Таймлайн конференции

25 марта, вторник. 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	Вечер в развлекательном комплексе

26 марта, среда. Первый день работы конференции

8:00	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»	
8:00 – 9:00	Завтрак	
9:00 - 10:00	Регистрация участников конференции	
10:00 - 12:00	Официальное открытие конференции. **Пленарное заседание** *Конференц-зал (Ресторанный комплекс)* *Подробнее на стр. 7*	
12:00 -12:30	Кофе-брейк	
12:30 – 14:00	**Секция** **«СКЗИ. Новое в требованиях, концепции, использования, сертификации»** *Большой конференц-зал* *Ведущий:* ***Кузьмин А.С.,*** *ФСБ России* *Подробнее на стр. 7*	**Секция** **«Электронная подпись, практика применения»** *Конференц-зал «Марс»* *Ведущий:* ***Маслов Ю. Г.,*** *коммерческий директор, «КРИПТО-ПРО»* *Подробнее на стр. 8*
14:00 -15:00	Обед	
15:00 - 16:30	**Круглый стол** **«Подлинная безопасность, разговор на троих»** *Большой конференц-зал* Эксперты: • ***Качалин А.И,*** *заместитель генерального директора, «Перспективный мониторинг»*	**Секция** **«Криптография и криптоанализ»** *Конференц-зал «Марс»* Ведущие: • ***Кузьмин А.С.,*** *ФСБ России* • ***Попов В.О.,*** *Ассоциация «РусКрипто», «КРИПТО-ПРО»* *Подробнее на стр. 9*

	• ***Гордейчик С.В.,*** *технический директор, Positive Technologies* • ***Купреев О.В.,*** *ведущий исследователь, Digital Security* *Подробнее на стр. 12*	
16:30 -17:00	Кофе-брейк	
17:00 - 19:00	**Секция «Технологии создания безопасного программного обеспечения»** *Большой конференц-зал* Ведущие: • ***Проскурин В.Г.,*** *к.т.н., доцент, заместитель председателя учебно-методического совета учебно-методического объединения вузов России по образованию в области ИБ* • ***Аветисян А.И.,*** *д.ф.-м.н., доцент, ученый секретарь, ИСП РАН* *Подробнее на стр. 12*	**Секция «Криптография и криптоанализ»** *Конференц-зал «Марс»* Продолжение работы секции *Подробнее на стр. 9*
19:30 - 20:30	Ужин	
21.00 - 23.00	Фуршет в честь открытия конференции «РусКрипто’2014» *Конференц-зал (Ресторанный комплекс)*	

27 марта, четверг. Второй день работы конференции

8:00	Трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA»	
8:00 – 10:00	Завтрак	
10:00 - 11:30	**Секция «Криптография для мобильных платформ»** *Большой конференц-зал* Ведущие: • ***Федорушкин И.В.,*** *Samsung Electronics* • ***Калайда И.А.,*** *НИИ СОКБ* *Подробнее на стр. 14*	**Секция «Безопасность интернета вещей»** *Конференц-зал «Марс»* Ведущий: ***Гордейчик С.В.,*** *научный редактор SecurityLab.ru, технический директор Positive Technologies* *Подробнее на стр. 15*
11:30 – 12:00	Кофе-брейк	
12:00 -13:30	**Секция «Криптография для мобильных платформ»** *Большой конференц-зал* Продолжение работы секции *Подробнее на стр. 14*	**Секция «Продукты и технологии информационной безопасности»** *Конференц-зал «Марс»* Ведущий: ***Антимонов С.Г.,*** *председатель совета директоров, ЗАО "ДиалогНаука"* *Подробнее на стр. 16*
13:30 – 14:30	Обед	
14:30 - 16:00	**Секция «Использование инфраструктуры УЦ для решения задач идентификации и аутентификации»** *Большой конференц-зал* Ведущий: ***Комисаренко В.В.,*** *директор по развитию ЗАО «БЕЛТИМ СБ», директор ассоциации «РусКрипто»* *Подробнее на стр. 17*	**Секция «Безопасность современных информационных технологий — новые возможности и новые угрозы»** *Конференц-зал «Марс»* Ведущие: • ***Зегжда П.Д.,*** *д.т.н., профессор, Заслуженный деятель науки РФ, Заведующий кафедрой «Информационная безопасность компьютерных систем», СПбГПУ* • ***Баранов А.П.,*** *д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России* *Подробнее на стр. 18*

16:00 - 16:30	Кофе-брейк	
16:30 – 19:00	**Секция «Криптография и криптоанализ»** *Большой конференц-зал* Продолжение работы секции *Подробнее на стр. 10*	**Секция «Перспективные исследования в области кибербезопасности»** *Конференц-зал «Марс»* Ведущий: ***Котенко И.В.,*** *д.т.н., профессор, заведующий научно-исследовательской лабораторией проблем компьютерной безопасности, СПИИРАН* *Подробнее на стр. 18*
19:30 – 20:30	Ужин	
21:00 – 23:00	Вечерний коктейль и торжественное закрытие конференции *Конференц-зал (Ресторанный комплекс)*	

28 марта, пятница. День отъезда

9:00 – 11:00	Завтрак
11:45	Трансфер отель «Солнечный Park Hotel & SPA» – м. Речной вокзал

Первый день работы конференции

10:00 – 12:00	**Пленарное заседание** *Конференц-зал (Ресторанный комплекс)*

Официальное открытие конференции

Развитие требований к российским средствам криптографической защиты информации
Кузьмин Алексей Сергеевич, *ФСБ России*
Перспективы внедрения новых российских криптографических стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 и новая редакция требований ФСБ России к средствам криптографической защиты информации.

Перспективные направления исследований в защите информации
Баранов Александр Павлович*, д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

Приветственное слово
Eric Filiol, *Director of the Operational Cryptology and Virology Lab at ESIEA, Laval, France*

Приветственные слова от спонсоров и партнеров конференции

12:30 – 14:00	**Секция «СКЗИ. Новое в требованиях, концепции использования, сертификации»** *Конференц-зал (Ресторанный комплекс)*

Ведущий: ***Кузьмин Алексей Сергеевич ,*** *доктор физ.мат. наук, академик Академии криптографии, первый заместитель начальника ЦЗИСС ФСБ России, председатель ТК26*

В последнее время Центром защиты информации и специальной связи ФСБ России проводится активная работа по пересмотру понятия СКЗИ, требований к СКЗИ, определений сертифицированных СКЗИ. Этот процесс также связан с деятельностью ЦЗИСС и ТК26 по разработке и внедрению новых стандартов криптографической защиты данных, методических рекомендаций по криптографическим протоколам, форматам хранения ключей, интерфейсам СКЗИ. Целью работы секции является обмен мнениями заинтересованных специалистов в области развития понятий и требований, связанных с разработкой исследованиями и сертификацией СКЗИ.

Развитие требований к СКЗИ
Кузьмин Алексей Сергеевич, *ФСБ России*

Концепция СКЗИ информационных технологий
Попов Владимир Олегович, *Ассоциация «РусКрипто», КРИПТО-ПРО*

Направления развития требований к СКЗИ
Простов Владимир Михайлович, *ФСБ России*

Вопросы организации экспертизы предложений участников рынка в ТК26
Сериков Игорь Анатольевич, *ОАО «ИнфоТеКС», ТК*

12:30 – 14:00	**Секция «Электронная подпись, практика применения»** *Конференц-зал «Марс» (Конференц-комплекс)*

Ведущий: ***Маслов Юрий Геннадьевич****, коммерческий директор, «КРИПТО-ПРО»*

Состояние и развитие законодательства в области использования электронной подписи

Кузнецов Александр Юрьевич*,* ***Данилова Кристина Владимировна,*** *Минкомсвязь России*

В докладе будут отражены вопросы текущего применения законодательства и нормативно-правовой базы в области электронной подписи и направления её совершенствования и развития.

Ниши применения для различных видов электронной подписи

Храмцовская Наталья Александровна*, ведущий эксперт по управлению документацией компании ЭОС*

В докладе будет рассказано о законодательно-нормативных требованиях использования электронных подписей, о сложившейся практике их применения в сопоставлении с зарубежным опытом. Автор ставит своей целью показать, что у каждого из видов электронной подписи есть собственная ниша, где его применение удобно и экономически оправдано. В докладе отмечается, что использование усиленных электронных подписей в настоящее время создает проблемы в случае необходимости длительного хранения таких документов. Уже сейчас отечественное законодательство допускает определенную гибкость, особенно в условиях корпоративной среды.

Удостоверяющие центры: пределы доверия. Практика авторизации удостоверяющих центров при федеральных операторах электронных торговых площадок и АЭТП

Панов Валентин Николаевич*, зам. ген. директора ЗАО «Аналитический Центр», руководитель Комиссии по авторизации УЦ*

УЦ от момента создания до начала работы в различных системах ЭДО проходят через «сито» проверок со стороны регуляторов и организаторов систем ЭДО. Какова реальная цена этих проверок и каковы гарантии участникам СЭДО в случае ущерба в результате допуска на рынок «неадекватных» УЦ или при отсутствии контроля за их деятельностью? Практика проверки и взаимодействия с УЦ при авторизации на федеральных ЭТП и в ходе дальнейшей работы.

Применение квалифицированной электронной подписи в современной эпохе

Маслов Юрий Геннадьевич*, коммерческий директор, «КРИПТО-ПРО»*

В докладе будут рассмотрены практические моменты по использованию квалифицированной электронной подписи, которые построены пусть и на небольшом, но всё же опыте. К таким моментам относится и организации деятельности удостоверяющего центра, и оформление квалифицированных сертификатов ключей проверки электронной подписи, и организационные документы по использованию квалифицированной электронной подписи в информационных системах.

Роль общественных объединений бизнеса в становлении цивилизованного рынка электронных услуг

Миклашевич Анатолий Вадимович, *исполнительный директор НП «РОСЭУ»*

Широкое развитие рынка электронных услуг в сфере B2B, и B2G и участие в этой деятельности большого количества компаний приводит к необходимости урегулирования взаимоотношений бизнеса и государства.

Значительную роль в этом регулировании могут сыграть профессиональные объединения. Объединившись, мы сможем защитить как себя, так и наших клиентов, потребителей наших услуг.

15:00 – 19:00 **Секция «Криптография и криптоанализ»**
Конференц-зал «Марс» (Конференц-комплекс)

Ведущие:
Кузьмин Алексей Сергеевич, *ФСБ России*
Попов Владимир Олегович, *Ассоциация «РусКрипто», «КРИПТО-ПРО»*

Часть 1

Режимы блочных шифров: вопросы синтеза, анализа и эксплуатационные качества

Шишкин Василий Алексеевич, *ФСБ России*

Блочные шифры заняли одну из ведущих позиций в современной криптографической практике благодаря своей универсальности. Последнее достигается использованием различных конструкций, получивших название режимов (работы) блочных шифров. В докладе предполагается провести сравнительный анализ различных режимов в каждой из следующих трех групп: режимы шифрования, режимы выработки имитовставки, режимы аутентифицированного шифрования.

Merkle-Damgård vs Sponge: сравнительный анализ двух конструкций функций хэширования

Маршалко Григорий Борисович, Шишкин Василий Алексеевич, *ФСБ России*

Начало 21 века ознаменовалось стремительным развитием методов анализа функций хэширования. Результатом этого стала необходимость разработки новых подходов к их синтезу. В данной работе проводится сравнительный анализ свойств двух наиболее распространенных конструкций функций хэширования: конструкции Меркля-Дамгорда, лежащей в основе семейства хэш-функций «Стрибог», принятых в качестве национального стандарта Российской Федерации ГОСТ Р 34.11-2012, и sponge-конструкции, примером которой является хэш-функция «Keccak», планируемая к принятию в качестве национального стандарта США.

О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012

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

Рассматривается набор сопутствующих алгоритмов, предлагаемых для использования в криптографических протоколах на основе российских стандартов алгоритма хэширования и процессов формирования и проверки электронной подписи. Приводится ряд утверждений с обоснованием свойств рассматриваемых алгоритмов, опирающихся на свойства функции сжатия ГОСТ Р 34.11-2012, предположения о задачах Диффи-Хеллмана (распознавательной и вычислительной) и дискретного логарифмирования в группах точек эллиптических кривых.

О возможности стандартизации протоколов выработки общего ключа

Сергей Владимирович Гребнев, *ФСБ России*

В работе описывается возможная структура нормативного документа, вводящего стандартизированный набор протоколов выработки общего ключа, приводится перечень протоколов, предлагаемых для включения в состав стандартизированного решения, рассматриваются их основные криптографические и эксплуатационные характеристики.

Часть 2

О формализации и систематизации основных понятий дифференциального криптоанализа итеративных блочных шифров

Пестунов Андрей Игоревич, *Новосибирский государственный университет экономики и управления – «НИНХ», Институт вычислительных технологий СО РАН*

Формализованы основные понятия дифференциального криптоанализа с использованием бинарных масок. Показано, что усеченная характеристика – это наиболее общее понятие, а все остальные (усеченный дифференциал, характеристика и дифференциал) являются ее частными случаями. Формализована конкатенация усеченных характеристик.

О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе

Алексеев Евгений Константинович, *к.ф.-м.н., инженер-аналитик 1 категории, КРИПТО-ПРО*

Производится краткий обзор известных результатов о свойствах скрученных кривых Эдвардса, рассматриваются аспекты использования кривых из данного класса совместно с российским стандартом электронной подписи и с сопутствующими алгоритмами ключевого обмена на его основе. Приводится ряд оценок изменения быстродействия конечных реализаций алгоритмов в программных СКЗИ при работе с данным классом эллиптических кривых в широком классе, интересных с точки зрения практики случаев.

Обеспечение криптографически защищенных групповых коммуникаций с функцией отказуемости

Коростелева Мария Викторовна, Гамаюнов Денис Юрьевич, *Лаборатория безопасности информационных систем Факультет Вычислительной математики и кибернетики МГУ имени М. В. Ломоносова*

Доклад посвящен исследованию свойств протокола mpOTR (multy-party Off-The-Record messaging), который предназначен для криптографически защищенных многопользовательских коммуникаций через интернет с обеспечением аналога "приватных переговоров"- возможностью отказа участника от факта участия в них и авторства сообщений.

О вероятностях r-раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием

Пудовкина Марина Александровна, *Национальный исследовательский ядерный университет (МИФИ)*

Раундовая функция XSL-алгоритма блочного шифрования является композицией трёх преобразований: преобразования сдвига (сложение с ключом), нелинейного преобразования (s-бокса) и линейного преобразования. Для XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием вместо «классической» r-раундовой разностной характеристики в разностном методе предлагается рассматривать r-раундовую характеристику, заданную последовательностью смежных классов инвариантного подпространства линейного преобразования. Это позволяет улучшить оценки вероятностей r-раундовых пар разностей, что может привести к увеличению числа атакуемых раундов.

О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом

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

Двумерная задача дискретного логарифмирования является обобщением классической задачи дискретного логарифмирования. В докладе рассматривается ряд оценок средней трудоемкости решения этой задачи алгоритмом Годри-Шоста в случае использования автоморфизмов порядка 2, 4 или 6; также для указанных случаев приводятся улучшенные оценки.

О периодичности функционирования генераторов псевдослучайных чисел RC4, IA, IBAA

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

Генераторы псевдослучайных чисел RC4, IA. IBAA и другие этого типа моделируются неавтономным автоматом, состоящим из параллельного соединения нескольких взаимно управляемых неавтономных автоматов, один из которых считается основным. Его состояниями – ключами являются отображения кольца вычетов по модулю m в кольцо вычетов по модулю 2^K, K>2m. Приводятся условия гарантированности периодов последовательностей этих отображений в процессе функционирования указанных генераторов.

Часть 3 (Второй день, 27 марта, четверг)

The Control of technology by nation state : Past, Present and Future - The Case of Cryptology and information security

Eric Filiol, *Director of the Operational Cryptology and Virology Lab at ESIEA, Laval, France*

Алгоритм хэширования MCSSHA-7

Масленников Михаил Евгеньевич, *к. ф.-м. н., начальник отдела разработки ПО, ФГУП НТЦ «Система»*

В докладе рассматривается способ хэширования, основанный на неавтономном регулярном регистре сдвига с обратной связью над кольцом Z/N. Стойкость хэширования достигается за счет того, что знаки входного сообщения подаются на вход регистра не в каждый такт, а с задержкой, во время которой на вход PC подаются нули. Такой подход позволяет реализовывать быстрые и весьма простые схемы хэширования, пригодные к использованию, например, в таких устройствах, как смарт-карты. Предлагается конкретный вариант алгоритма хэширования из семейства MCSSHA.

Эффективная реализация базовых криптографических конструкций: перспективного алгоритма блочного шифрования с длиной блока 128 бит, функции хэширования ГОСТ Р 34.11-2012 и ЭЦП ГОСТ Р 34.10-2012

Бородин Михаил Евгеньевич*, Рыбкин Андрей Сергеевич, «ИнфоТеКС»*

Работа посвящена исследованиям принципиальных алгоритмических возможностей ускорения заявленных в названии криптографических конструкций. Предложены новые способы оптимизации и приведены полученные оценки производительности.

Об исследовании возможностей построения эффективных реализаций одного перспективного LSX-шифра

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

В докладе представлены предварительные результаты теоретических и экспериментальных исследований алгоритма шифрования, построенного по LSX-схеме, с точки зрения возможности построения эффективных реализаций на базе существующего поколения CPU с поддержкой SIMD-расширений и на GPU.

Эффективная реализация алгоритма ГОСТ 28147-89 с помощью технологии GPGPU

Кролевецкий Алексей Владимирович, *ведущий программист отдела перспективных разработок ООО «Код Безопасности»*

В докладе рассматриваются особенности реализации алгоритма ГОСТ 28147-89 на архитектурах современных CPU и GPU. Описываются технологии и методы программирования GPU для вычислений общего назначения. Выполнено сравнение скорости шифрования на CPU и GPU от различных производителей.

О шифровании данных в устройствах с блочной внутренней структурой

Коробов Владимир Владимирович*, «ОКБ САПР»*

Приводится краткий обзор режимов, рекомендуемых стандартами IEEE P1619 для применения в устройствах с блочной внутренней структурой. Рассматривается возможность применения таких режимов совместно с российскими криптографическими алгоритмами. Предлагается технология распараллеливания вычислений для одновременного шифрования и выработки имитозащитной вставки.

О создании эффективной аппаратной реализации ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 на основе ПЛИС

Родионов Андрей Юрьевич, *ЗАО «ОКБ САПР»*

Рассматриваются алгоритм умножения Монтгомери, групповые операции с точками в Якобиевом представлении, скалярное произведение точки на число. Приведен их анализ и адаптация для аппаратной реализации на ПЛИС в соответствии с принципом максимального распараллеливанию вычислений.

Редукция NP сложной задачи. Шифрование с открытым ключом

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

В работе рассматриваются варианты построения легко разрешимых задач NP сложной задачи целочисленного программирования. Показаны методы редукции данных задач, которые маскируют легко разрешимую задачу. Приводятся примеры использования для криптографии с открытым ключом.

Сложение по модулю 2^n в блочном шифровании

Каррондеев Андрей Михайлович, *МГТУ им. Н.Э. Баумана, факультет «Информатика и системы управления», кафедра «Информационная безопасность», группа ИУ8-104*

Работа посвящена анализу стойкости алгоритмов блочного шифрования, имеющих структуру SP-сетей, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n. Предложены линейные и нелинейные аппроксимации данной операции. Приведен пример их использования для проведения атаки типа Known Plaintext Attack на шифр, имеющий структуру SP-сети. Показано, что замена операции XOR на + mod 2^n приводит к увеличению стойкости блочных шифров.

15:00 - 16:30	**Круглый стол «Подлинная безопасность, разговор на троих»**
	Конференц-зал (Ресторанный комплекс)

Эксперты:

- ***Качалин Алексей Игоревич****, заместитель генерального директора, Перспективный мониторинг.*
- ***Гордейчик Сергей Владимирович,*** *технический директор, Positive Technologies*
- ***Купреев Олег Владимирович,*** *ведущий исследователь, Digital Security*

Комплексное обеспечение информационной безопасности задача многогранная и не всегда прозрачная. Эксперты отрасли обсудят, что очень важно, а что нет, расскажут о реально работающих механизмах и своих подходах к решению этой задачи.

17:00 – 19:00	**Секция «Технологии создания безопасного программного обеспечения»**
	Конференц-зал (Ресторанный комплекс)

Ведущие:

- ***Проскурин Вадим Геннадьевич,*** *к.т.н., доцент, заместитель председателя учебно-методического совета учебно-методического объединения вузов России по образованию в области ИБ*
- ***Аветисян Арутюн Ишханович,*** *д.ф.-м.н., доцент, ученый секретарь, ИСП РАН*

Обратная отладка мобильных приложений

Фурсова Наталья Игоревна, *Кафедра ИТиС, Новгородский государственный университет имени Ярослава Мудрого*

Рассматриваются способы обратной отладки в применении к мобильным приложениям. Предлагается метод для выполнения отладки с использованием детерминированного воспроизведения программ.

Восстановление формата данных путем анализа бинарного кода: состояние и перспективы

Падарян Вартан Андроникович*, ВМиК МГУ*

В докладе рассматриваются вопросы применения динамического анализа бинарного кода для решения задачи восстановления форматов данных. Описываются аспекты, затрудняющие анализ, такие как шифрование данных и способы их преодоления. Перечисляются области применения восстановленных форматов.

Современные тенденции развития технологий анализа и защиты программного обеспечения

Докладчик уточняется, кафедра криптологии и дискретной математики, МИФИ

Обфусцирующий компилятор на базе LLVM

***Курмангалеев Шамиль Фаимович**, Институт системного программирования РАН*

Доклад посвящен вопросам практического применения методов запутывания кода к широкому кругу задач. Приведен обзор обфускаторов, построенных на базе компиляторных инфраструктур. Обсуждаются вопросы трансформации программ во время компиляции для защиты от эксплуатации уязвимостей на примере переполнения буфера, динамического шифрования буферов, содержащих обрабатываемые данные, для защиты обрабатываемой программой информации. Разработанные методы реализованы в обфусцирующем компиляторе на базе LLVM.

О представлении МРОСЛ ДП-модели в формализованной нотации Event-B (Rodin Platform)

***Девянин Петр Николаевич,** д.т.н., доцент, УМО ИБ*

Рассматривается подход к переходу от математической нотации представления мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели), ориентированной на реализацию в отечественной защищенной операционной системе специального назначения Astra Linux Special Edition (ОССН), к формализованной нотации Event-B (Rodin Platform). Такой переход позволит верифицировать описание модели и осуществить дедуктивные доказательства ее свойств, а дальнейшем, задав на основе формальной нотации спецификации (предусловия и постусловия) функций механизма управления доступом ОССН с использованием инструмента дедуктивной верификации кода Why (в среде разработки Frama-C), обосновать адекватность реализации модели в программном коде ОССН.

Методы выявления и предотвращения недекларированного выполнения программ

***Компаниец Радион Иванович**, директор Департамента разработки и испытаний, ООО «Газинформсервис»*

Предлагаются автоматные и графовые модели контроля потоков управления в исполняемых кодах программ. Рассматриваются процедуры автоматического синтеза программы автомата контроля для предотвращения недекларированного выполнения программы. Дается обзор практической реализации методов в ИК Ирида.

Новый подход к защите графических подсистем рабочих станций LINUX

***Проскурин Вадим Геннадьевич,** к.т.н., доцент, УМО ИБ*

Описываются результаты проведенного анализа защищенности графических подсистем современных версий Linux. Показано наличие множественных уязвимостей, позволяющих вредоносным графическим приложениям несанкционированно повышать свои полномочия, похищать конфиденциальную информацию. Для устранения данных уязвимостей предложен новый подход, основанный на реализации мандатного контроля целостности с инкапсуляцией недоверенных графических приложений в отдельные графические терминалы и виртуализацией их информационного обмена с доверенными графическими приложениями, выполняющимися на основном графическом терминале.

Второй день работы конференции

10:00 – 13:30	**Секция «Криптография для мобильных платформ»** *Конференц-зал (Ресторанный комплекс)*

Ведущие:

- ***Федорушкин Илья Владимирович**, Samsung Electronics*
- ***Калайда Игорь Алексеевич**, генеральный директор, НИИ СОКБ*

Специфика разработки конкурентных решений для защиты трафика мобильных устройств в Российской Федерации

***Харитонов Роман Леонидович,** руководитель проектов, «С-Терра СиЭсПи»*

В докладе будут описаны отличительные принципы разработки криптографических средств для защиты трафика мобильных устройств, дана оценка емкости рынка продуктов для обеспечения безопасности мобильных устройств, обозначены основные требования со стороны регуляторов и возможности соответствия им со стороны разработчиков средств защиты и производителей устройств. Кроме того, будут рассмотрены особенности реализации проектов в области применения СКЗИ на мобильных устройствах на российском рынке.

ЭП на SIM-карте. Почему это безопасно

***Груздев Сергей Львович,** генеральный директор, «Аладдин Р.Д.»*

В рамках доклада будут представлены технологии, реализующиеся в новейшей разработке компании "Аладдин Р.Д." – SIM-карте с электронной подписью "на борту", благодаря которой как физические, так и юридические лица смогут получить новый доверенный канал, использование которого максимально удобно и надёжно.

Реализация СКЗИ на мобильных платформах с ОС iOS и Android

***Василенков Александр Сергеевич,** менеджер продуктов, ОАО «ИнфоТеКС»*

В докладе рассматриваются вопросы достижения комплексной информационной безопасности наиболее популярных сценариев использования мобильных устройств в корпоративной среде. Доклад построен на базе накопленного реального опыта компании «ИнфоТеКС» и ее технологических партнеров по созданию средств криптографической защиты информации для мобильных платформ.

Ключевые носители для смартфонов и планшетов

***Горелов Дмитрий Львович,** коммерческий директор, компания «Актив»*

Использование отторгаемых ключевых носителей важное требование многих информационных систем, использующих технологии электронной подписи. Для мобильных платформ пока очень мало устройств, которые могут успешно решить эту задачу. Что российские и зарубежные разработчики предлагают потребителю? Какова российская специфика данных решений?

И ещё раз о корректности встраивания

***Хенкин Петр Владимирович**, начальник отдела, ЗАО «Перспективный Мониторинг»*

Корректно ли реализована криптография в прикладном ПО на мобильных устройствах, опубликованных в магазинах приложений? Результаты исследования, показавшего некорректные методы использования криптографии во многих потребительских приложениях. Примеры обнаруженных популярных приложений с явными проблемами и уязвимостями, выводы о причинах и возможных последствиях допущенных изъянов, возможном воздействии на данные пользователя, в том числе и на других устройствах.

Практические аспекты организации защищенного подключения iOS- приложений к корпоративным ресурсам

***Альперович Михаил Моисеевич**, Директор Лаборатории Защищенной Мобильности, Digital Design*

В докладе обобщен опыт внедрения корпоративных решений для iOS- устройств с использованием протоколов SSL/TLS на базе сертифицированных СКЗИ от «КРИПТО-ПРО». Это решает задачи аутентификации, шифрования и контроля целостности данных, передаваемых по открытым каналам связи.

10:00 – 11:30	**Секция «Безопасность интернета вещей»** *Конференц-Зал «Марс» (Конференц-комплекс)*

Ведущий: ***Гордейчик Сергей Владимирович,*** *научный редактор SecurityLab.ru, технический директор Positive Technologies*

Армия освобождения домохозяек: структура, состав вооружений, методы коммуникации

Петухов Андрей Александрович, *Лаборатория безопасности информационных систем ВМК МГУ, м.н.с*

В докладе будет сделан обзор актуальных угроз для различных классов "умных" вещей. Будут рассмотрены векторы атаки через Интернет и через беспроводные подключения. Наконец, будут представлены различные "футуристические" варианты построения собственного SkyNet из умных вещей

Слишком Smart Grid в облаках

Чайкин Артем Александрович, *ведущий специалист, группа безопасности приложений, Positive Technologies*

В связи с «облачной» лихорадкой в облачные приложения и сервисы переводят все, до чего дотягиваются руки. В настоящее время в «облако» активно переводятся различные Man2Machine и Machine2Machine системы. Доклад будет посвящен последствиям необдуманного сочетания двух модных технологий – Cloud и SmartGrid.

Как отличить принтер-вундеркинд от IP-телефона?

Москвитин Андрей, *специалист по решениям информационной безопасности, Cisco*

Угрозы для внутренней сети предприятия в эру BYOD. Проблематика – чем опасны неуправляемые устройства на предприятии. Как отличить принтер-вундеркинд от IP-телефона? Как вовремя узнать, что атакующий притворяется принтером? Способы и решения.

Безопасность Интернета вещей. Все ужасы угроз АСУ ТП. Теперь у вас дома!

Качалин Алексей Игоревич, *зам. генерального директора, ЗАО «Перспективный Мониторинг»*

Интернет вещей – тема, поднимающая массу вопросов по части информационной безопасности. Многообразие устройств, архитектур программ и протоколов обмена с одной стороны и, как следствие, все известные на сегодня угрозы и уязвимости. Давайте обсудим – какие возможности получает атакующий при атаке на кардио-монитор или кондиционер? Кому сообщает телевизор о ваших пристрастиях в выборе контента? что скоро будет видно из квартиры и слышно из вашей машины?

Первым делом – самолеты!

Докладчики выступают инкогнито

Как Интернет работает на борту самолета? Что за странный ящичек с видео в спинке сиденья перед вами? Что с ним можно такого сделать, чтобы весело и с пользой? А чего сделать нельзя или наоборот – категорически нельзя делать?!

12:00 – 13:30	**Секция «Продукты и технологии информационной безопасности»** *Конференц-Зал «Марс» (Конференц-комплекс)*

Ведущий: ***Антимонов Сергей Григорьевич,*** *председатель совета директоров, ЗАО "ДиалогНаука"*

Практическое применение статистических и временных индикаторов для выявления и расследования инцидентов ИБ

Кропотов Владимир Борисович*, эксперт по информационной безопасности*

Феномен криптовалюты «Биткоин». Построение математических моделей децентрализованных информационных систем, реализующих функции платежных систем криптовалют. Подходы к комплексной оценке безопасности, в том числе оценке криптографической стойкости

Комисаренко Владимир Владимирович, *директор по развитию, ЗАО «БЕЛТИМ СБ», директор ассоциации «РусКрипто»*

Роговой Александр Сергеевич*, специалист отдела информационной безопасности, ОАО «Банк Москва-Минск»*

В последнее время криптовалюта «Биткоин» привлекает огромное внимание широкого круга специалистов в сферах банковского дела, экономики, политики и информационной безопасности. Создано множество специализированых Интернет-ресурсов. Однако крайне мало специалистов дало оценку информационной и криптографической безопасности информационных систем, реализующих функции криптовалют. В докладе приводятся современное состояние, тенденции, прогнозы и основные подходы к комплексной оценке безопасности, в том числе оценке криптографической стойкости.

Защищенный удаленный доступ для разных платформ, специфика и особенности

Куликов Андрей Валерьевич, *директор департамента разработки криптографических продуктов, ООО «Новые технологии безопасности»*

Сегодня сложно найти организацию, которая не использует удаленный доступ. Растет как вариативность используемых для доступа устройств, равно как и угрозы компрометации передаваемой, хранимой и обрабатываемой информации. Защита при передаче обеспечивается с использованием криптографии, аутентификация при подключении может происходить с помощью различных методов, в том числе стойких (с использованием сертификатов) или облегченные варианты на базе статических или динамических паролей (OTP). Отдельной задачей стоит проверка соответствия рабочего окружения платформы при ее удаленном подключении. В докладе будут рассмотрены различные варианты организации защиты.

Кибервойна, день первый. Виды и возможности современного кибероружия

Масалович Андрей Игоревич, *к.ф-м.н, ведущий эксперт по конкурентной разведке*

В докладе рассматривается структура и образцы основных видов современного кибероружия - наступательного, оборонительного и разведывательного.

Приводятся примеры возможных последствий его применения. Также рассматривается инструментарий информационных войн корпоративного, регионального и международного уровней.

14:30 – 16:00	**Секция «Использование инфраструктуры УЦ для решения задач идентификации и аутентификации** *Конференц-зал (Ресторанный комплекс)*

Ведущий: ***Комисаренко Владимир Владимирович****, директор по развитию ЗАО «БЕЛТИМ СБ», директор ассоциации «РусКрипто»*

Методика оценки рисков безопасности аутентификации пользователя при применении электронной подписи

Сабанов Алексей Геннадьевич, *к.т.н., заместитель директора, ЗАО «Аладдин Р.Д.»*
Связь аутентификации и электронной подписи. Методика оценка рисков. Анализ угроз и уязвимостей аутентификации. Концепция моделирования процессов аутентификации.

Аутентификация +\-10 лет

Царев Евгений Олегович, *эксперт по информационной безопасности*
Развитие от дискет до беспроводных систем. Унификация или разделение устройств аутентификации? «Глобализация» систем аутентификации.

Обеспечение аутентификации и авторизации в Интернет: опыт электронного правительства

Ванин Михаил Владимирович, *Начальник отдела разработки систем идентификации и аутентификации, R-Style*
При выполнении работ по развитию Единой системы идентификации и аутентификации (ЕСИА) в составе инфраструктуры электронного правительства решалась задача — обеспечить предоставление подключенным к ЕСИА информационным системам данных о зарегистрированных пользователях. Для этого было осуществлено развитие механизмов обеспечения аутентификации и авторизации взаимодействующих с ней через Интернет систем и пользователей. В докладе будет рассказано об особенностях работы этих механизмов, основанных на использовании таких технологий как OpenID Connect, OAuth 2.0 и возможности их дальнейшего применения при развитии в РФ экосистемы обеспечения безопасности взаимодействия в Интернете.

Аутентификация и электронная подпись - взгляд оператора мобильной связи

Сикорский Александр Борисович, *к.т.н., начальник отдела криптографической защиты информации, МТС*
Особенности работы оператора мобильной связи в качестве оператора ЭДО и Удостоверяющего центра. Консалтинг как форма снятия неопределенностей в выработке вариантов перехода на электронный документооборот внутри компании оператора и при работе с контрагентами. Функционал применения квалифицированной электронной подписи для аутентификации и юридически значимого электронного документооборота.

14:30 – 16:00	**Секция «Безопасность современных информационных технологий — новые возможности и новые угрозы»** *Конференц-Зал «Марс» (Конференц-комплекс)*

Ведущие:

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

Расширяющееся киберпространство — новые горизонты возможностей и угроз

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

В настоящее время постиндустриальное общество находится в состоянии глобальной компьютеризации систем управления промышленными объектами и их интеграции в сеть Интернет, что неизбежно увеличивает уязвимость с точки зрения информационной безопасности. Технологии нападения и защиты неразрывно связаны друг с другом, и создать эффективное решение можно только опираясь на глубокие знания о методах и технологиях, используемых противоположной стороной. Целью настоящего доклада является попытка проанализировать основные тенденции появления новых угроз безопасности и механизмов их осуществления, что должно способствовать предотвращению их реализации.

Адаптивная обманная система для рефлексивного управления злоумышленником

***Лаврова Дарья Сергеевна**, аспирант кафедры «Информационная безопасность компьютерных систем», СПбГПУ*

В докладе рассматривается формализованный с использованием алгебры конфликтов Лефевра конфликт информационной безопасности между злоумышленником и администратором безопасности, производится выбор стратегий рефлексивного управления злоумышленником для реализации посредством механизма обманных систем. Предлагается концепция адаптивной обманной системы, основанная на динамическом реагировании на действия злоумышленника и реализующая рефлексивное управление злоумышленником путем навязывания ему определенной стратегии поведения.

MESH NETWORK: защищенная сеть или "дыра" в безопасности

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

Изначально mesh-сети использовались армией США во время проведения специальных операций. Сейчас они внедряются повсеместно — от небольших офисов и "умных" домов до целых районов. Механизмы безопасности, применяемые в mesh-сетях, основаны на криптографических алгоритмах и направлены, в первую очередь, на защиту от внешнего нарушителя. При этом внутренний нарушитель в таких сетях обладает широкими возможностями по нарушению маршрутизации трафика и реализации связанных с этим угроз, единого подхода к защите от которых в настоящее время не существует.

«Безопасный стиль вождения» - защита компьютерной инфраструктуры современных автомобилей

***Печенкин Александр Игоревич**, к.т.н., руководитель проектов, «НеоБИТ»*

Современный автомобиль обладает множеством функций, нацеленных на повышение комфорта и безопасности вождения, – ABS, ESP, EBD, парковочный автопилот, различные мультимедийные и навигационные системы и т.д. Все компоненты автомобиля управляются электронными системами, использование которых с одной стороны позволяет эффективнее решать поставленные задачи, а с другой приводит к появлению новых угроз безопасности. В докладе рассмотрены возникающие угрозы, возможные их источники и сценарии атак.

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

Конференц-Зал «Марс» (Конференц-комплекс)

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

Модели и методики визуального анализа данных для решения задач компьютерной безопасности

***Новикова Е.С.**, к.т.н., доцент, СПбГЭТУ «ЛЭТИ»*

Анализируются различные модели и методики визуального анализа, разработанные для мониторинга сетевого трафика, анализа таблиц маршрутизации, оценки политик безопасности и уровня защищенности компьютерных сетей. Формулируются основные требования к подсистеме визуального анализа как составной части автоматизированных систем мониторинга и управления информационной безопасностью, предлагается общий подход к ее проектированию. Демонстрируются возможности разработанной системы визуального анализа для моделирования атак и оценки уровня защищенности.

Обработка событий безопасности в условиях реального времени с использованием подхода, основанного на анализе деревьев атак

Чечулин Андрей Алексеевич, *к.т.н., лаборатория проблем компьютерной безопасности, СПИИРАН*
Котенко Игорь Витальевич, *д.т.н., профессор, зав.лабораторией проблем компьютерной безопасности, СПИИРАН*

Рассматривается предлагаемый подход к оценке защищенности компьютерных сетей, позволяющий производить анализ поступающих событий безопасности в реальном времени. Рассмотрены основные элементы используемых моделей, алгоритмов и методик. Приведено описание разработанного программного прототипа системы и результаты экспериментов, подтверждающие достижение заявленных показателей эффективности оценки защищенности.

Адаптивная под условия продолжительного мониторинга система визуализации событий информационной безопасности

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

Доклад посвящен системе визуализации событий информационной безопасности, способной адаптировать свой интерфейс и методы отображения под текущего оператора, основываясь на характеристиках взаимодействия с ним.

Проектирование и верификация механизмов защиты систем со встроенными устройствами на основе экспертных знаний

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

Рассматриваются модели, методики и программные средства проектирования и верификации комбинированных механизмов защиты информационно-телекоммуникационных систем со встроенными устройствами, основанные на использовании экспертных знаний специалистов в области защиты информации.

Исследование средств обнаружения шеллкодов для платформы ARM

Петров Иван, Гайворонская Светлана Александровна*, МГУ им. М.В.Ломоносова*

Проводится анализ существующих методов детектирования с позиции их применимости к шеллкодам, написанным для архитектуры ARM. Представляются реализованные детекторы ARM-шеллкодов, как расширение для библиотеки детектирования шеллкодов - Demorpheus.

Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

Федорченко Андрей Владимирович*, ОКБ «КАРАТ»*

Приводится обзор наиболее распространенных баз уязвимостей, таких как CVE, NVD и OSVDB. Анализируются их основные достоинства и недостатки с точки зрения использования этих баз при анализе защищенности компьютерной сети. Представляются результаты анализа основных тенденций в области обнаружения уязвимостей в программно-аппаратных продуктах таких компаний как Microsoft, Apple, Cisco, Google и т.д.

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 применяются в системах 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:
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 цифровой подписи (ЭЦП). USB-токены Рутокен являются ключевыми носителями в массовых российских проектах, базирующихся на технологии ЭЦП и инфраструктуре открытых ключей (PKI).

Продукция Рутокен имеет 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) 925-7790

Компания «ИнфоТеКС»

ОАО «ИнфоТеКС» - лидер отечественного рынка программных и программно-аппаратных VPN-решений и средств защиты информации в TCP/IP сетях. Компания основана в 1989 году и зарегистрирована в 1991 г. среди первых акционерных обществ России. За более чем 20 лет присутствия на рынке ИБ созданная компанией технология ViPNet успешно зарекомендовала себя в масштабных проектах федерального уровня и стала фактически стандартом сертифицированной защиты конфиденциальной информации.
Согласно данным рейтинга CNews Analytics «Крупнейшие компании России в сфере защиты информации 2013» компания входит в ТОП-10 крупнейших компаний, работающих на российском рынке ИБ.

Совместно со своими партнерами ОАО «ИнфоТеКС» предлагает полный спектр услуг по созданию 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.

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

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

Компания «Газинформсервис»

Компания «Газинформсервис» основана в 2004 году. Сегодня «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 удостоверяющего центра, испытательной лаборатории, проводит работы по аттестации и сертификации, а также оказывает консалтинговые услуги в области информационной безопасности и обеспечения безопасности объектов.

Основные виды деятельности — системная интеграция в области информационной безопасности и информационных технологий, а так же интегрированных инженерных систем безопасности.

Контактная информация:
www.gaz-is.ru
pr@gaz-is.ru
+7 (812) 305-20-50

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.

"Аладдин Р.Д." активно развивает свой бизнес в направлении разработки решений и оказании услуг для крупных корпоративных клиентов и государственного сектора. 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. Лидерские позиции "Аладдин Р.Д." подкреплены 18-летним опытом работы на российском рынке информационной безопасности, а также прочными партнёрскими отношениями с ведущими российскими разработчиками систем криптографической защиты информации (СКЗИ), системными интеграторами и ведущими технологическими лидерами: Athena Smartcard Solutions, Microsoft, Apple, Vasco, Gemalto, MasterCard, Visa и др.

Компания "Аладдин Р.Д." прошла сертификацию менеджмента качества на соответствие российским стандартам ГОСТ Р ИСО 9001-2011.

Контактная информация:
www.aladdin-rd.ru
aladdin@aladdin.ru
+7 (495) 223-00-01

Компания R-Style

Компания R-Style работает на высокотехнологичном рынке России и стран СНГ с 1991 года. На сегодняшний день компания является крупнейшим поставщиком ИТ-решений и бизнес-систем. Основное направление деятельности – системная интеграция. R-Style реализует комплексные проекты «под ключ», поддерживает высокие компетенции в следующих областях:

- Инфраструктура.
- Информационная безопасность.
- Телекоммуникации и связь.
- Разработка и внедрение бизнес-решений, специализированного (заказного) ПО, инженерных систем.
- ИТ-аутсорсинг и ИТ-консалтинг.
- Обучение в сфере ИТ.

Среди заказчиков компании R-Style: Пенсионный фонд России, Центральный Банк России, Федеральная налоговая служба России, Федеральное казначейство, Федеральная служба охраны, «Электронная Москва», «Российские железные дороги», «Росгранстрой», ДИТ города Москвы, ФСФР России, Министерство юстиции России, «Сбербанк России», «Райффайзен Банк», «Аэрофлот», «Ростелеком», «МТС», «Вымпелком» (Билайн), «Мегафон», Большой Театр, Knauf, «СИБУР», «Красный Квадрат», конкурс «Евровидение», Oriflame, «Очаково», «Вимм-Билль-Данн», «Русснефть», «ФСК», «РусГидро» и многие другие. Партнерами компании являются ведущие мировые производители оборудования и программного обеспечения, среди которых: IBM, HP, Oracle, Microsoft, Intel, Epson, Canon, Xerox, Red Hat, Novell, Philips, AMP, Cisco, Acer, APC и др. По оценкам авторитетных аналитических агентств (IDC, CNews, «РА Эксперт», «Финанс») компания R-Style на протяжении многих лет входит в десятку ведущих ИТ-компаний и провайдеров ИТ-услуг. Качество услуг компании соответствует стандарту ГОСТ Р ИСО 9001–2001 (ISO 9001–2000). Компания имеет 100% всех необходимых лицензий, включая работу со сведениями, содержащими государственную тайну.
R&D-центры и филиалы компании R-Style расположены в восьми федеральных округах России и странах СНГ (Беларусь). Компания гарантирует самый высокий уровень сервиса в любой точке России и СНГ.

Контактная информация:
www.r-style.com
project@R-Style.com
+7 (495) 640-60-10

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), серебряным партнером Samsung.

«С-Терра СиЭсПи» 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 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.

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

Компания Check Point Software Technologies Ltd.

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:
www.rus.checkpoint.com
+7 (495) 967- 7444

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 компании 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.

«Код Безопасности» оказывает партнерским организациям поддержку в реализации проектов по внедрению продуктов компании в сложные информационные системы. Сервисный центр компании готов предоставить профессиональную техническую поддержку партнерам и Заказчикам компании 24 часа и 7дней в неделю.

Контактная информация:
www.securitycode.ru
info@securitycode.ru
+7 (495) 982-3020

ISBC

Группа компаний ISBC является ведущим российским поставщиком оборудования и решений для построения систем информационной безопасности, контроля физического доступа, программ лояльности с использованием смарт-карт. На данный момент ISBC Group выступает эксклюзивным дистрибьютором продукции ведущих мировых вендоров оборудования и решений в сфере смарт-карт, RFID и NFC-технологий. Один из продуктов ISBC – ключевые носители **ESMART® Token,** предназначенные для безопасного хранения и использования цифровых сертификатов, ключевой информации и электронной подписи.

Контактная информация:
www.smart-card.ru/contact/
sale@isbc.ru
+7 (495) 739-8699

Компания Stonesoft

Компания Stonesoft является ведущим разработчиком решений в сфере обеспечения корпоративной сетевой безопасности с более, чем 20 летним опытом. Наше портофолио включает межсетевой экран Firewalls/VPNs нового поколения, систему предотвращения вторжений IPS и шлюз защиты удаленного доступа SSL VPN, разработанные для организаций любого размера. Основа нашего успеха – трансформируемое, единое программное ядро, легкое в использовании благодаря централизованной системе управления, и наша инновационная защита против динамических техник обхода (AET). Наши успехи признаются многочисленными сертификатами, аналитиками индустрии ИБ и требовательными клиентами. Благодаря высочайшему уровню обслуживания клиентов, легкости управления и низкой стоимости владения (TCO) решений, Stonesoft имеет самый высокий в отрасли процент удержания клиентов.

В июле 2013 года Stonesoft была приобретена компанией McAfee, мировым лидером в области технологий безопасности, являющейся дочерним предприятием корпорации Intel. С этого времени все продукты Stonesoft являются частью портфолио McAfee. McAfee дает возможность предпринимателям, государственному сектора и домашним пользователям безопасно использовать преимущества Интернета. Предполагается, что решения Stonesoft упрочат лидерские позиции McAfee на рынке сетевой безопасности и послужат дополнением к стратегии Security Connected (структура Security Connected - это концепция безопасности, обеспечивающая всестороннюю защиту ИТ-инфраструктуры.), которая охватывает – безопасность сетей, конечных точек, мобильных решений и облаков. Ожидается, что такие передовые технологии Stonesoft как межсетевой экран нового поколения и защита от динамических техник обхода, сделают предложение McAfee для рынка сетевой безопасности наиболее комплексным и эффективным.

Контактная информация:
www.ssl.stonesoft.ru
sale@isbc.ru
+7 (495) 739-8699

Российский фонд фундаментальных исследований

Российский фонд фундаментальных исследований занимает весьма значимое место в системе организации отечественной науки. В настоящее время РФФИ – это не только сложившаяся структура, но и новая система отношений, охватывающая все стороны жизни научного сообщества. Фонд поддерживает наиболее активный научно-технический потенциал страны, обеспечивает ученых России финансовой поддержкой, реализует конкурсные механизмы финансирования научных исследований на основе экспертных оценок наиболее уважаемых членов научного сообщества.

Контактная информация:
www.rfbr.ru/rffi/ru
+7(495) 952-58-47

Компания «Перспективный мониторинг»

Закрытое акционерное общество «Перспективный мониторинг» (ЗАО «ПМ») оказывает услуги в области информационной безопасности на российском рынке более 5 лет, специализируется на проведении работ по исследованию состояния безопасности информационных систем организаций.В портфель услуг компании входит исследование информационных систем, анализ программного кода приложения, расследование инцидентов, проведение теста на проникновение.

Компания располагает штатом высококвалифицированных исследователей и инженеров с многолетним опытом работы в органах безопасности, а также в ведущих иностранных и российских системных интеграторах. В своей деятельности ЗАО «ПМ» использует технологии мирового уровня, проводит собственные разработки в области сбора и анализа данных в информационных системах.Основная задача компании – собрать команду профессионалов, способную найти для каждого клиента решение, которое отвечает потребностям бизнеса заказчика, соответствует лучшим практикам и мировым стандартам. Компания является лицензиатом ФСТЭК и ФСБ

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

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

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:
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 18 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»;
- 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.;
- 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.

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

Контактная информация:
www.infosystems.ru
security@infosystem.ru
+7(495) 231-30-49

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):

- 26 марта в 8.00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 26 марта в 19.15 вечера трансфер отель «Солнечный Park Hotel & SPA» – м. Речной вокзал.
- 27 марта в 8.00 утра трансфер м. Речной вокзал – отель «Солнечный Park Hotel & SPA».
- 27 марта в 19.15 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»:

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

Внимание! Автобусы с табличкой «РусКрипто'2014» отправятся ровно в 11:45, 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 – 25 марта в 18:00, выезд – 28 марта в 12:00.

Контакты организаторов:

Кочукова Виктория – т. 8 (925) 884-44-08
Ульянова Светлана – т. 8 (985) 134-80-40
Никифорова Тамара – т. 8 (905) 711-34-52