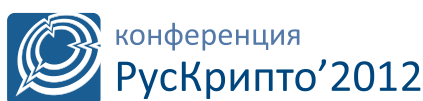


РусКрипто'2012

В период с 28 марта по 31 марта второй год подряд в подмосковском отеле «Солнечный Park Hotel&SPA» состоялась XIV международная конференция «РусКрипто'2012», посвященная актуальным вопросам теории и практики информационной безопасности (ИБ).



конференция
РусКрипто'2012

В ходе уникального мероприятия профессионалами в сфере ИБ, участниками и гостями конференции обсуждались следующие злободневные вопросы:

- состояние, перспективы мировой криптографии, а также возможные пути построения единого пространства доверия;
- выполнение ФЗ «Об электронной подписи», развитие удостоверяющих центров и операторов информационных систем;
- криптография и криптоанализ: развитие базовых стандартов и методических рекомендаций;
- перспективы развития антивирусной индустрии;
- технологии безопасности систем дистанционного банковского обслуживания;
- технологии защиты и нападения;
- рынок сетевой безопасности РФ;
- электронная подпись без границ;
- перспективные исследования в области кибербезопасности;
- криптография в облачных решениях и пр.

В конференции участвовали разработчики средств защиты информации, представители ведущих научных учреждений и учебных заведений, госслужащие, специалисты из коммерческих и государственных структур. География участников конференции оказалась весьма широ-

кой: более 200 гостей мероприятия представляли Москву, Санкт-Петербург, Новосибирск, Томск, Екатеринбург, Ростов-на-Дону, Курск, Самару, Пермь, Воронеж и другие города России. В конференции также приняли участие представители ближнего (Белоруссия, Казахстан, Украина) зарубежья. По итогам конференции «РусКрипто'2012» лучшие из прозвучавших на ней докладов опубликованы в специальном выпуске журнала, рекомендованного ВАК.

На пленарном заседании, открывшем конференцию, с приветственными словами выступили ее организаторы и ряд докладчиков. В частности, заместитель директора ФГУП ГНИВЦ ФНС России, профессор Высшей школы экономики А. П. Баранов, осветил актуальные задачи обеспечения информационной безопасности конфиденциальной информации в крупных корпоративных компьютерных системах и поделился опытом организации защиты в корпоративном облаке. При этом были затронуты интересные и малоизученные темы защиты гипервизоров и прикладных сервисов корпоративного облака. Доцент МГТУ им. Баумана, председатель совета директоров ассоциации «РусКрипто» А. Е. Жуков сделал исключительно интересный и насыщенный обзор новинок мировой криптографии, в том числе исследований так называемой облегченной криптографии, а заместитель секретаря ТК-26 «Криптографическая защита информации» А. И. Лунин и первый заместитель начальника центра

ФСБ России, председатель ТК-26, профессор А. С. Кузьмин подготовили совместный доклад о насущных проблемах создания информационного общества и роли криптографии в этом процессе. В докладе были определены основные цели и задачи создания доверенного информационного общества, а также направления их решения.

На круглом столе «Закон «Об электронной подписи» и его подзаконные акты. Как быть Удостоверяющим Центрам и операторам информационных систем?» завязалась живая дискуссия о проблемах использования электронной подписи в ежедневной деятельности организации. С интересным сообщением выступил эксперт по ИБ «Академии Информационных Систем» Д. О. Левиев, предложивший для соответствия новым требованиям использовать усиленную неквалифицированную электронную подпись и усиленную квалифицированную электронную подпись (ЭП) на основе криптографических средств, соответствующих российским ГОСТам. Далее докладчик пояснил, каким образом компании на практике могут учитывать требования, предъявляемые к средствам реализации удостоверяющих центров (УЦ) и ЭП законом № 152-ФЗ. Начальник отдела ИБ проекта «Информационное общество» компании ОАО «Ростелеком» И. А. Трифаленков рассказал о корпоративном опыте построения информационных систем головного удостоверяющего центра (ИС ГУЦ), в том числе, о создании совокупности инфор-

мационных систем, обеспечивающих предоставление услуг, связанных с постановкой и проверкой квалифицированной ЭП, об автоматизации деятельности уполномоченного органа в области ЭП и пр.

Благодаря выступлениям ведущих экспертов традиционная секция «Криптография и криптоанализ» собрала большую аудиторию и, по отзывам специалистов, стала одной из наиболее интересных на конференции. В частности, А. В. Лунин (ОАО «ИнфоТеКС»), заместитель секретаря ТК-26 обрисовал основные пути развития базовых стандартов криптографической защиты информации в России и за рубежом, начальник отдела защиты коммерческой тайны и персональных данных ОАО «Универсальная электронная карта» Д. В. Азин рассказал о криптографии и информационной безопасности в проекте Универсальная электронная карта, инженер аналитик ООО «Крипто-Про» С. В. Смышляев сообщил о новых способах противодействия атакам на протокол TLS, сотрудники ФСБ России В. И. Рудской, С. В. Гребнев, Д. М. Дыгин и В. О. Дрелихов сделали интересные доклады о криптографическом исследовании алгоритма шифрования ГОСТ 28147-89, реализации схемы ЭЦП ГОСТ Р 34.10, прыгающих клеточных автоматах. Доцент МИФИ, директор Ассоциации «РусКрипто» М. А. Пудовкина в своем сообщении сосредоточилась на разностных характеристиках обобщенного алгоритма шифрования Фейстеля 2-го типа.

В ходе секций «Настоящее и будущее антивирусной индустрии» и «Технологии защиты и нападения» активно обсуждались актуальные проблемы антивирусной защиты, уязвимости виртуальной защиты, новые технологии нападения и защиты. Так, руководитель отдела по подготовке технических решений Stonesoft Corp Д. В. Ушаков рассказал об основных тенденциях защиты от сетевых угроз и новых техниках защиты от старых угроз, а аналитик в области ИБ из ТНК-ВР В. Б. Кропотов и аналитик по безопасности P1 Security Ф. В. Ярочкин показали основные тренды сетевых атак,



Председатель Совета Ассоциации защиты информации Г. В. Емельянов и ректор АИС Ю. В. Малинин

вызванные активными действиями пользователей в 2011–2012 годах.

На круглом столе «Технологии безопасности систем ДБО» интересный доклад о существующих проблемах ДБО и путях их разрешения сделал представитель ОАО «Россельхозбанк» А. М. Сычев. В том числе, докладчик поделился опытом выполнения требований закона № 152-ФЗ для надлежащей защиты персональных данных в корпоративной системе банка на основе решений SAP. Коммерческий директор компании «Актив» Д. Л. Горелов провел обзор средств технической защиты клиентских мест дистанционного банковского обслуживания.

На секции «Электронная подпись без границ» прозвучали интересные сообщения советника Департамента электронного правительства Министерства связи и массовых коммуникаций РФ А. А. Домрачева о легализации иностранных электронных документов в интернет-экономике, начальника сектора управления защиты информации Оперативно-аналитического центра при Президенте Республики Беларусь В. В. Комисаренко о проблемах внедрения механизма ЭЦП и советника генерального директора ООО «Газинформсервис» С. А. Кирышкина о внедрении ЭП в автоматизированные трансграничные системы документооборота.

В секции «Перспективные исследования в области кибербезопасности» внимание участников привлекли доклады заведующего лаборато-

рией проблем компьютерной безопасности СПИИРАН, профессора И. В. Котенко и его учеников о моделировании и анализе событий в системах управления информацией и событиями безопасности. В них были представлены и обоснованы подходы к исследованию механизмов кибербезопасности на основе интеграции агентно-ориентированного и имитационного моделирования на уровне сетевых пакетов, аналитического анализа графов атак, методов эмуляции и виртуализации сетевых процессов. В рамках которого были разработаны соответствующие средства моделирования. Результаты экспериментов показали возможность использования предложенных подходов для аналитического моделирования механизмов кибербезопасности и анализа защищенности проектируемых сетей. Доклад представителя ИКСИ ФСБ РФ П. Н. Девянина был посвящен проблеме обоснования адекватности формальных моделей безопасности логического управления доступом и их реализации в компьютерных системах», в частности, обсуждались вопросы развития ДП-моделей операционных систем. Интересные доклады сделали сотрудники ЛВК ВМК МГУ им. М. В. Ломоносова: Д. Ю. Гамаюнов на тему «Разграничение доступа и минимизация ущерба от атак с помощью сильного принципа наименьших привилегий», А. П. Петухов о возможностях систем обнаружения web-сайтов, распространяющих вредоносное программное обес-

eToken ГОСТ

персональное средство формирования ЭП

- » Строгая двухфакторная аутентификация пользователей
- » Обеспечение юридической значимости ЭДО
- » Поддержка основных операционных систем и браузеров



*Сертификат соответствия
требованиям ФСБ России
к СКЗИ классов КС1 и КС2*

Аппаратная реализация российских криптоалгоритмов:
ГОСТ 34.10-2001, ГОСТ 34.11-94, ГОСТ 28147-89

Работает без установки драйверов в Windows, Mac OS, Linux

Комплект разработчика

Аладдин РД

ЗАО «Аладдин Р.Д.»
Тел.: +7 (495) 223-00-01
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

печение, С. Гайворонская о гибридном методе обнаружения шеллкодов в высокоскоростных каналах передачи данных.

В секции «Криптография в облачных решениях, безопасность информационных систем с размытыми контурами» представители академических школ рассказали о проблемах и путях их разрешения при использовании криптографии во внешних и внутренних, корпоративных облаках. В частности, заведующий кафедрой ИБ компьютерных систем СПбГПУ, профессор П. Д. Зегжда сделал интересный доклад на тему «Облачные вычисления. Виртуальная безопасность или безопасность виртуализации?», а гендиректор компании «Аладдин Р. Д.» С. Л. Груздев – на тему «Строгая аутентификация и квалифицированная электронная подпись для порталных решений и облачных сервисов».

Отметим, что все мероприятия конференции вызвали бурные обмены мнениями, которые по окончании работы секций и круглых столов плавно перемещались в кулуары.

В заключении отметим, что в этом году конференцию активно поддержали участием многие федеральные министерства и ведомства, такие как ФСБ России, Минкомсвязи России, Минобороны России, МВД России, общероссийские ассоциации и объединения (УМО ИБ, МОО «АЗИ», НКО АЭТП, RISSPA, АП КИТ и др. Организаторы конференции – Ассоциация «РусКрипто» совместно с Академией Информационных Систем – уже во второй раз в качестве площадки для проведения конференции сделали выбор в пользу гостиничного комплекса «Солнечный Park Hotel», инфраструктура которого в этом году удачно дополнилась комфортабельным SPA-корпусом и изумрудным бассейном. Гостеприимство, хорошие условия проживания и развитая инфраструктура гостиничного комплекса, радушие сотрудников и обслуживающего персонала, задор и талант аниматоров позволили сделать работу конференции более интересной и плодотворной, привлечь новых участников и заложить новые вехи развития «РусКрипто». ■