Таймлайн конференции

17 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

18 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 - 11:30	Официальное открытие конференции **Пленарное заседание** *Конференц-зал* *Подробнее на стр. 7*	
11:30 -12:00	Кофе-брейк	
12:00 – 13:30	**Круглый стол** **«Влияние проблемы импортозамещения на развитие средств криптографической защиты информации** *Конференц-зал* *Ведущий:* ***Кузьмин А.С.,*** *ФСБ России* *Подробнее на стр. 7*	**Секция** **«Продукты и технологии безопасности для мобильных платформ»** *Зал Марс* *Ведущий:* ***Горелов Д.Л., «****Актив»* *Подробнее на стр. 8*
13:30 -14:30	Обед	
14:30 - 16:30	**Секция** **«Электронный документооборот и электронная подпись. Диалоги»** *Конференц-зал* *Ведущие:* ▪ ***Маслов Ю.Г.,*** *«КРИПТО-ПРО»* ▪ ***Соловяненко Н.И.,*** *Институт государства и права РАН* ▪ ***Соловьев Н.Н.,*** *компания*	**Секция** **«Криптография и криптоанализ»** *Зал Марс* *Ведущие:* ▪ ***Кузьмин А.С.,*** *ФСБ России* ▪ ***Попов В.О.,*** *Ассоциация «РусКрипто», «КРИПТО-ПРО»* ▪ ***Жуков А.Е.,*** *Ассоциация*

	«Гроссмейстер» *Подробнее на стр. 9*	*«РусКрипто», МГТУ им. Баумана* *Подробнее на стр. 9*
16:30 -17:00	Кофе-брейк	
17:00 - 18:00	**Секция «Использование СКЗИ в банковской сфере»** *Конференц-зал* *Ведущие:* ▪ ***Левиев Д.О.,*** *НП ПСИБ* ▪ ***Репан Д.В.,*** *«БИФИТ»* *Подробнее на стр. 11*	**Секция «Криптография и криптоанализ»** *Зал Марс* Продолжение работы секции *Подробнее на стр. 9*
18:00 - 19:00	Блок вопросов и ответов «Частное мнение специалистов»	
19:30 - 20:30	Ужин	
19:30	Обратный трансфер м. Речной Вокзал	
21.00 - 23.00	Фуршет. Торжественное открытие конференции	

19 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 «Облака, технологии виртуализации и информационная безопасность»** *Конференц-зал* *Ведущие:* ▪ ***Фатеев О.А.,*** *IBS, RCCPA* ▪ ***Голов А.В.,*** *«Код Безопасности»* *Подробнее на стр. 12*	**Секция «Компьютерная криминалистика»** *Зал Марс* *Ведущий:* ***Чиликов А.А.,*** *МГТУ им. Н.Э. Баумана* *Подробнее на стр. 13*
11:30 – 12:00	Кофе-брейк	

Таймлайн конференции

12:00 -13:30	**Секция «Российские продукты для российского рынка»** *Конференц-зал* *Ведущий:* ***Белявский А.К.,*** *Zecurion* *Подробнее на стр. 14*		**Секция «Технологии создания безопасного программного обеспечения»** *Зал Марс* *Ведущие:* ▪ ***Проскурин В.Г.*** ▪ ***Аветисян А.И.,*** *ИСП РАН* *Подробнее на стр. 14*
13:30 – 14:30	Обед		
14:30 - 16:00	**Дискуссионная панель «Формирование отечественной отрасли информационной безопасности»** *Конференц-зал* *Ведущие:* ▪ ***Лукацкий А.В.,*** *Cisco Systems* ▪ ***Орешин М.С.,*** *НПО РусБИТех* *Подробнее на стр. 15*	**Секция «Кибербезопасность по сути вещей – от общих формальных моделей к практике»** *Зал Марс* *Ведущий:* ***Зегжда П. Д.,*** *СПбГПУ* *Подробнее на стр. 16*	**Мастер-класс «Реальная информационная безопасность предприятия»** *Зал Юпитер* *Ведущие:* ▪ ***Кропотов В.Б.,*** *Positive Technologies* ▪ ***Масалович А.И.,*** *АИС* *Подробнее на стр. 17*
16:00 - 16:30	Кофе-брейк		
16:30 – 19:00	**Секция «Аппаратные средства, технологии и криптография»** *Конференц-зал* *Ведущий:****Грунтович М.М.,*** *ЗАО«ОКБ САПР»* *Подробнее на стр. 17*	**Секция «Перспективные исследования в области кибербезопасности»** *Зал Марс* *Ведущий:* ***Котенко И.В.,*** *СПИИРАН* *Подробнее на стр. 18*	**Мастер-класс «Управление талантами»** *Зал Юпитер* *Ведущий:* ***Волков Д.,*** *“Сообщество «Success Insights» CIS”* *Подробнее на стр. 19*
19:00 – 19:30	Торжественное закрытие конференции *(Ресторанный комплекс)*		
19:30 –21:00	Ужин		
19:30	Обратный трансфер м. Речной Вокзал		

20 марта, пятница. День отъезда

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

Первый день работы конференции

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

Официальное открытие конференции

Приветственное слово

Кузьмин Алексей Сергеевич, *ФСБ России*

Перспективные задачи в области защиты информации

Баранов Александр Павлович, *д.ф-м.н., заместитель генерального директора, ГНИВЦ ФНС России*

Дайджест новостей мировой криптографии

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

Приветственные слова от спонсоров и партнеров конференции

12:00 – 13:30	**Круглый стол «Влияние проблемы импортозамещения на развитие средств криптографической защиты информации»** *Конференц-зал*

Ведущие:

- ***Кузьмин Алексей Сергеевич,*** *ФСБ России (по согласованию)*
- ***Лунин Анатолий Васильевич,*** *Технический комитет по стандартизации «Криптографическая защита информации» (ТК26), ОАО «ИнфоТеКС»*

Участники конференции приглашаются к обсуждению роли криптографических стандартов в импортозамещении. Понятно, что мы давно живем не в изолированном криптографически защищенном пространстве. Директивно ввести отечественные стандарты не везде возможно. Но с другой стороны идет навязывание российским потребителям техники под флагом совместимости с международными системами и выполнения международных рекомендаций. Возможный путь решения проблемы - гармонизация стандартов, но не за счет принятия международных стандартов, а за счет развития базы российских и придания им статуса международных. Это позволит производителям и потребителям совместно двигаться от стандартов - к унификации, от унификации - к борьбе с кризисом. Та же совместимость решений различных отечественных производителей через выполнение стандартов даст возможность российским потребителям экономить средства.

Единый стандарт ключевого носителя PKI. Миф или реальность?

Федотов Андрей Владимирович, *заместитель начальника отдела разработки и внедрения СЗИ департамента телекоммуникационных систем, ООО «Фактор-ТС»*

В докладе будет проведена оценка ранее сложившегося подхода в части использования разных форматов ключевых носителей разными разработчиками СКЗИ. Будут показаны недостатки сложившегося подхода, анонсированы методические рекомендации, разработанные в рамках работ, проводимых ТК26, предложена к использованию кроссплатформенная свободно распространяемая реализация PKCS#15.

Работы по стандартизации сопутствующих криптографических алгоритмов и криптографических протоколов

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

Рассматриваются вопросы стандартизации криптографических протоколов для обеспечения защищенной передачи конфиденциальной информации в сетях общего пользования, а также необходимых для их реализации сопутствующих криптографических алгоритмов на основе российских стандартов. Обсуждаются требования к виду документов по стандартизации в данной области, а также к сопровождающим документам, содержащим оценку качеств предлагаемых решений.

Не IPSec'ом едиными или о целесообразности наличия нескольких рекомендованных ТК26 VPN– протоколов в России

Уривский Алексей Викторович, *к.ф.-м.н., зам. начальника отдела по научно-исследовательским работам, «ИнфоТеКС»*

Импортозамещение, импортозависимость, криптоконверсия

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

В докладе будет рассмотрена роль требований регулятора к средствам криптографической защиты информации в условиях ограничений, вводимых ведущими IT - производителями на поставку в Россию IT – продуктов и технологий. Рассмотрена возможность и приведены примеры использования в криптосредствах доверенных программной и аппаратной компонент среды функционирования.

12:00 – 13:30 Секция «Продукты и технологии безопасности для мобильных платформ»

Зал Марс

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

Осознанная мобильность. От безопасности к доверию

Смирнов Николай Валерьевич, *руководитель отдела научных исследований и развития продуктов, «ИнфоТеКС»*

В докладе рассказывается об опыте компании в отношении создания продуктов ИБ под мобильные платформы, движению к продуктам высоких классов безопасности и доверенной мобильной платформе.

Защита мобильных объединенных коммуникаций

Альперович Михаил Моисеевич, *заместитель директора департамента Digital Design*

В докладе будет рассмотрена реализация системы объединенных коммуникаций (Unified Communications, UC) с обеспечением криптографической защиты информации сертифицированными средствами.

Облачная подпись и мобильные платформы

Смирнов Павел Владимирович, *к.т.н, зам. начальника отдела разработок, «КРИПТО-ПРО»*

Очень часто подпись в «облаке» — единственный способ использовать криптографию на мобильном устройстве. В докладе будет представлен обзор европейского рынка облачной ЭП и рассказано о требованиях по криптографической защите серверов электронной подписи с точки зрения документов, разработанных Европейским Комитетом по Стандартизации (CEN).

Традиционные средства криптографии и аутентификации на мобильных платформах

Иванов Владимир Евгеньевич, *директор по развитию , «Актив»*

Проверенные временем технологии и продукты, которые применяются на обычных компьютерах, очень сложно переносятся на мобильные платформы. То, что работает «из коробки» на ноутбуке, требует отдельного встраивания в операционную систему планшета или смартфона. По какому пути идут разработчики и каковы ожидания рынка. Какие возможности есть у заказчиков и интеграторов.

Эффективная мобильная безопасность для корпоративных пользователей – разговор на языке бизнеса

Широков Василий Васильевич, *заместитель генерального директора по развитию бизнеса, Check Point Software Technologies (Россия)*

Как сформировать мобильную бизнес-среду, которая обеспечит легкий, удобный, доступ к корпоративным данным, обеспечивая при этом их надлежащий уровень защиты? Как создать окружение, в котором мобильные менеджеры могли бы оперативно и безопасно обращаться из любой точки в любое время к корпоративным документам, файлам, другим ресурсам? Как обеспечить мобильный доступ к корпоративной почте, контактам, календарям, файлам, каталогам, бизнес-приложениям не перемешивая их с личными данными и приложениями?

14:30 – 16:30	**Секция «Электронный документооборот и электронная подпись. Диалоги»** *Конференц-зал*

Ведущие:

- ***Маслов Юрий Геннадьевич,*** *коммерческий директор, «КРИПТО-ПРО», эксперт НП «РОСЭУ»*
- ***Соловяненко Нина Ивановна,*** *старший научный сотрудник Института государства и права РАН*
- ***Соловьев Николай Николаевич****, советник генерального директора, компания «Гроссмейстер»*

Особенности электронного документооборота информации ограниченного доступа
Соловьев Николай Николаевич, *советник генерального директора, компания* «Гроссмейстер«

Длительное архивное хранение электронных документов: правовые особенности и технологические решения
Кирюшкин Сергей Анатольевич, *председатель комитета по тематике инфраструктуры открытых ключей, МОО "АЗИ"*

Применение российского законодательства об электронной подписи: нормы полезные и проблемные
Соловяненко Нина Ивановна, *старший научный сотрудник Института государства и права РАН*

Вопросы для обсуждения в режиме диалога между ведущими и аудиторией:

- Что далее делать с Федеральным законом об электронной подписи: развивать конструкцию (аккредитованных) удостоверяющих центров, развивать положения о видах электронной подписи, трансформировать в закон об электронном документе, отменить и разработать новый закон, отменить совсем?
- Финансовые требования при аккредитации удостоверяющего центра – эффективные или спорные?
- Какие изменения в законодательстве остро необходимы для электронного документооборота и есть ли такие?
- Какие конструкции необходимы в российском праве для трансграничного электронного документооборота; нужно ли их закреплять в законе или достаточно сложившейся практики?

14:30 - 19:00	**Секция «Криптография и криптоанализ»** *Зал Марс*

Ведущие:

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

Обзор результатов анализа хэш-функций ГОСТ Р 34.11-2012
Лавриков Иван Викторович, Маршалко Григорий Борисович, Шишкин Василий Алексеевич, *к. ф.-м. н.,* ***Рудской Владимир Игоревич,*** *ТК 26*
В докладе будет представлен обзор опубликованных к настоящему времени результатов криптографических исследований, а также исследований вопросов реализации хэш-функций, определяемых стандартом ГОСТ Р 34.11-2012, также известных как «Стрибог».

О подходах к синтезу режимов древовидного хэширования
Лавриков Иван Викторович, Маршалко Григорий Борисович, Шишкин Василий Алексеевич, *к. ф.-м. н., ТК 26*
В докладе будет представлен обзор существующих подходов к синтезу и обоснованию выбора параметров режимов древовидного хэширования.

О некоторых свойствах алгоритма выработки производных ключей CryptoPro Key Meshing

Миронкин Владимир Олегович, *Лаборатория ТВП*

В докладе рассматриваются некоторые теоретико-вероятностные характеристики отображения, определяемого алгоритмом выработки производных ключей CryptoPro Key Meshing, описанным в RFC 4357.

Об одном алгоритме развертки ключа из пароля

Нестеренко Алексей Юрьевич, *к.ф.-м.н., НИУ ВШЭ*

Предлагается алгоритм преобразования пароля в ключ, основанный на разложении некоторого иррационального числа, определяемого паролем пользователя, в заданной системе счисления.

Сравнительный обзор схем личностного шифрования, использующих билинейные отображения конечных групп

Гуселев Антон Михайлович, *ТК 26,* ***Косолапов Дмитрий Олегович,*** *к.ф.-м.н.,* ***ЕМС***

В докладе будет представлен набор характеристик для сравнения указанных в названии схем личностного (identity-based) шифрования и в терминах этих характеристик дан обзор наиболее популярных схем, в том числе, входящих в недавно принятый международный стандарт ISO/IEC 18033-5.

Построение ДСЧ на основе измерения времени доступа к оперативной памяти

Агафьин Сергей Сергеевич, *НИЯУ МИФИ*

В ряде случаев использование дополнительного оборудования для генерации случайных чисел может быть невозможно или избыточно в рамках применяемой модели нарушителя. Это приводит к потребности в датчиках, которые для функционирования использовали бы только штатное аппаратное обеспечение. Однако, существующие подобные ДСЧ обладают рядом недостатков: низкая скорость, слабая теоретическая база, узкая применимость. В докладе предложен новый подход к получению случайных чисел на x86-совместимых системах, который лишен большинства типичных недостатков. Представлено теоретическое обоснование возможности построения подобного датчика, приведены результаты тестирования статистических свойств реализации ДСЧ на операционных системах семейств Linux и Windows, а также представлены результаты некоторых исследований подверженности предлагаемого ДСЧ внешним влияниям.

О протоколах аутентифицированной выработки ключа на основе пароля

Смышляев Станислав Витальевич, *к.ф.-м.н., начальник отдела защиты информации, «КРИПТО-ПРО»*
Алексеев Евгений Константинович, *к.ф.-м.н., ведущий инженер-аналитик, «КРИПТО-ПРО»*

Доклад посвящен протоколам аутентифицированной выработки общего ключа с использованием малоэнтропийного общего секрета – пароля. Важной особенностью протоколов такого типа является дополнительное к стандартным требование об отсутствии у активного противника возможности получить критерий отбраковки пароля, который позволяет в дальнейшем найти пароль полным перебором без дополнительного взаимодействия с участниками. В докладе рассмотрены некоторые предложенные ранее протоколы такого типа, их особенности и известные уязвимости. Описан вариант такого протокола, предложенный авторами, с пояснениями, касающимися особенностей его построения. Описывается модель противника, в которой исследуется стойкость данного протокола. Приводятся полученные оценки и основные идеи доказательства.

Исследование статистических свойств выходных последовательностей функции сжатия алгоритма Стрибог

Любушкина Ирина Евгеньевна, *к.т.н., главный специалист, «АНКАД»*
Панасенко Сергей Петрович, *к.т.н., зам. директора по науке и системной интеграции, «АНКАД»*

В данной работе проводится анализ внутренней функции сжатия алгоритма Стрибог (ГОСТ Р 34.11-2012) на предмет ее вырождения при различных значениях входных данных. Целью анализа являлось изучение статистических свойств выходной последовательности функции сжатия и поиска групп неслучайных значений. Поиск «плохих» значений входных последовательностей, приводящих к регулярной неслучайности, проводился путем локального перебора всех возможных значений.

Советский суперкомпьютер К-340А и секретные вычисления

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

Под секретными вычислениями подразумевается обработка зашифрованных данных без их дешифрования. Есть

вариант компьютеров, основанных на системе остаточных классов (СОК) или в современных терминах на основе модулярной арифметики. Такие компьютеры разрабатывались в 50-70е годы прошлого столетия для создания РЛС. К ним относится суперкомпьютер К-340А и др. Все они основаны на модулярной арифметике. Особенностью данных компьютеров является очень высокий параллелизм, что позволяет делать вычисления в реальном времени. Недостатки – проверка выхода за диапазон данных, сравнение больше/меньше. С точки зрения разработчиков этих систем – "модулярная и двоичная арифметика несовместимы". Цель работы - построить систему полностью гомоморфного шифрования, которая бы имитировала этот класс вычислительных устройств.

О теоретико-автоматном подходе к эквивалентности ключей шифров

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

Для решения задачи определения классов эквивалентных ключей ряда шифров и расстояния единственности шифров иногда возможно использовать результаты теории автоматов по оценке степени различимости связного перестановочного автомата с заданным диаметром. В связи с чем в докладе анонсируются такие достижимые оценки.

Система криптографических стандартов Республики Беларусь

Шенец Николай Николаевич, *к.ф.-м.н., Санкт-Петербургский государственный политехнический университет*

Обзор государственных стандартов Республики Беларусь в области криптографической защиты информации. Рассказ о применении этих стандартов при построении республиканских систем защиты информации. Анализ стандартов, сравнение с российскими и международными стандартами в области криптографии.

Развитие матрично-графового подхода к оценке перемешивающих свойств композиций криптографических функций

Фомичев Владимир Михайлович, *д.ф.-м.н., профессор, Финансовый университет при Правительстве Российской Федерации, заместитель технического директора по науке, «Код Безопасности»*

Представленный матрично-графовый подход к изучению множеств существенных переменных основан на исследовании примитивности и экспонентов неотрицательных матриц и орграфов. Дан обзор результатов по различным классам матриц и графов.

О перемешивающих графах частного класса модифицированных аддитивных генераторов

Дорохова Алиса Михайловна, *«Криптология и дискретная математика», Кафедра 42, НИЯУ МИФИ,*

Доклад посвящен оценке экспонентов перемешивающих графов преобразований, соответствующих некоторым модификациям аддитивных генераторов.

Применение гомоморфного шифрования для построения криптосистемы с открытым ключом

Егорова Вера Владимировна, *магистрант,* ***Чечулина Дарья Константиновна,*** *магистрант, Новосибирский Государственный Университет, лаборатория Современных Компьютерных Технологий (ЛСКТ)*

Доклад посвящен методам построения систем шифрования с открытым ключом из систем с секретным ключом с помощью полностью гомоморфного шифрования.

17:00 – 19:00	**Секция «Использование СКЗИ в банковской сфере»** *Конференц-зал*

Ведущие: ***Левиев Дмитрий Олегович,*** *председатель совета членов НП ПСИБ*
Репан Димитрий Васильевич, *президент компании «БИФИТ»*

Переход на аппаратные средства СКЗИ для массового пользователя

Шилов Станислав Олегович, *директор по продажам, «БИФИТ»*

Вопросы жизненного цикла СКЗИ с поддержкой старых и новых ГОСТов. Учет ограничений реального сектора экономики

Левиев Дмитрий Олегович, *председатель совета членов НП ПСИБ*

Панельная дискуссия с участием ведущих экспертов отрасли

Второй день работы конференции

10:00 – 11:30	**Секция «Облака, технологии виртуализации и информационная безопасность»** *Конференц-зал*

Ведущий:
***Фатеев Олег Александрович**, директор по развитию бизнеса облачных вычислений IBS, президент, RCCPA (Russian Cloud Computing Professional Association)*
***Голов Андрей Викторович**, генеральный директор, «Код Безопасности»*

Системы информационной безопасности и технологии виртуализации

***Полянский Денис Евгеньевич**, менеджер продукта, «Код Безопасности»*
Особенности виртуализации с точки зрения информационной безопасности, какие специфические угрозы которые порождают данные технологии. Требования регуляторов. Существующие механизмы защиты сред виртуализации.

Российское сертифицированное средство виртуализации рабочих мест (VDI). Варианты практического использования

***Романченко Дмитрий Владимирович,** директор Центра технологий безопасности, IBS*
Рассказ о создании, сертификации и внедрении системы виртуализации рабочих мест. Рассмотрение вариантов практического использования. Интеграция в корпоративную инфраструктуру. Совместимость с российскими средствами криптографическими защиты каналов передачи информации.
Российские сертифицированные средства виртуализации.

VPN в облаках и не только

***Веселов Александр Геннадьевич,** начальник отдела технического консалтинга, «С-Терра СиЭсПи»*
Повсеместное применение виртуализации приводит к еще большей централизации ресурсов. А при таком подходе защищенный доступ к центральной точке - жизненная необходимость. Вслед за различными пользовательскими сервисами в виртуальную среду переходят средства защиты, которые ранее работали на отдельных аппаратных платформах. Такие перспективные новинки сочетают в себе надежную, проверенную временем защиту и преимущества виртуализации. В том числе есть прецедент сертификации подобного продукта в ФСБ России.

Защита информации в облаке за счет выделения критичных данных в отдельных безопасный сегмент

***Баркетов Павел Анатольевич**, технический директор, SOFTPOINT*
Большие, высоконагруженные системы предъявляют повышенные требования программным и аппаратным средствам. А если часть обрабатываемой информации необходимо защищать дополнительно, то сложность и стоимость решения может возрасти многократно. О подходах к решению данной проблемы пойдет речь в докладе.

Криптографические плагины для браузеров

***Смирнов Павел Владимирович,** к.т.н, зам. начальника отдела разработок, «КРИПТО-ПРО»*
Защищённый доступ к «облаку» и использование облачных сервисов подразумевают применение криптографии. Способов использования российских криптосредств в браузере не так много. Один из них – установка специального криптографического плагина. Поскольку веб является недоверенной средой, плагин должен не просто передавать вызовы криптосредству, но и обеспечивать надёжный барьер между средой обитания нарушителей и криптографическими ключами. Учитывают ли это разработчики плагинов?

10:00 – 11:30	**Секция «Компьютерная криминалистика»** *Зал Марс*

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

Криминалистический анализ RAM - обнаружение, расшифрование и интерпретация зашифрованных криптографических объектов и данных

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

Хоруженко Георгий Игоревич, *аспирант кафедры «Криптология и дискретная математика», НИЯУ МИФИ*

Получение доступа к данным, защищенным с помощью различных программных средств, является одной из самых сложных и актуальных задач цифровой криминалистики. Одним из возможных путей получения доступа к защищенным данным является получение образа RAM (live-memory analysis). В ряде случаев атаки в такой модели довольно просты, поскольку ключевая информация (пароли, ключи шифрования) доступна в образе RAM в открытом виде (в том или ином формате). Однако, ключевая информация доступна в открытом виде далеко не всегда и задача требует дополнительного изучения. Наша работа посвящена исследованию распространенных механизмов защиты данных в RAM и решению вышеуказанной задачи в случаях, когда ключевая информация защищена в памяти путем применения таких механизмов. В качестве примеров рассмотрен ряд популярных средств защиты (KeePass, WinRAR, 1Password).

Эволюция в защите данных Android-приложений

Карондеев Андрей Михайлович, *Oxygen Software*

Большинство разработчиков Android-приложений рано или поздно сталкиваются с необходимостью защиты данных. Защита данных наиболее востребована в приложениях типа «мессенджер», которые вынуждены хранить списки контактов и историю общения локально для обеспечения быстрого доступа к этим данным. Сейчас почти все современные Android-мессенджеры предоставляют различные функции для защиты истории переписки. В докладе демонстрируется эволюция механизмов защиты на примере Android-месенджеров.

Целевые атаки на банкоматы, способы совершения и способы обнаружения

Матвеева Веста Сергеевна, *ведущий специалист по компьютерной криминалистике, Group-IB, аспирантка кафедры «Криптология и дискретная математика», НИЯУ МИФИ*

В России зафиксированы атаки на двух производителей банкоматов NCR и Wincor. Используются разные подходы, которые нацелены на хищение средств со счета банка, не владельцев карт. В рамках доклада будут рассказаны способы их совершения и обнаружения следов таких атак в системах. Отдельно будет освещен вопрос кражи данных с пластиковых карт с магнитной полосой без дополнительных накладных устройств на банкомат.

Расследование инцидентов, связанных с мобильными бот-сетями и вредоносным ПО

Гончаров Николай Олегович, Горчаков Денис Сергеевич, *МГТУ им. Н.Э. Баумана*

Мобильные зловреды стали настоящей проблемой крупных банков и платёжных систем. Зона ответственности за противодействие мобильному мошенничеству плавно размывается между операторами связи и финансовыми учреждениями. Для автоматизации процесса расследования данного рода инцидентов было разработано решение, позволяющее отслеживать активность вредоносного ПО, фиксировать попытки отправки данных мошенникам, выявлять центры управления заражёнными устройствами, а также счета, номера, кошельки и аккаунты, через которые выводятся украденные средства. Удаётся на раннем этапе обнаружить новые, только формирующиеся бот-сети, нарушить их работу и заблокировать вывод средств. Будет рассказано об опыте использования данного решения в расследовании инцидентов.

12:00 – 13:30	**Секция «Российские продукты для российского рынка»** *Конференц-зал*

Ведущий: ***Белявский Александр Константинович****, коммерческий директор, Zecurion*

Что должна уметь современная система мониторинга событий

Юдин Алексей Анатольевич, *директор по корпоративным продуктам, Positive Technologies*

Мониторинг событий безопасности в современной ИТ системе - задача довольно непростая. Огромное количество событий, сложные цепочки корреляций, трудности в настройке - все это делает внедрение SIEM систем сложным и малоэффективным. В своем докладе мы расскажем о том, какие задачи должна уметь решать современная SIEM система, чтобы процесс мониторинга событий приносил реальную пользу специалисту по ИБ.

Функционал Microsoft TMG, как самостоятельное решение в линейке DLP-вендора

Подкопаев Роман Игоревич, *вице-президент по России и СНГ, Zecurion*

Чем заменить «незаменимые» Microsoft Forefront TMG и ISA Server? Есть ли российские разработчики качественных прокси-серверов и полноценных UTM-решений? Какая практика миграции существует в мире? Что необходимо учитывать, переходя с Microsoft TMG на другой продукт? Как Zecurion UTM позволит мигрировать с Microsoft TMG и чем полезна интеграция с DLP?

Построение инфраструктуры доверия в системах электронного документооборота

Макеев Максим Станиславович, *«Газинформсервис»*

В докладе рассматриваются вопросы применения службы Доверенной третьей стороны в прикладных системах документооборота. Предлагаются варианты построения системы юридически-значимого документооборота, создаваемого в условиях ограничения возможностей применения сертифицированных СКЗИ.

Защита графических копий документов с применением систем защищенной печати

Хурцилава Тимур Вахтангович, *директор департамента внедрения и обслуживания комплексных систем безопасности, «НИИ СОКБ»*

Контроль распространения копий документов как в электронном виде, так и на бумажных носителях, остается актуальной задачей. Доклад посвящен описанию методов и способов скрытой маркировки копий защищаемых документов, а также их реализации в системах электронного документооборота.

12:00 – 13:30	**Секция «Технологии создания безопасного программного обеспечения»** *Зал Марс*

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*

Модули для инструментирования исполняемого кода в симуляторе QEMU

Васильев Иван Александрович*, Новгородский государственный университет имени Ярослава Мудрого*

Представлен механизм подключаемых модулей для симулятора QEMU для инструментирования исполняемого кода. Механизм инструментирования позволяет выполнять анализ производительности или поиск ошибок в коде, выполняемом в виртуальной машине. В отличие от распространенных систем, подключаемые к симулятору модули могут выполнять инструментирование системного кода, в том числе компонентов операционной системы.

Применение программных эмуляторов для полносистемного анализа бинарного кода мобильных платформ

Падарян Вартан Андроникович, *Институт системного программирования РАН*

В своем развитии мобильные платформы сблизились с настольными компьютерами не только в производительности, но и в устройстве программного обеспечения. Это позволяет рассматривать вопрос адаптации к особенностям мобильных платформ хорошо себя зарекомендовавших методов анализа ПО настольных компьютеров и серверов. Комбинированный метод анализа бинарного кода может выявлять утечку чувствительных данных, рассматривая всю совокупность развернутого на компьютере ПО. Для переноса этого метода требуется решить задачу получения необходимых для анализа динамических данных, а именно - трасс выполнения машинного кода. В докладе будут рассмотрены сложности, возникающие при запуске прошивок мобильных устройств на программных эмуляторах с целью получения трасс выполнения, а также показаны возможные пути преодоления этих сложностей.

Дедуктивная верификация системы защиты информации ОС Astra Linux

Девянин Петр Николаевич, *УМО ИБ*

Система защиты информации (СЗИ) операционной системы специального назначения ОС Astra Linux Special Edition строится на основе концепции модуля информационной безопасности (Linux Security Module - LSM). Требования к СЗИ формулируются в виде формальной мандатно-сущностно-ролевой ДП-модели (МРОСЛ ДП-модели), которая описывается в нотации Event-B и верифицируется при помощи инструмента Rodin. Требования к интерфейсам модуля LSM описываются на спецификационном расширении языка Си ACSL, а реализация модуля безопасности верифицируется при помощи инструментов Frama-C/Why-3. Наиболее сложной частью проекта является разработка спецификации и верификация модуля LSM. Верификация модуля ядра операционной системы требует расширения функциональности существующих инструментов дедуктивной верификации Frama-C/Why-3, в частности, требуется реализация новых возможностей по спецификации и верификации программ, активно использующих адресную арифметику и работающих с данными, разделяемыми между несколькими потоками управления. В докладе будут описаны текущие результаты проекта и представлена модифицированная цепочка инструментов дедуктивной верификации, учитывающая специфику модулей ядра ОС Linux.

Методы и инструменты для статического и динамического анализа программного обеспечения

Дрозд Юрий Анатольевич, *начальник испытательной лаборатории, «Газинформсервис»*

В докладе рассматриваются возможности инструментов технологии Ирида при решении задач поиска скрытых дефектов (недокументированных возможностей) в условиях отсутствия исходных текстов программ. Предлагаются методы паспортизации программ на основе автоматных лингвистических моделей.

14:30 – 16:00 **Дискуссионная панель «Формирование отечественной отрасли информационной безопасности»**

Конференц-зал

Санкции, введенные против России, уже оказывают существенное влияние на рынок информационных технологий. Наиболее сильно это ощущается в проектах в области безопасности. Санкции настойчиво подталкивают бизнес и государство к построению полноценной, независимой отрасли информационной безопасности. Как должны действовать участники этого процесса? Когда необходимо жесткое регулирование, а где нужно использовать в основном рыночные механизмы? Какие практики и чей опыт могут быть полезны? Где грань между отечественным и международным?

В обсуждении примут участие эксперты, условно поделенные на два лагеря. За патриотическую линию будет отвечать Михаил Орешин, заместитель генерального директора НПО РусБИТех, а оппонировать ему будет известный специалист по информационной безопасности Алексей Лукацкий.

14:30 – 16:00	**Секция «Кибербезопасность по сути вещей – от общих формальных моделей к практике»** *Зал Марс*

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

Разработка процессора с безопасной архитектурой — путь к решению проблемы уязвимости программного обеспечения
Москвин Дмитрий Андреевич, *к.т.н., доц., руководитель проектов, «НеоБИТ»*

Универсальная отечественная платформа обеспечения безопасности распределенных информационно-телекоммуникационных систем
Коноплев Артем Станиславович, *к.т.н., доц., руководитель проектов, «НеоБИТ»*

Моделирование безопасности Интернета вещей с помощью адаптивных графов
Зегжда Дмитрий Петрович, *д.т.н., профессор кафедры «Информационная безопасность компьютерных систем», СПБГПУ*

Выявление инцидентов безопасности в Интернете вещей
Лаврова Дарья Сергеевна, *аспирант кафедры «Информационная безопасность компьютерных систем », СПбГПУ*

Контроль доступа к рабочим станциям в контексте Интернета вещей
Беззатеев Сергей Валентинович, *д.т.н., профессор, заведующий кафедрой технологий защиты информации, Санкт-Петербургский государственный университет аэрокосмического приборостроения*

Подход к построению обобщенной модели кибербезопасности
Зегжда Петр Дмитриевич*, профессор, д.т.н., Заслуженный деятель науки РФ, зав. кафедрой «Информационная безопасность компьютерных систем», СПбГПУ*

Стендовые доклады:

Некоторые применения решеток для построения криптографических примитивов
Александрова Елена Борисовна, *к.т.н., профессор кафедры «Информационная безопасность компьютерных систем», СПБГПУ*

Применение методов решения задач точного покрытия для поиска уязвимостей программного обеспечения
Селянин Денис Евгеньевич, *аспирант кафедры «Информационная безопасность компьютерных систем», СПбГПУ*

14:30 – 16:00	**Мастер-класс «Реальная информационная безопасность предприятия»** *Зал Юпитер*

Ведущие:

- ***Кропотов Владимир Борисович,*** *руководитель отдела мониторинга, Positive Technologies*
- ***Масалович Андрей Игоревич,*** *ведущий эксперт по конкурентной разведке, Академия Информационных Систем*

Как сделать так, чтобы инфраструктура вашей компании была более безопасной. Какие опасности подстерегают и как против них бороться. Как быть более защищенным в наш цифровой век. Советы практиков.
Простые и эффективные приемы, с помощью которых хакер и интернет-разведчик сможет добраться до вашей конфиденциальной информации, например: экспресс-сканирование уязвимостей, перехват паролей, атаки на CMS, Google Hack, Google Dork, инъекции и пр.

16:30 – 19:00	**Секция «Аппаратные средства, технологии и криптография»** *Конференц-зал*

Ведущий: ***Грунтович Михаил Михайлович,*** *руководитель обособленного подразделения в городе Пензе, «ОКБ САПР»*

Проблемы обеспечения информационной безопасности в системах промышленной автоматизации

Крутиков Алексей Олегович, руководитель направления, «Инсайд РУС»

В докладе рассматриваются проблемы в области информационной безопасности, возникающие в ходе развития современных систем промышленной автоматизации и методы их решения с использованием устройств, соответствующих нормам и стандартам, принятым в области промышленной автоматизации.

Новый качественный уровень отечественных СКЗИ как результат политики импортозамещения в сфере информационной безопасности и защиты данных

Кожемякин Никита Михайлович, *директор по развитию бизнеса, Группа компаний ISBC*
Вараксин Денис Владимирович, *директор по маркетингу ОАО «НИИМЭ и Микрон»*
Группа компаний ISBC и ОАО «НИИМЭ и Микрон» запускают новую линейку СКЗИ ESMART Token ГОСТ на базе отечественного микрочипа. Об особенностях и ключевых характеристиках СКЗИ расскажут докладчики.

Эффективная реализация стандарта ГОСТ Р 34.11-2012 на 16-битных микроконтроллерах

Кролевецкий Алексей Владимирович, *ведущий специалист отдела перспективных разработок, «Код Безопасности»*
Об оптимизация алгоритма ГОСТ Р 34.11-2012 для устройств с малой памятью и малой разрядностью. Небольшой объем памяти делает затруднительным реализацию алгоритма ГОСТ Р 34.11-2012 с помощью предрасчетных таблиц, а малая разрядность увеличивает число операций при реализации согласно тексту стандарта. В докладе будет рассказано о методах оптимизации и достигнутых результатах.

Особенности криптографических протоколов и инфраструктуры расширенного контроля доступа к данным и функциям удостоверения личности гражданина Российской Федерации

Мелузов Антон Сергеевич, *заместитель руководителя департамента информационной безопасности, ФГУП НИИ«Восход»*
В докладе описываются особенности организации защиты информации и контроля доступа к данным и функциям бесконтактной микросхемы, применяемой в удостоверении личности гражданина России. Рассмотрены криптографические протоколы и структуры данных, используемые при взаимодействии терминалов и бесконтактных микросхем УЛГ, описаны отличия внутренней структуры и механизмов работы российских УЛГ и зарубежных eID. Кратко изложен поход к обоснованию стойкости протоколов.

Реализация доверенной среды для мобильных устройств на базе стандартов Trusted Execution Environment и Secure Element

Дударев Михаил Игоревич, *технический консультант, Global Platform, автор проекта jCardSim (jcardsim.org)*

Рассказ о стандарте Trusted Execution Environment, об архитектуре Secure Element и ее реализации на платформе Java Card. Архитектура Secure Element и технология NFC. Что такое Android HCE и его применение. Samsung Knox как пример реализации доверенной среды - плюсы и минусы.

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

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

Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами

Котенко Игорь Витальевич, *д.т.н., профессор, лаборатория проблем компьютерной безопасности, СПИИРАН,* ***Новикова Евгения Сергеевна,*** *к.т.н., СПбГЭТУ«ЛЭТИ»,* ***Архипов Юрий Анатольевич,*** *ЗАО «НПП «ТЕЛДА»*
Предлагается методика визуальной аналитики для отображения множества метрик безопасности, используемых для оценки защищенности и оценки эффективности механизмов защиты в больших компьютерных сетях. Рассматривается реализованный прототип системы визуальной аналитики, предназначенный для мониторинга безопасности и управления инцидентами.

Проблемы обнаружения логических уязвимостей в современных веб-приложениях

Раздобаров Александр Вячеславович, Гамаюнов Денис Юрьевич, *к.ф.-м.н., с.н.с., лаборатория интеллектуальных систем кибербезопасности факультета ВМК, МГУ имени М.В.Ломоносова*
Рассматривается проблема анализа веб-приложений, построенных с использованием современных динамических технологий HTML5, JavaScript, AJAX и подобных, с целью обнаружения сложных логических ошибок этапа проектирования.

Формирование экспертных знаний для разработки защищенных систем «Интернета вещей»

Бушуев Сергей Николаевич, *д.т.н., профессор, ЗАО «НПП «ТЕЛДА»*
Десницкий Василий Алексеевич, *к.т.н., лаборатория проблем компьютерной безопасности, СПИИРАН*
Представляется проблема анализа знаний в области безопасности информационно-телекоммуникационных систем, отличающихся разнородностью входящих в них устройств, структурно-функциональными особенностями и специфичным набором угроз информационной безопасности. Конкретные экспертные знания, выявленные при анализе систем концепции «Интернет вещей», используются в качестве основы для разработки специализированных методик и программных средств проектирования компонентов защиты для таких систем.

Моделирование аспектов функционирования веб-приложений в контексте задачи обнаружения атак

Носеевич Георгий Максимович, *SolidLab*
Сформирован список уровней рассмотрения и аспектов функционирования веб-приложений, моделирование которых необходимо для поиска всего спектра аномалий взаимодействия между веб-приложением и его клиентами. Приведены примеры формализмов, пригодных для моделирования. Указанные виды математических моделей допускают автоматическое построение на основе нормального трафика.

Подход к выявлению потенциально опасных дефектов в спецификациях документов, регламентирующих порядок создания и сертификации средств защиты информации

Бирюков Денис Николаевич, *к.т.н.,* ***Ломако Александр Григорьевич,*** *д.т.н., профессор,* ***Еремеев Михаил Алексеевич,*** *д.т.н., профессор,* ***Мажников Павел Викторович,*** *к.т.н., доцент, Военно-Космическая академия имени А.Ф.Можайского*
Рассматривается основные аспекты технологии, позволяющей формализовать спецификации документов с требованиями к средствам информационной безопасности на основе онтологических моделей, производить семантическое пополнение онтологий ролевыми связями понятий, порождать спецификации потенциально возможных

проектов искомых средств информационной безопасности и осуществлять верификацию потенциально опасных дефектов в спецификациях.

Корреляция данных безопасности в сетях «Интернет вещей»

Смирнов Дмитрий Борисович, *ЗАО «НПП «ТЕЛДА»*
Чечулин Андрей Алексеевич, *к.т.н., лаборатория проблем компьютерной безопасности, СПИИРАН*
Проводится анализ различных методик корреляции данных безопасности, разработанных для мониторинга сетевого трафика, оценки политик безопасности и уровня защищенности сетей «Интернета вещей». Рассматриваются основные ограничения, накладываемые предметной областью на процессы обработки данных.

Фильтры обработки входных данных как источники уязвимостей

Порхун Анастасия Олеговна, *лаборатория безопасности информационных систем, факультет ВМК, МГУ имени М. В. Ломоносова*
Представляется проблема обнаружения специального класса уязвимостей веб-приложений, которые обусловлены ошибками в реализации или использовании фильтров обработки входных данных, при которых специально сформированные валидные данные (например, картинки, видеоролики) после фильтрации могут быть преобразованы в нужный злоумышленнику вид, например, в исполнимый код.

Построение нейросетевой и иммуноклеточной системы обнаружения вторжений

Браницкий Александр Александрович, *лаборатория проблем компьютерной безопасности, СПИИРАН*
Полушин Владимир Юрьевич, *к.т.н., доцент, ЗАО «НПП «ТЕЛДА»*
Рассматриваются методы обнаружения и классификации аномальных образцов сетевых соединений с использованием аппарата искусственных нейронных сетей и эволюционной модели иммунной системы. Представляется архитектура системы обнаружения вторжений, основанная на применении предложенных подходов. Демонстрируются результаты вычислительных экспериментов, показывающих эффективность выбранных методов с учетом показателей ложных срабатываний, корректности обнаружения и классификации атак.

16:30 – 19:00 **Мастер-класс «Управление талантами»**
Зал Юпитер

Ведущий: ***Волков Денис,*** *президент профессионального сообщества, объединяющего специалистов в сфере управления талантами – "Сообщество «Success Insights» CIS"; заместитель руководителя программ магистерской подготовки и MBA по направлению «ИТ-консалтинг», Доцент кафедры Управления знаниями и прикладной информатики в менеджменте, Институт компьютерных технологий МЭСИ.*

Каждый владелец, руководитель успешной ИТ-компании подтвердит, что талантливые сотрудники - это главный капитал любой процветающей организации. Без высококвалифицированных, одаренных и стремящихся к дальнейшему развитию талантливых людей любая организация обречена на постепенное угасание и неминуемую смерть. Как привлекать, нанимать и мотивировать к эффективной работе талантливых специалистов? Какой должна быть организация и ее руководители, чтоб лучшие кадры работали именно в ней?