задачи дискретного логарифмирования и возникает, в частности, при использовании специальных алгоритмов вычисления кратной точки на эллиптических кривых с эффективными автоморфизмами. В 2010 году W. Liu получил оценки сложности ее решения для случаев автоморфизмов порядка 2 и 4. В настоящем докладе рассмотрен случай автоморфизма порядка 6.

Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида-Маллера

*Чижов Иван Владимирович, **Бородин Михаил Алексеевич**, факультет ВМК, МГУ имени М.В. Ломоносова*

Предлагается новый алгоритм восстановления секретного ключа по открытому для криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида-Маллера RM(r,m). В том случае, если НОД (r,m-1) ограничен, алгоритм имеет полиномиальную сложность. Практические результаты показывают, что предложенная атака позволяет осуществить взлом криптосистемы Мак-Элиса, построенной на коде длины 65526 битов, за 7 часов на персональном компьютере.

Алгоритмы развертывания ключа XSL-шифрсистем, стойкие относительно линейного метода анализа

***Хоруженко Георгий Игоревич**, аспирант кафедры «Криптологии и дискретной математики», НИЯУ МИФИ*

В работе предложен класс линейных алгоритмов развертывания ключа некоторых XSL-шифрсистем. Доказывается стойкость шифрсистем с данными алгоритмами развертывания ключа к анализу линейным методом.

12:30 – 13:30	**Круглый стол «Вопросы и ответы»** *Конференц-зал (Ресторанный комплекс)*

14:30 – 16:30	**Секция «Российский и международный опыт построения систем обнаружения и предупреждения компьютерных атак. Путь от частных инициатив и бизнес проектов к построению глобальных систем»** *Конференц-зал (Ресторанный комплекс)*

***Ведущий:** Лукацкий Алексей, эксперт по информационной безопасности, менеджер по развитию бизнеса Cisco*

Кибербезопасность стала очень горячей темой. Задачи ставятся уже на государственном уровне и к их решению привлекаются серьезные ресурсы. Строятся системы обнаружения, предупреждения и ликвидации компьютерных атак в масштабе государств, идет взаимодействие на межгосударственном уровне. Цель секции: собрать ведущих экспертов коммерческих, общественных организаций и обсудить, что и как нужно делать, чтобы создать реально работающую глобальную систему в обозримые сроки.

Участвуют эксперты:

- **Гордейчик Сергей Владимирович**, научный редактор SecurityLab.ru, технический директор, Positive Technologies
- **Лепихин Владимир Борисович**, начальник лаборатории сетевой безопасности, Информзащита
- **Медведовский Илья Давидович**, директор, Digital Security
- **Комаров Андрей Андреевич**, технический директор CERT-GIB, Group-IB
- **Демидов Олег Викторович**, координатор программы ПИР-Центра «Глобальное управление интернетом и международная информационная безопасность»

17:00 – 19:00	**Секция «Анализ кода и технологии защиты: динамический и статический анализ, виртуализация кода, исследование на недекларированные возможности»** *Конференц-зал «Юпитер» (Конференц-комплекс)*

Ведущие:

- *Проскурин Вадим Геннадьевич, к.т.н., доцент, заместитель председателя учебно-методического совета учебно-методического объединения вузов России по образованию в области информационной безопасности;*
- *Аветисян Арутюн Ишханович, доктор физико-математических наук, доцент, ученый секретарь, ИСП РАН*

Анализ качества ПО с точки зрения безопасности: международный опыт

Лукацкий Алексей*, эксперт по информационной безопасности*

В России сегодня начинается волна публикаций и выступлений на мероприятиях, посвященных анализу качества программного обеспечения с помощью различных механизмов - от пентестов до анализа исходных или бинарых кодов. При этом мы не совершаем революции, а следуем общемировой тенденции, так как специалисты давно поняли, что предотвращать уязвимости на этапе разработки ПО гораздо проще и выгоднее, чем бороться с дырами на этапе эксплуатации. Какова международная практика анализа качества ПО?

SAST/DAST/IAST: от теории к практике

Баранов Денис Сергеевич*, руководитель группы анализа защищенности приложений, Positive Technologies*

В настоящее время существует богатая теоретическая база по автоматизированному анализу приложений на предмет уязвимостей реализации. Однако при переходе от теории к практике неминуемо приходится сталкиваться с ограничениями и идти на компромиссы. Причем ограничения могут быть связаны как методами и подходами анализа, так и сугубо субъективными моментами, такими как целевая аудитория пользователей. В рамках доклада на основе опыта разработки средств статического, динамического и интерактивного анализа безопасности приложений будут рассмотрены возникающие сложности и возможные подходы к их решению.

Обнаружение уязвимостей логики приложений методом статического анализа: где правда, где реклама?

Петухов Андрей Александрович*, научный сотрудник лаборатории БИС ВМК МГУ имени М. В. Ломоносова, технический директор, SolidLab*

Недостатки, влияющие на качество (и безопасность) приложений, можно поделить на две группы: типичные недостатки (переполнения, уязвимости форматной строки, SQLi, XSS и т.п.) и специфичные недостатки (англ. application specific). В докладе будет проведена оценка справедливости высказываний вендоров статических анализаторов об их возможностях по поиску специфичных недостатков безопасности в приложениях. Будет представлена методика поиска подобных ошибок на примере поиска ошибок контроля доступа: задача будет декомпозирована на шаги, для каждого из которых будет указано, что можно сделать автоматически и как, а что - только вручную.

Проведение динамического анализа корректности взаимодействия прикладного ПО с СКЗИ

Сорокин Павел Федорович*, НПП «Гамма»*

В работе рассматривается динамический анализ взаимодействия прикладного ПО с СКЗИ, функционирующим под управлением ОС Windows и взаимодействующего с СКЗИ по интерфейсу CryptoAPI.

Об анализе трасс при тестировании программ методом фазинга

Макаров Алексей Николаевич*, УМО ИБ*

Рассматриваются вопросы, связанные с улучшением покрытия кода при тестировании методом фазинга. Предлагается генерировать входные данные на основе анализа трасс, полученных на предыдущих итерациях тестирования.

Перспективы применения детерминированного воспроизведения работы виртуальной машины при решении задач компьютерной безопасности

***Довгалюк Павел**, кафедра ИТиС, НовГУ им. Ярослава Мудрого*

Доклад посвящен применению метода детерминированного воспроизведения работы виртуальной машины для решения задач компьютерной безопасности. Реализованный в симуляторе QEMU метод позволяет использовать обратную и детерминированную отладку, а также логирование работы систем как с целью обнаружения уязвимостей, так и с целью расследования случаев эксплуатации уязвимостей.

Разработка обфусцирующего компилятора на базе LLVM

***Курмангалеев Шамиль Фаимович**, ИСП РАН*

Разработана методика запутывания программы во время компиляции, направленная на повышение сложности статического анализа программ. Рассматривается набор преобразований совмещающих в себе маскировку потока данных и потока управления запутываемой программы. Запутывание программы производится на уровне промежуточного представления компилятора, что позволяет проводить преобразования с учетом всей доступной компилятору информации о программе. Рассматривается программная среда, поддерживающая данную методику.

Обнаружение уязвимостей по безопасности на основе статического анализа исходного кода

***Журихин Дмитрий Михайлович, Несов Владимир Сергеевич**, ИСП РАН*

Статический анализ программ позволяет находить уязвимости и критические ошибки, трудно обнаруживаемые другими средствами. В докладе описывается метод масштабируемого межпроцедурного статического анализа потоков данных и основанная на нём расширяемая система автоматического поиска дефектов в реальных программах на языках Си/Си++.

Второй день работы конференции

10:00 – 13:30

Секция «Информационная безопасность финансово-кредитных организаций»

Конференц-зал (Ресторанный комплекс)

Ведущие:

- *Левиев Дмитрий Олегович, председатель Совета НП ПСИБ;*
- *Виноградов Александр Юрьевич, Начальник Управления ИБ, Златкомбанк*

Нормативное регулирование вопросов безопасности ДБО. Тенденции и перспективы

Царев Евгений Олегович, *Академия Информационных Систем*

Нормативное регулирование ДБО в России развивается де-факто с 2006 года, первые документы появились в форме писем Банка России и преследовали целью согласование использования систем ДБО с 115-ФЗ О противодействии отмыванию доходов полученных преступным путем. Со временем повсеместное использование систем ДБО способствовало созданию рынка мошенничества в системах ДБО, который в настоящий момент оценивается в 95млн.$ в год. С 2009 года, нормативные документы уже ориентировались на внешнего злоумышленника. К настоящему времени наработана обширная нормативная база, содержащая как рекомендации, так и требования к системам ДБО и организациям использующим их.

Вопросы лицензирования деятельности по работе с СКЗИ региональных представительств кредитно-финансовых организаций

Ермолаев Сергей Владимирович, *Транскапиталбанк*

Проблемы лицензирования региональных структурных подразделений Банков. Предложения по организации работы Органа криптографической защиты Банка по обеспечению клиентов ДБО в регионах средствами криптозащиты.

Моделирование возможностей нарушителей в среде функционирования средств электронной подписи

Левиев Дмитрий Олегович, *председатель Совета НП ПСИБ*

Рассматриваются результаты разрешения конфликта моделирования возможностей нарушителей по нормативным документам ФСТЭК России, ФСБ России и риск-ориентированного подхода оценки их возможностей. Показываются ставшие стандартными допущения для возможностей нарушителей и порядок предоставление доверия определенным категориям нарушителей в рамках построения систем защиты. Даются варианты взаимного использования результатов моделирования возможностей нарушителей при проектировании и эксплуатации систем в защищенном исполнении с использованием шифровальных (криптографических) средств.

Реализация доверенного отображения подписанного документа в системах ДБО

Смирнов Павел Владимирович, *к.т.н, заместитель начальника отдела разработок, КРИПТО-ПРО*

Отображение подписываемого документа «доверенным» образом применяется в системах ДБО для защиты от атаки подмены документа. В существующих решениях слабо развита поддержка распространённых форматов подписанных сообщений, используются несовместимые форматы разметки отображаемых данных. Предлагается общий способ отображения документа при подписании и при проверке, применимый к стандартным форматам подписанных сообщений CMS и XMLDSIG, независимый от используемого средства отображения.

Противодействие мошенничеству в сервисе online-платежей Яндекс.Деньги

Армарчук Анна Алексеевна, *аналитик Службы ИБ и противодействия мошенничеству, Яндекс.Деньги*

Будут рассмотрены основные виды мошенничества и соответствующие им функции безопасности, предлагаемые пользователям сервиса платежей. Также будет описан процесс управления безопасностью, охватывающий все этапы от обращения пользователя в службу поддержки до автоматического мониторинга активности пользователей в системе. Будет дан обзор сервиса изнутри, включая описание антифрод-системы собственной разработки и ряда отдельных мониторингов, оперативно внедряемых с разной степенью эффективности.

Открытая дискуссия «Как обосновать необходимость использования сертифицированных средств отечественной криптографии в банках владельцам бизнеса?»

Участвуют представители ФСБ, Банка России, разработчики СКЗИ, представители коммерческих банков.

10:00 – 11:30 **Секция «Криптография и аппаратные платформы»**
Конференц-зал «Марс» (Конференц-комплекс)

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

О создании эффективных программных реализаций отечественных криптографических стандартов

Казимиров Александр Владимирович*, Researcher, Selmer Center, University of Bergen*
Рассматриваются свойства ГОСТ 28147-89 и ГОСТ Р 34.11-2012 с точки зрения задачи построения эффективных реализаций. Исследование возможности построения эффективных реализаций ГОСТ 28147-89 на архитектурах с поддержкой расширений SSE4 и AVX. Определяются перспективные направления исследований свойств алгоритма ГОСТ Р 34.11-2012.

Особенности реализации новых российских криптографических стандартов на процессорах архитектуры ARM7

Тараскин Олег Геннадьевич*, Заместитель директора проекта Рутокен по науке, Актив*
ARM – одна самых успешных архитектур в микропроцессорной индустрии. Подавляющее число электронных устройств, выпускаемых в настоящий момент, содержит внутри себя микроконтроллер ARM. В докладе будут рассмотрены особенности реализации и оптимизации новых российских алгоритмов подписи и хеширования для микропроцессоров с ядром ARM7.

О возможности модификации алгоритма шифрования ГОСТ 28147-89 с сохранением приемлемых эксплуатационных характеристик

*Дмух Андрей Александрович****, Маршалко Григорий Борисович****, Дыгин Денис Михайлович ФСБ России*
В докладе представлена модификация развертки ключа в алгоритме шифрования ГОСТ 28147-89, которая исключает возможность применения атаки, предложенной в 2011 году японским специалистом Т. Исобе. Оценивается сложность реализации данной модификации на платформах с ограниченными ресурсами (lightweight-реализация).

Аппаратная реализация криптографических алгоритмов в защищенных микроконтроллерах Inside Secure

Платонов Владимир Владимирович*, к.т.н., профессор кафедры «Информационная безопасность компьютерных систем», СПбГПУ*
В докладе рассматривается аппаратная реализация различных криптографических алгоритмов в защищенных микроконтроллерах компании Inside Secure (в прошлом Atmel). Представлены возможности встроенного программного обеспечения для реализации функций аутентификации, шифрования, генерации ключей и одноразовых паролей, цифровой подписи и др.

Аппаратная реализация ГОСТ 28147-89 для прозрачного шифрования потоков данных

Шарамок Александр Владимирович*, к.т.н., начальник отдела разработки средств беспроводной связи, Анкад*
В докладе излагается эволюция подходов к аппаратной реализации алгоритмов шифрования, в частности алгоритма криптографического преобразования ГОСТ 28147-89. Рассматриваются преимущества и недостатки различных способов аппаратной и программной реализации алгоритмов шифрования. Дается оценка эффективности реализации алгоритма ГОСТ 28147-89 для различных применений.

12:00 – 13:30 **Секция «PKI в России, в СНГ, в мире»**

Конференц-зал «Марс» (Конференц-комплекс)

Ведущий: *Комисаренко Владимир Владимирович, начальник сектора Государственной системы управления открытыми ключами Республики Беларусь, Национальный центр электронных услуг*

Сравнительный анализ действующих в Российской Федерации и Республике Беларусь нормативных правовых требований в сфере технологии электронной цифровой подписи и инфраструктур открытых ключей

Комисаренко Владимир Владимирович, *начальник сектора Государственной системы управления открытыми ключами Республики Беларусь, Национальный центр электронных услуг*

В Российской Федерации и Республике Беларусь действуют различные нормативные правовые требования в сфере технологии электронной цифровой подписи и инфраструктур открытых ключей. В тоже время специалисты понимают, что используемые идеи и принципы одинаковы. И цель - обеспечение высокой степени безопасности применения криптографических технологий в сочетании с удобством и эффективностью практического применения – одна. В докладе приводятся результаты сравнительного анализа нормативных правовых требований, действующих в Российской Федерации и Республике Беларусь.

Технологическое, организационное и нормативное обеспечение трансграничного электронного юридически-значимого документооборота в процедурах электронной торговли

Кирюшкин Сергей Анатольевич, *к.т.н., советник генерального директора, Газинформсервис*

Обоснование наличия достаточных правовых условий для организации трансграничного защищенного электронного юридически-значимого документооборота при взаимодействии с использованием сервисов доверенной третьей стороны.

Усиленная квалифицированная подпись и аутентификация

Сабанов Алексей Геннадьевич, *к.т.н., зам.ген.директора, Аладдин Р.Д.*

Использование ЭП становится необходимым при возникновении правовых отношений между субъектами и выражается в подписывании электронного документа или сообщения в прикладных системах. Аутентификация неотъемлемо участвует в процессе создания ЭП перед подписанием документа. На докладе будет рассказано о роли аутентификации при придании электронному документу юридической силы, а также для обеспечения надежности идентификации личности, обладающей полномочиями подписи.

Вопросы развития ЭЦП в Украине

Потий Александр Владимирович*, д.т.н. проф. АО Институт информационных технологий, Харьковский университет Воздушных Сил*

В Украине активно создаются и развиваются инфраструктуры открытых ключей и ЭЦП. В докладе рассматриваются этапы развития и внедрения ЭЦП в различные информационные услуги государственных и коммерческих структур, вопросы правового, организационного и материально-технического обеспечения системы ЭЦП в Украине, отдельные технические решения украинских производителей в данной сфере. Раскрываются перспективы дальнейшего внедрения электронных услуг с ЭЦП в Украине.

14:30 – 16:10	**Секция «Криптография в проекте Универсальная Электронная Карта»** *Конференц-зал (Ресторанный комплекс)*

Ведущий: *Щепинов Вадим Александрович, вице-президент, УЭК*

О текущем состоянии проекта УЭК и базовых архитектурных концепциях безопасности

Глазков Борис Михайлович*, директор департамента технического развития и ИБ, УЭК*

Текущее состояние развития инфраструктуры Единой платежно-сервисной системы «Универсальная электронная карта», базовые технологии, обеспечивающие безопасность при выпуске и обслуживании универсальных электронных карт. Актуальные вопросы, связанные с развитием инфраструктурных компонентов системы.

Ключевые системы и криптографическая защита данных в системе Универсальной Электронной Карты

Попов Владимир Олегович*, к.ф.-м.н, директор по научной работе, КРИПТО-ПРО*

Описываются информационные потоки и ключевые потоки при производстве, персонализации и использовании УЭК; структурные элементы системы, определяющие обработку ключевых и информационных потоков. Обзор механизмов защиты ключей и информации, использования криптографических алгоритмов.

Карточная криптография в решениях – от поставщика карточных платформ

Мытник Константин Яковлевич*, начальник отдела смарт-карт, НИИМЭ и Микрон*

Доклад посвящен основным криптографическим механизмам, используемым в смарт-технологиях: генерация электронной подписи владельца карты, аутентификация сторон информационного обмена, реализуемая на основе PKI или симметричных криптографических алгоритмов, обеспечение аутентичности и конфиденциальности передаваемых сообщений.

Защита каналов связи между участниками единой платёжно-сервисной системы «Универсальная электронная карта»

Авраменко Юрий Вячеславович*, вице-президент, ИнфоТеКС*

О требованиях к защите каналов связи между различными категориями участников в единой платежно-сервисной системе УЭК и решениях для них. Также в докладе будет дана информация о текущем состоянии разработок, ведущихся компанией ИнфоТеКС в связи с проектом УЭК.

Предложения ОАО «УЭК» по стандартизации криптопротоколов в технологиях УЭК

Безнос Александр Владимирович*, начальник отдела микропроцессорных систем, УЭК*

Доклад посвящен применению в проекте УЭК международного стандарта Global Platform. Он регламентирует в технологиях смарт-карт обеспечение безопасной обработки и хранения данных. Будут рассмотрены предложения по применению в криптопротоколах этого стандарта (Secure Channel Protocol – 02) российских криптографических алгоритмов.

14:30 – 16:10	**Секция «Современные технологии на службе средств защиты и вредоносного программного обеспечения – «искусство войны» в сети Интернет»** *Конференц-зал «Марс» (Конференц-комплекс)*

Ведущие:

- *Зегжда Петр Дмитриевич, профессор, д.т.н., Заслуженный деятель науки РФ, Заведующий кафедрой «Информационная безопасность компьютерных систем» СПбГПУ;*
- *Баранов Александр Павлович, д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

Обеспечение безопасности виртуализированных систем

***Зегжда Петр Дмитриевич**, профессор, д.т.н., Заслуженный деятель науки РФ, зав. кафедрой «Информационная безопасность компьютерных систем», СПбГПУ*

В докладе будут проанализированы возможности виртуализации, как базы средств зашиты, разработана модель безопасности виртуализированных систем на примере облачных вычислений и предложены возможные подходы к обеспечению безопасности систем виртуализации.

Открытое программное обеспечение как основа информационной безопасности в сети Интернет

***Баранов Александр Павлович**, д.ф-м.н., Заместитель Генерального директора ФГУП ГНИВЦ ФНС России*

Программное обеспечение с открытым кодом составляет серьезную конкуренцию пропиетарному ПО с точки зрения богатства функциональных возможностей и стоимости эксплуатации. В докладе рассматриваются различные аспекты безопасности использования ПО с открытым кодом в Интернет-приложениях.

Суперкомпьютеры и безопасность – новые задачи и новые возможности

***Зегжда Дмитрий Петрович**, д.т.н., профессор, руководитель компании, НеоБИТ*

В настоящее время наша страна переживает очередной виток информатизации, который заключается в создании высокопроизводительных вычислительных центров и суперкомпьютеров. В докладе рассматриваются факторы, обуславливающие специфику безопасности суперкомпьютеров и развернутых на их базе сервисов, включая облачные, пути использования возможностей суперкомпьютеров для решения задач обеспечения безопасности, а также возможности использования суперкомпьютеров в кибервойнах.

Обеспечение устойчивости функционирования распределенных многоагентных систем в сети Интернет в условиях целенаправленного разрушающего воздействия

***Степанова Татьяна Владимировна**, к.т.н, доц. кафедры «Информационная безопасность компьютерных систем», СПбГПУ*

Одним из основных средств для организации атак на компьютерные системы в настоящее время являются бот-сети, объединяющие хосты в сети Интернет, находящиеся под управлением вредоносных программ и согласованно осуществляющие деструктивные действия. Такие свойства современных бот-сетей, как сложная организация, нетривиальные топологии и взаимодействие друг с другом, позволяют успешно реализовывать угрозы безопасности компьютерных систем. В докладе будет представлена модель противостояния бот-сетей, позволяющая формализовать методы обеспечения устойчивости их функционирования в сети Интернет.

Обеспечение безопасности АСУ ТП путем обнаружения и устранения уязвимостей

***Москвин Дмитрий Андреевич**, к.т.н., доц., руководитель проектов, НеоБИТ*

Имеющийся опыт тестирования безопасности АСУ ТП показывает, что они содержат большое количество различных уязвимостей, которые могут быть в прошивках контроллеров, в SCADA-системах, в системном и прикладном ПО. Рассматриваются различные последствия успешных эксплуатаций таких уязвимостей, начиная от отказа систем мониторинга и управления и заканчивая нарушениями технологического процесса с выходом из строя оборудования и социально-экономическими последствиями.

Фаззинг сетевых протоколов с использованием генетических алгоритмов

***Печенкин Александр Игоревич**, аспирант, ст. преп. кафедры «Информационная безопасность компьютерных систем», СПбГПУ*

В докладе рассматривается разработанный и реализованный авторами метод повышения эффективности фаззинга на основе применения генетического алгоритма для выбора тестовых данных с предложенными целевыми функциями и критериями отбора.

Уязвимости гипервизоров и систем облачных вычислений

***Никольский Алексей Валерьевич**, аспирант, ст. преп. кафедры «Информационная безопасность компьютерных систем», СПбГПУ*

В докладе подробно описывается несколько известных уязвимостей гипервизоров, которые, по мнению авторов, наиболее ярко демонстрируют новые угрозы безопасности, появляющиеся в облаках.

16:30 – 19:00 Секция «Продукты и технологии информационной безопасности»

Конференц-зал (Ресторанный комплекс)

***Ведущий:** Рябко Сергей Дмитриевич, к.ф.-м.н., президент группы компаний «С-Терра»*

Как защитить информацию на iOS-устройствах при помощи российских СКЗИ?

***Гильберг Константин Валерьевич,** руководитель направления мобильной безопасности, Digital Design*

В ходе доклада будет рассмотрена уникальная линейка программных продуктов, разработанных компанией DIGITAL DESIGN. Продукты рассчитаны на пользователей государственных и коммерческих организаций, использующих в работе мобильные устройства iPad и iPhone. Для защиты информации, передаваемой по сети и хранимой в памяти iOS-устройства, применяются криптографические алгоритмы, отвечающие российским стандартам.

Доверенный сеанс: позиционирование технологии

***Рябко Сергей Дмитриевич,** генеральный директор, С-Терра СиЭсПи*

Технологии построения доверенного сеанса сегодня в фокусе внимания многих производителей. Предмет доклада – состав требований, масштабируемость для систем массового обслуживания, вопросы интеграции и типизации решений, простоты и удобства пользования, особенности «вертикальных» сценариев доверенного сеанса для различных сегментов рынка.

Вопросы оценки стойкости нейросетевой системы биометрической аутентификации

***Маршалко Григорий Борисович,** ФСБ России*

Рассматриваются требования стандарта ГОСТ Р 52633 к процедуре обучения нейронных сетей биометрической системы аутентификации и общие требования к обеспечению безопасности систем такого рода. Показано, что компрометация параметров нейронной сети приводит к фатальным для безопасности системы последствиям.

Обнаружение нарушений политик безопасности при работе в сетях WiFi для помещений с ограниченным доступом

***Старичков Владимир Викторович,** с.н.с., УМО ИБ*

Доклад посвящен вопросам обеспечения информационной безопасности при работе абонентов корпоративных сетей WiFi в помещениях с ограниченным доступом. Рассматриваются типовые нарушения политик безопасности и анализируются возможности выявления нарушений с применением специализированных технических средств.

Практика проведения инструментального анализа ИБ ИС

***Качалин Алексей Игоревич,** Зам. генерального директора, Перспективный мониторинг*

Инструментальный анализ ИБ – процесс технологически сложный и творческий, зависящий от многих «переменных» - квалификации исследователей, применяемых инструментов, внешних факторах - публикации информации о выявленных уязвимостях в ПО. Но определяющий фактор удовлетворенности заказчика от проведенных работ - аналитическая работа на предварительных этапах, в ходе выполнения и подготовки отчетных материалов. Подходы к декомпозиции задач, выявлению и обработке рисков проведения инструментального анализа, методики, использование которых, позволяет повысить взаимопонимание исследователей и заказчика.

Высокоскоростное шифрование данных и удаленный доступ для ЦОДов и отказоустойчивых систем. Реальность и мифы

***Карагедян Карен Ашотович**, Директор по продажам Stonesoft в России, СНГ и странах Балтии, Stonesoft Russia*
В докладе рассматриваются проблемы организации высокоскоростных защищенных каналов связи, а также высоконагруженных систем. Освещаются традиционные подходы и способы организации взаимодействия на уровне подсистем. Обсуждаются возможности оптимизации инфраструктуры и архитектуры средств защиты с целью повышения производительности.

Участие пользователей - анализ реализаций атак через интернет

***Кропотов Владимир, Четвертаков Виталий, Ярочкин Федор,** независимые исследователи информационной безопасности*
Будет показано как похождение пользователей по интернет, открытие файлов и писем из недоверенных источников ставят по угрозу сети, из которых пользователь получает доступ в интернет.

Эволюция SIEM: маркетинг или вынужденные меры

***Шелестова Олеся Александровна**, системный аналитик, исследовательский центр Positive Technologies*
Необходимо уметь вовремя обнаруживать и предотвращать угрозы. Для сбора событий используются SIEM-системы, ошибочно называемые лог-менеджментом. Докладчик расскажет о месте лог-менеджмента в пирамиде процессов SIEM, об эволюции SIEM, о решаемых задачах и проблемах при внедрении, о возможностях — с учетом потребностей бизнеса.

16:30 – 19:00 Секция «Перспективные исследования в области кибербезопасности»

Конференц-зал «Марс» (Конференц-комплекс)

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

Обеспечение сетевой безопасности с помощью программно-конфигурируемых сетей

***Смелянский Руслан Леонидович**, чл.-корр. РАН, профессор, директор по науке «Центра прикладных исследований компьютерных сетей» МГУ им. М.В.Ломоносова*
***Гамаюнов Денис Юрьевич**, к.ф.-м.н., с.н.с., и.о. зав.лабораторией безопасности информационных систем факультета ВМК МГУ им. М.В.Ломоносова*
Рассматривается задача разграничения доступа на основе информации об ожидаемом поведении (потоках) между приложениями в сети и анализируется концепция программно-конфигурируемых сетей.

Моделирование атак, анализ защищенности и визуализация в SIEM-системах

***Котенко Игорь Витальевич**, д.т.н., профессор, зав.лабораторией проблем компьютерной безопасности, СПИИРАН*
Представляется проблема аналитического моделирования атак и механизмов защиты на основе графов атак, анализа защищенности и визуализации событий и показателей защищенности в SIEM-системах. Представляется архитектура и аспекты реализации программных компонентов SIEM-системы, разрабатываемой в рамках проекта MASSIF Европейской рамочной программы FP7 Европейского Союза.

Адаптация мандатной сущностно-ролевой ДП-модели к условиям функционирования ОС семейства LINUX

***Девянин Петр Николаевич**, д.т.н., доцент, УМО ИБ*
Для строгого формального обоснования безопасности механизма логического управления доступом в отечественной защищенной операционной системе Astra Linux Special Edition и его теоретического моделирования на основе семейства ДП-моделей предлагается мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в ОС семейства Linux.

Построение графов атак для корреляции событий безопасности

***Чечулин Андрей Алексеевич**, лаборатория проблем компьютерной безопасности, СПИИРАН*

Представляется подход, с помощью которого на основе данных о топологии сети и свойствах отдельных хостов строятся графы атак, а на основе отчетов от системы обнаружения атак и анализа заранее созданных графов атак для различных потенциальных нарушителей становится возможным определить будущие действия нарушителя. Также с помощью данного подхода появляется возможность проводить ретроспективный анализ событий в сети, что позволяет выявить некоторые неизвестные ранее уязвимости (0-day).

Анализ и фильтрация сетевого трафика в высокоскоростных каналах передачи данных с использованием ПЛИС

***Беззубцев С.О.**, Лаборатория безопасности информационных систем факультета ВМК МГУ им. М.В.Ломоносова*

***Гамаюнов Денис Юрьевич**, к.ф.-м.н., с.н.с., и.о. зав.лабораторией безопасности информационных систем факультета ВМК МГУ им. М.В.Ломоносова*

***Самойлов Максим Николаевич**, Лаборатория безопасности информационных систем факультета ВМК МГУ им. М.В.Ломоносова*

Рассматривается проблема анализа и фильтрации сетевого трафика для каналов с пропускной способностью 10Гбит/сек и выше для задач обеспечения информационной безопасности. Рассматривается задача разработки специализированных микропрограмм для программно-реконфигурируемых вычислителей семейства ПЛИС. Предложен проблемно-ориентированный язык программирования, позволяющий описывать типовые задачи анализа и фильтрации трафика в виде функциональных блоков ПЛИС, и последующей композиции алгоритмов из этих блоков. Прототип системы фильтрации вредоносного исполнимого кода на основе алгоритма Racewalk разработан и реализован на семействе ПЛИС Virtex 6. Проведённые эксперименты показали достижимость основных желаемых показателей – точность, пропускная способность, отсутствие потерь трафика.

Проектирование защищенных информационных систем со встроенными устройствами

***Десницкий Василий Алексеевич**, лаборатория проблем компьютерной безопасности, СПИИРАН*

Представляются решения по разработке методологии проектирования защищенных информационных систем со встроенными устройствами, предложенные в рамках проекта SecFutur Европейской рамочной программы FP7 Европейского Союза. Методология основывается на определении ролей, вовлеченных в процесс, их ответственностей, задании последовательностей выполняемых действий, а также применения специализированных методик и инструментов проектирования, анализа и тестирования информационных систем, отдельных устройств и компонентов на различных стадиях процесса разработки.

Категорирование Web-сайтов для систем блокирования Web-страниц с неприемлемым содержимым

***Комашинский Д.В.**, F-Secure, Финляндия*

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

Рассматривается задача разработки автоматической системы блокирования Web-страниц с неприемлемым содержимым на основе анализа текста, html-тегов и изображений с помощью методов Data Mining. Представляются механизмы анализа сайтов, содержащих информацию на различных языках. Представляется архитектура и алгоритмы работы системы сбора, хранения и анализа данных, необходимых для классификации сайтов. Характеризуются проведенные эксперименты по анализу принадлежности набора сайтов к той или иной категории.

Компания «КРИПТО-ПРО»

С момента создания (2000 г.) компания КРИПТО-ПРО занимает лидирующее положение в области разработки средств криптографической защиты информации (СКЗИ) и развития Инфраструктуры Открытых Ключей (PKI) на территории РФ. Компания внесла существенный вклад в адаптацию международных рекомендаций применительно к российским криптографическим алгоритмам.

Специалистами КРИПТО-ПРО созданы:

- первое в России сертифицированное СКЗИ, интегрированное с операционной системой 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.

Продукты компании КРИПТО-ПРО широко используются в органах власти федерального и регионального уровней, в коммерческих организациях крупного, среднего и малого бизнеса. Это системы электронного документооборота, исполнения госзаказа, сдачи бухгалтерской и налоговой отчетности и т.п. Внедрение программных продуктов специалисты КРИПТО-ПРО сопровождают полным спектром консалтинговых услуг по применению электронно-цифровой подписи и шифрования. Компания ведет непрерывную разработку в целях улучшения имеющихся программных продуктов и создания нового ПО, призванного оперативно решать новые задачи, возникающие в сфере защиты информации. Решения КРИПТО-ПРО активно используются ведущими российскими и западными разработчиками IT-систем.

Контактная информация:
http://www.cryptopro.ru/
info@cryptopro.ru
+7 (495) 780-4820

Компания «Актив»

Компания «Актив» является ведущим российским разработчиком в сфере защиты информации и ведет свою деятельность с 1994 года. Компания 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 подписи (ЭП). USB-токены Рутокен являются ключевыми носителями в массовых российских проектах, базирующихся на технологии ЭП и инфраструктуре открытых ключей (PKI). Рутокен используется как самостоятельный продукт, так и в качестве одного из компонентов комплексных решений в области информационной безопасности. Основные сферы применения: системы дистанционного банковского обслуживания, электронные торги, информационные системы органов государственной власти, электронный документооборот B2B, B2C, G2B и внутрикорпоративный документооборот.

Продукция Рутокен имеет сертификаты ФСБ и ФСТЭК, подтверждающие соответствие требованиям к СКЗИ класса КС2 для защиты информации, не содержащей сведений, составляющих гос. тайну, и соответствие требованиям к техническим средствам защиты информации класса НДВ3, которые позволяют использовать идентификаторы Рутокен в системах, обрабатывающих конфиденциальную информацию, а также при работе с информацией, имеющей гриф «С».

Контактная информация:
http://aktiv-company.ru/
info@aktiv-company.ru
+7 (495) 925-7790

Компания «ИнфоТеКС»

ОАО «ИнфоТеКС» (Информационные Технологии и Коммуникационные Системы) — одна из ведущих High Tech компаний России, является лидером отечественного рынка программных VPN-решений и средств защиты информации в TCP/IP сетях, на рабочих станциях, серверах и мобильных компьютерах. ОАО «ИнфоТеКС» выполняет функции официальной секретарской компании Технического комитета по стандартизации №26 «Криптографическая защита информации».

Компания осуществляет полный цикл разработки и технической поддержки целого спектра средств защиты информации ViPNet, рассчитанных на обработку информации ограниченного доступа, включая персональные данные:

- программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI);
- средства межсетевого экранирования и персональные сетевые экраны;
- средства шифрования данных, хранимых и обрабатываемых на компьютерах и в сети;
- системы централизованного управления и мониторинга СЗИ;
- средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы юридически значимого документооборота, порталы и т.п.)

Компания совместно со своими 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.

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

Компания «Аладдин Р.Д.»

«Аладдин Р.Д.» - ведущий российский разработчик и поставщик продуктов и решений для обеспечения информационной безопасности. Компания специализируется на комплексном подходе к решению задач аутентификации и защиты персональных данных.

В последние годы компания «Аладдин Р.Д.» активно развивает свой бизнес в направлении разработки решений и оказании услуг для крупных корпоративных клиентов и государственного сектора. Это позволило ей войти в ТОП-3 крупнейших компаний России в сфере разработки аппаратного обеспечения для информационной безопасности по итогам рейтинга IDC, а также ТОП-100 крупнейших ИТ-компаний (рейтинг CNews2011) и ТОП-50 крупнейших ИТ-разработчиков (рейтинг CNews 2011). Продукты компании и комплексные решения на их основе востребованы в различных секторах отечественной экономики, в том числе в банковском, государственно-административном, а также в ТЭК и ряде других. Компания «Аладдин Р.Д.» прошла сертификацию менеджмента качества на соответствие российским стандартам ГОСТ Р ИСО 9001-2008. Лидерские позиции «Аладдин Р.Д.» подкреплены 18-летним опытом работы на российском рынке информационной безопасности, а также прочными партнерскими отношениями с ведущими российскими разработчиками систем криптографической защиты информации (СКЗИ), системными интеграторами и мировыми ИТ-вендорами: Microsoft, Oracle, и др.

Контактная информация:
http://www.aladdin-rd.ru
aladdin@aladdin-rd.ru
+7 (495) 223-0001

Компания «С-Терра СиЭсПи»

ЗАО «С-Терра СиЭсПи» основана в 2003 году и является одним из ведущих российских разработчиков и производителей средств сетевой информационной безопасности для построения виртуальных частных сетей (VPN). Продукты S-terra сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3.

Компания является первым в России технологическим партнером Cisco (Cisco Solution Technology Integrator), а также соорганизатором доверенного производства продукции компании Cisco в России. В 2011 году С-Терра первой в России и Восточной Европе стала продавать свои продукты компании Cisco как ПО от оригинального производителя Cisco (Cisco's supplier of choice for the locally certified network security software within Russia).

С-Терра предлагает российским заказчикам технически совершенные, органически входящие в сетевую инфраструктуру решения, которые используют протокол IPSec и российские криптографические алгоритмы, сертифицированные по ГОСТ, и характеризуются высокой масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения S-terra обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также с использованием технологии построения доверенного сеанса. Система централизованного управления, сертифицированная ФСБ России в составе линейки продуктов, позволяет удобно и эффективно управлять VPN-продуктами S-terra.
Решения компании предназначены для организаций, нуждающихся в надежной защите VPN-соединений с применением российской криптографии, например, для защиты конфиденциальной информации и персональных данных. Нам доверяют защиту своей информации такие компании федерального значения, как СО ЕЭС, Норильский никель, МЧС, Почта России и другие.

Контактная информация:
http://www.s-terra.com/
information@s-terra.com
+7 (499) 940-9061

Компания Check Point

Компания Check Point Software Technologies Ltd. — мировой лидер в области обеспечения интернет-безопасности, единственный поставщик средств обеспечения полной безопасности Total Security для сетей, данных и конечных узлов, объединенных единой средой управления. Компания Check Point предлагает клиентам высочайший уровень защиты от всех типов угроз, ее решения позволяют упростить управление безопасностью, а также снизить совокупную стоимость владения. Check Point разработала первое в отрасли решение Fire Wall-1 и реализованную в нем запатентованную технологию поиска угроз. Сегодня Check Point продолжает инновации, развивая Software Blade, динамическая архитектура которого позволяет создавать безопасные, гибкие и простые решения, способные полностью адаптироваться к требованиям безопасности любой организации или сетевой среды. Клиентами Check Point стали десятки тысяч предприятий и организация всех масштабов, в том числе все компании, входящие в список Fortune-100. Отмеченные наградами решения Check Point Zone Alarm защищают миллионы клиентов от хакеров, шпионских программ и незаконного доступа к конфиденциальным данным.

Контактная информация:
http://rus.checkpoint.com/
+7 (495) 967- 7444

Digital Design

Digital Design (1992-2013) - ведущий российский разработчик ПО и IT-интегратор. Компания создает тиражируемые программные решения для корпоративного рынка мобильных устройств. Отличительной чертой решений Digital Design является их строгое соответствие требованиям к защите информации, предъявляемых со стороны компаний и российских регуляторов. Основу компетенции составляют: детальное знание мобильных платформ, применение отечественных средств криптографической защиты информации, опыт реализации программных средств защиты информации. Продукты компании: Защищенная почта для iPad и iPhone, ГОСТ SSL VPN для iPad и iPhone, Планшет руководителя для iPad. Клиенты компании: ОАО "Российские железные дороги", ОАО "Сбербанк России", Министерство промышленности и торговли РФ и др. www.digdes.ru

Контактная информация:
http://www.digdes.ru
info@digdes.com
+7 (499) 788-74-94

Перспективный мониторинг

ЗАО «Перспективный мониторинг» - российская компания, оказывающая услуги в области информационной безопасности. ЗАО «Перспективный мониторинг» специализируется на проведении работ по исследованию состояния безопасности информационной системы организации, выявлению недокументированных и уязвимых сервисов. Компания оказывает экспертную поддержку при разработке политик, требований и инструкций по обеспечению ИБ, актуализации существующих регламентов под изменяющиеся требования бизнеса.

Среди сотрудников компании – как молодые специалисты, выпускники ведущих ВУЗов, обладающие актуальными знаниями, так и опытные профессионалы, успешно выполнившие проекты по разработке средств обеспечения ИБ, внедрению средств и систем защиты информации, работы по анализу защищенности информационных систем. В своей деятельности компания «Перспективный мониторинг» использует признанные мировые технологии и средства инструментального анализа ИБ, а также проводит собственные разработки в области сбора и анализа данных в информационных системах.

Сотрудники компании регулярно участвуют в профильных российских и международных конференциях и форумах по информационной безопасности, аудиту и анализу защищенности информационных систем, криптографии, СОРМ.

Контактная информация:
http://advancedmonitoring.ru/
+7 (495) 737-61-97

Компания ООО «НеоБИТ»

Компания «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:
http:// www.neo-bit.ru
info@neo-bit.ru
+7 (812) 535-28-06

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 250 специалистов. География участников из года в год расширяется, охватывая как новые города России, так и страны СНГ и дальнего зарубежья.

Контактная информация:
http://www.ruscrypto.ru/
info@ruscrypto.ru

Академия Информационных Систем (АИС)

АИС – профессиональный учебный центр подготовки и переподготовки специалистов и руководителей в области информационных технологий, информационной безопасности, управления, международных систем менеджмента. Обучение проводится на основании государственных лицензий и аккредитаций, по окончании обучения слушателям выдаются государственные удостоверения и/или сертификаты вендоров.

- Очное обучение, повышение квалификации и профессиональная переподготовка
  - Авторизованное обучение и авторские курсы, Microsoft, Cisco Systems, Oracle, Check Point, TrendMicro, RIT Technologies, Watch Guard, ViPNet, Крипто Про, Mandriva, AltLinux, StoneGate, Redhat, McAfee и др.
  - Авторские курсы направлений: Linux/Unix, HUAWEI, Alcatel, Samsung & LG, AVAYA DEFINITY, Asterisk, IP-телефония и корпоративные сети, СКС
  - Системы виртуализации VMware, Xen
  - Обеспечение информационной безопасности (свыше 50 курсов), включая программы, согласованные с ФСТЭК России, ФСБ России, Банком России
  - Обучение по программам согласованным с профильными ассоциациями и партнерствами, такими как НП АБИСС, НАУФОР
  - Международные системы менеджмента ISO 9001, ISO 27001, BS 25999, ISO 20000, ISO 14001, PAS99 и др.
  - Конкурентная разведка
- Дистанционное интерактивное обучение в области информационных технологий, информационной безопасности и менеджмента.
- Организация и проведение деловых мероприятий.

Контактная информация:
http://infosystems.ru/
info@infosystem.ru
+7(495) 231-30-49

Памятка участникам конференции

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 8:00 до 23:00. Время завтраков, обедов и ужинов для участников «РусКрипто'2013» указано в программе.

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

- 28 марта в 7.30 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 28 марта в 19.30 вечера трансфер отель «Солнечный Park Hotel & SPA» – м. Речной вокзал.
- 29 марта в 7.30 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 29 марта в 19.30 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»:

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

Внимание! Автобусы с табличкой «РусКрипто'2013» отправятся ровно в 12:00, просьба заранее сдать номера и не опаздывать.

Отель «Солнечный Park Hotel & SPA»:

Солнечногорский район, Ленинградское шоссе, 74 км

Телефон/факс: +7 (925) 922-42-00, +7 (499) 755-88-88

Расчетный час:

Заезд – 27 марта в 18:00, выезд – 30 марта в 12:00.