Более 350 экспертов собрались на **X Юбилейном межотраслевом Форуме CISO FORUM 2017: Суровые будни CISO**, который прошел 17-18 апреля 2017 г. в DoubleTree by Hilton Moscow. Организатор мероприятия – компания **infor-media Russia**, спонсорами мероприятия стали ГК ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ (Бренд Security Vision) – Золотой партнер; Cisco – Стратегический партнер; «Лаборатория Касперского», Компания Вэб Контрол, Imperva SecureSphere, Palo Alto Networks, Fortinet, ИНФОРМЗАЩИТА, Check Point Softwear Technologies Ltd. – Официальные партнеры; ESET, FireEye, АО ДиалогНаука, ООО «Новые технологии безопасности, Cross Technologies, Акрибия, ООО «Микролап Текнолоджис», КРОК, Mobile Cat – партнеры; Аванпост, ООО «Научно-испытательный институт систем обеспечения комплексной безопасности» – Партнеры технологической сессии; Solar Security – партнер бизнес-потока; ЗАО «Национальный удостоверяющий центр», ООО «Р-Вижн», Тайгер Оптикс, Tenable Network Security – участники выставки.

CISO форум открыла пленарная дискуссионная панель «Информационная безопасность: вчера, сегодня, завтра. Взгляд CISO на основные перспективы и тренды ИБ в России». Модератором панели выступил **Евгений Климов**, НИП «Информзащита». Эксперты подняли вопрос эволюции ИБ в России за последние 10 лет, обсудили тренды в области угроз, экономики и ИТ, рассмотрели развитие отраслевых стандартов в области ИБ и стратегии повышения эффективности работы служб информационной безопасности.

Роман Попов, «Транснефть», склонен к классической системе защиты. «Нужно спать спокойно и работать спокойно. Важно 100% видеть, но не 100% защищать, потому что это невозможно» - отметил Роман. **Сергей Ходаков**, Сколково, рассказал, что 1-2 проекта приходят в Сколково ежемесячно и основные тренды на данный момент – это аналитика и мониторинг. Независимый эксперт **Алексей Лукацкий** отметил, как важно найти баланс между требованиями регуляторов и маленькими компаниями. Сейчас сертификация проводится так долго, что часто на рынок выходят программы, сертифицированные, но уже не выпускающиеся. Основными трендами Алексей назвал аутсорсинг; безопасность из облака; безопасность облака и комплаенс: государство закручивает гайки по всем направлениям. **Сергей Демидов**, «Московская Биржа», сделал акцент на плотной работе с регулятором, в ходе которой постоянно делаются попытки найти совместные решения. Сергей призвал всех работать с регулятором, чтобы со временем изменить мир. А среди современных трендов назвал кадровый голод и изменения в системе образования; интеграцию взаимодействия IT и CISO; BigData и Machine Learning. **Алексей Волков**, Сбербанк, отметил, что главный банк страны постоянно отслеживает интересные проекты российских и иностранных компаний с целью внедрения. «Продукты есть. Нет внедренцев этих продуктов» - сказал Алексей. И есть большая нехватка кадров. Сбербанк в последнее время не только сотрудничает с ВУЗами, но и сам готовит кадры, а в 2016 году открылась собственная академия. «Важно создать сотрудникам такие условия работы, чтобы человек сам хотел работать, а не искать новое место работы», - подчеркнул Алексей. **Сергей Трушкин**, «РусАл», был солидарен с коллегами и его ТОП-5 трендов на данным момент стали конвергенция АСУТП; Digital; BigData; рост доли рынка аутсорсинга и повышения образования ИБ специалистов.

Программу продолжила практическая сессия «Лучшие практики и главные тенденции в защите информации» и **Олег Демидов**, ПИР-ЦЕНТР, с докладом «ИБ, международная безопасность и стратегическая стабильность: итоги-2016 и прогнозы на будущее». Олег сделал акцент на том, что в каждой стране свои термины и нет общей терминологии, из-за чего сильно затягивается подписание договоров. Олег поднял тему международного противодействия киберпреступности и рассказал об инициативах частных игроков. **Александр Леонов**, Mail.ru, в продолжение сессии рассмотрел различные типы уязвимостей и подходы к ним. «Во всех подходах есть свои достоинства и недостатки. Непросто разобраться, критична уязвимость или нет, особенно в начале, когда мало информации», - отметил Александр.

Далее слушатели разделились на три потока: организационный, технологический и бизнес-поток. В бизнес-потоке «CISO на страже бизнеса» независимый эксперт **Рустэм Хайретдинов** провел мастер-класс «Создание и внедрение корпоративных правил. Сила обратной связи», в ходе которого рассказал, какие правила легче выполняются: пассивные (не делать), требующие небольшого изменения поведения, одинаковые для всех из ближнего круга, логически обоснованные. Рустэм представил принципы формирования привычек: четкие требования (все регламенты и инструкции должны быть доведены до каждого сотрудника), независимый контроль (легализованные технические меры), обратная связь (конкретные наказания за конкретные нарушения).

В технологическом потоке «Ноу-хау в области информационной безопасности. Лучшие кейсы и практические рекомендации от ведущих экспертов рынка» **Федор Горловский**, ГК «Интеллектуальная безопасность», и **Олег Бакшинский**, IBM Россия и СНГ, представили мастер-класс «Security Vision: управляй безопасностью», где осветили вопросы управления процессами информационной безопасности, риски ИБ и контроль за ними, а также поделились опытом построение ситуационных центров и раскрыли секреты возможной экономии через автоматизацию системы безопасности. «За 2016 год было украдено более 4 млрд записей персональных данных и это больше, чем за 2 предыдущих года. Атаки стали более эффективными, - подчеркнул Олег, - нет системы, которую нельзя было бы взломать».

В рамках организационного потока «Организация работы ИБ-департамента» **Наиль Айнетдинов**, TELE2, представил case-study «Полезные находки и зачем организациям смотреть на себя извне». Наиль поделился секретами, как использовать именные учетные записи и поисковики, как извлечь информацию из документов, выложенных в открытый доступ, из тематических ресурсов, как найти информацию о сотрудниках в СМИ. **Дмитрий Устюжанин**, ГК Мегаполис, напомнил делегатам, что существует огромное количество самых различных угроз, которые обязательно нужно делить на подкатегории: известные, неизвестные, скрытые, внутренние. Работать необходимо с каждой подкатегорий отдельно. «Важно найти баланс и быть адекватным. Это каждый должен решить сам. Нужно понимать, что все равно где-то ты будешь пропускать удар, но это не значит, что не нужно внедрять программы ИБ», - заключил Дмитрий.

Александр Шахлевич, Imperva, в своем выступлении напомнил, что информация уже далеко вышла за периметр организации и может храниться на внешних носителях, на мобильных устройствах и т.д. «Невозможно достичь 100% защищенности, поэтому нужно правильно расставить приоритеты», - сказал Александр.

Андрей Конусов, «Аванпост», выступил модератором практической сессии «Глазами бизнеса», в ходе которой независимый эксперт **Андрей Коротков** представил case-study «Безопасность глазами владельца бизнеса». Андрей раскрыл тему ожиданий бизнеса от информационной безопасности и рассказал о том, что не все риски одинаково бесполезны. **Виктор Ивановский**, Solar Security, в своем докладе «Дальше не придумали, импровизируй, или можно ли применить Agile к информационной безопасности» представил action plan: профиль рисков, эффективность мер, выявление проблем, создание плана. Виктор рассмотрел проекцию Agile на информационную безопасность и подчеркнул, что Agile не является универсальным методом, но работает там, где нужно быстро принимать решения. **Александр Севостьянов**, ТМК, в своем case-study «Ключевые проблемы построения информационной безопасности в иерархических организационных структурах» рассмотрел основные характеристики и особенности организаций, построенных на различных моделях, а также факторы, негативно влияющие на развитие ИБ в иерархической организации. От **Алексея Ермаченкова**, «Моспроект-3», делегаты узнали, как правильно обосновать свои потребности в ресурсах и в дальнейшем показать результаты от их использования. Также Алексей рассмотрел, почему в разных ситуациях лучше выбрать тот или иной вариант защиты и как убедиться, что защита работает. В заключение сессии **Ольга Теплоухова**, «Акрибия», представила доклад на тему «Риски информационной безопасности и методы обеспечения конфиденциальности персональных данных в рамках программы лояльности», в котором отметила, что многие сегменты рынка IT услуг демонстрируют незрелость в вопросах защиты информации. При этом внешние аудиты безопасности – это эффективный инструмент управления взаимоотношениями с контрагентами, а рассмотренная практика работы с контрагентами позволяет существенно снизить риски безопасности ПДн.

В практической сессии «Безопасность: мифы и реальность» **Андрей Акинин**, Web Control, развеял иллюзии защищенности и реальности web-безопасности: почему UTM не является панацеей и что лучше выбрать URL-категоризацию или анализ репутации. **Евгений Бударин**, Kaspersky Lab Russia, выступил с темой «Актуальная защита там, где просто антивируса недостаточно» «300000 новых вопросов возникает каждый день. Как выявить тот 1% атак, которые нужно далее расследовать? – спросил Евгений. Очень часто в практике приходится сталкиваться с отсутствием реагирования.

Евгений привёл реальные случаи из практики (случайно заражённая машина, случай с битым вложением, LiteManager) и рассмотрел, как развитие целенаправленной атаки отличается в теории и реальности.

Павел Таратынов, **Амир Алиев**, НИП "Информзащита", **Алексей Белоглазов**, Check Point Softwear, и независимый эксперт **Юлия Омельяненко** приняли участие в мастер-классе "Защита от APT и неизвестных угроз". Павел Таратынов озвучил цифру в 450 млн в год долларов - ущерб, который наносят всему миру кибератаки. В массовых атаках на финансовую отрасль в 2016 году пострадали 104 организации в 31 стране. Юлия Омельяненко рассмотрела виды Ransomware. Ransomware сложно уничтожить, т.к. воздействие идёт непосредственно на данные. Все чаще директорам по информационной безопасности приходится сталкиваться с ситуациями, когда вирус попадает на компьютер, зашифровывает все данные и преступники сразу присылают письмо с предложением получить ключ к зашифрованной информации за деньги. Амир Алиев на конкретных примерах разобрал, как может действовать защита: определяет угрозу, восстанавливает зашифрованные файлы, готовит отчёт. Алексей Белоглазов рассмотрел различные сценарии атак и цепочки взаимосвязанных процессов. Основная идея, обозначил Алексей, предотвращать все, что только можно, если не успели предотвратить, сразу начать расследовать.

Мастер-класс **Михаила Емельянникова**, "Емельянников, Попова и партнеры", "Персональные данные в судах: LinkedIn, Скартел и другие" вызвал так много вопросов, что долгое время после его завершения слушатели не отпускали Михаила. Делегаты узнали, можно ли обезличенные данные посетителей сайтов передавать или продавать иным лицам и сколько согласий в письменной форме надо получать у сотрудника, чтобы выполнить установленные требования. **Константин Коротнев**, "Газпром газэнергосеть", на своём мастер-классе "Управление рисками информационной безопасности" подчеркнул, что общая цель ИБ - снижение рисков, обеспечение соответствия, организация процессов ИБ. Развитие информационной безопасности состоит в интеграция ИБ в корпоративную культуру, минимизация затрат на ИБ и повышение эффективности и прозрачности ИБ. "Риск - это комбинация вероятности и ущерба," - напомнил Константин, поэтому крайне важно заниматься анализом рисков и сравнением событий.

Дмитрий Мананников, SPSR express, провел мастер-класс "Безопасность как бизнес-функция", в котором рассмотрел субъекты бизнеса и их цели. "Может ли бизнес достигать несколько целей? - спросил у слушателей Дмитрий. Бизнес часто ставит основной целью увеличение прибыли или сокращение расходов, но всегда ли цели бизнеса совпадают с целями службы безопасности? Каждую цель нужно разобрать на измеримые показатели и далее вести управление по целям.

Независимый эксперт **Алексей Лукацкий** собрал самую большую аудиторию своим мастер-классом "Процесс организации борьбы с фишингом". Алексей рассказал об использовании фальшивых доменов и URL crazy и привёл яркий пример Сбербанка, у которого на данный момент более 80 фальшивых доменов, большая часть которых вредоносные. Неправильные ссылки вставляются в сообщения и несут вредоносный код. Таким образом собираются логины и пароли. Злоумышленники могут использовать схожие символы (например, буква О и цифра 0). В заключение мастер-класса Алексей на примере сайта CISO форума показал, как в несколько кликов клонировать сайт.

Александр Санин, "Аванпост", в своём мастер-классе "Аутентификация и IDP - как готовить, чтобы было вкусно» поделился опытом построения системы, которая облегчит жизнь пользователям, если они не любят заводить много разных паролей, и подчеркнул, что подобные системы работают на разных количествах пользователей. **Роман Ванерке**, "ДиалогНаука", и **Станислав Павлунин**, "Тинькофф Банк", провели мастер-класс "Реализация защиты от APT в банке "Тинькофф". В 2015 году объём ущерба от атак составил 70 млн рублей. Атакуют все организации, но атаки именно на банки приносят наибольшую выгоду: деньги или персональные данные клиентов. Станислав Павлунин рассказал: до 3-4 атак в банке "Тинькофф" детектируют каждую неделю.

Первый день CISO форума завершился интересной культурной программой, в ходе которой делегаты смогли не только пообщаться друг с другом, но и задать спикерам вопросы, которые не успели озвучить во время заседаний.

Олег Седов, BISA, в качестве модератора открыл круглый стол "ИБ-служба моей мечты. Внутренняя кухня или безопасность у безопасника. Практическая составляющая роли и задач современного руководителя ИБ в структуре управления компании" утром 18 апреля. В начале круглого стола эксперты говорили об изменениях, произошедших в службе безопасности за последнее время. **Александр Виноградов**, КБ "Златкомбанк", отметил, что за последние 10 лет информационная безопасность в банковской сфере очень выросла.

Артём Воробьев, BAYER, рассказал, как сильно изменилась жизнь службы безопасности в компании BAYER за последние год: была внедрена система внутреннего контроля, произошёл значительный скачок в digital pharming. **Дмитрий Фролов**, Банк России, сделал акцент на том, что в 2013-2014 годах произошёл большой всплеск количества киберугроз по всему миру. Что касается банковской сферы в России, киберугрозы все больше входят в повседневную жизнь сотрудников безопасности, поэтому необходимо внедрить стратегический подход и найти грамотное сочетание бизнеса и

информационной безопасности. **Антон Иванов**, Сколково, поделился со слушателями, как сэкономить на ИБ и рассказал о создании сервисов в ИБ. Антон подчеркнул, что в последние годы все стали искать новые решения и вспомнили про стартапы. На вопрос "Как выглядит регулятор моей мечты?" **Дмитрий Устюжанин**, ГК Мегаполис, ответил, что о регуляторе трудно думать в положительном ключе, потому что он часто заставляет заниматься информационной безопасностью на бумаге в ущерб реальной работе. Поэтому регулятора мечты просто не существует. **Кирилл Мартыненко**, "Сбербанк", также отметил, что за последние несколько лет Сбербанка сильно изменился. По мнению Кирилла регулятор выступает гарантом стабильности. Также Кирилл отметил, что в Сбербанке поняли, что информационная безопасность сильно отстаёт от бизнеса, поэтому сейчас много сил направлено на максимальное сокращение этого отставания.

После круглого стола слушатели разделились на три потока: хакерский, технологический и юридический. **Дмитрий Гадарь**, банк "Открытие", выступил модератором хакерского потока. **Денис Батранков**, Пало Альто Нетворкс, в мастер-классе "НОУ-ХАУ от Palo Alto Networks, отметил, что очень важно знать, как нас атакуют и как правильно защищаться, и на конкретном примере показал, как быстро и качественно можно блокировать эксплойты. **Мона Архипова**, Acronis, представила мастер-класс "Risks vs Real world: как отличаются процессы на бумаге и в жизни". Большинство компаний используют в работе экспертную рисковую модель, принятую за базу во всех локальных и международных стандартах, но соответствуют ли современные реалии угрозам на бумаге? Исправление ошибок - это ядро. Регулярная работа над тюнингом повышает степень удовлетворенности пользователей. «ИБ - это не один раз настроить показатели, это постоянная работа», - заключила Мона.

В технологическом потоке **Алексей Андрияшин**, Fortinet в России, представил кейс «Адаптивная система безопасности Fortinet» и рассказал, что в последнее время возможностей для кибератак стало больше, т.к. стремительно выросло количество точек входа: мобильные телефоны, планшеты, наладонники. Очень важно отслеживать и защищать удаленные подключения. Кибербезопасность трансформируется в цифровую безопасность. «Отсутствие сетевых границ, увеличение скорости передачи информации и усложнение систем данных - основные тренды на данный момент», - высказал свою точку зрения Алексей.**Яков Гродзенский**, «Системный софт», выступил с кейсом «Интегрированная система управления рисками ИБ на основе анализа уязвимостей», где заявил, что иногда складывается впечатление, что угрозы возникают гораздо быстрее, чем средства защиты. Основными сложностями обеспечения защиты информации являются конфиденциальность, целостность, доступность. Остаточный риск становится менее управляемым. Методы защиты информации делятся на организационные и технические. В силу ограниченности бюджета мы часто смещаем акценты в сторону организационных мер, не учитывая риски. **Александр Хегай**, Cross Technologies, с кейсом «Персональные данные, которые мы забываем защитить» закрыл сессию. Компания Cross Technologies представляет разработку (Docs Security Suite, наутилус), дистрибуцию (VARONIS, Printer Guard, AccessData) и интеграцию (информационная безопасность, информационные технологии, консалтинг) программ. Александр подробно рассмотрел основные достоинства программ и возможности, которые они открывают.

В юридическом потоке **Ульяна Зинина**, Microsoft в России, представила доклад на тему «Искусственный интеллект бросает вызов». Ульяна рассмотрела сервисы на основе искусственного интеллекта: Uber (распознавание лица водителя); лечение опухолей в медицине; изучение зарплатных ожиданий от SuperJob; умная клавиатура, которая угадывает, какое слово будет следующим; перевод с любого языка на любой; персональный помощник. В первую очередь возникает вопрос: регулировать или нет, ведь регулирование - самый надёжный механизм воздействия в России. На данном же этапе проводятся исследования, как использовать искусственный интеллект, не накладывая на него строгого регулирования. Эксперт по информационной безопасности **Евгений Царев** продолжил сессию мастер-классом «Практика судебных дел, имеющих отношение к ИБ. Реальная ответственность директора по ИБ». В начале доклада Евгений рассмотрел основные варианты споров: споры по качеству, исполнение договоров подряда, трудовые споры, налоговые споры, банкротство; далее сделал разделение на IT и ИБ споры и привел примеры судебных дел из личной практики. Во второй части доклада слушатели узнали, как построить работу директора по информационной безопасности, чтобы не было правовых последствий: как правильно организовать работу сотрудника службы ИБ и вести себя в нестандартных ситуациях.

Мастер-класс «Умный подход к управлению уязвимостями» от **Игоря Булатенко**, QIWI, продолжил программу хакерского потока. Игорь отметил, как важен контроль уязвимостей. «Что можно найти под капотом стандартного сканера?» - спросил Игорь слушателей. Скриптовый язык, проверки уязвимости и неявную логику определения уязвимости. В последнее время все явственней становится гонка вооружений: "темная магия" по сбору информации, больше проверок - лучше сканер; harmless pentest и в заключение вопрос для раздумий – насколько вы доверяете своему security-вендору?

Очень заинтересовал слушателей мастер-класс независимого эксперта **Сергея Солдатова** «Трудовые будни охотника на угрозы», в котором спикер поделился широким спектром случаев из личного опыта. Сергей подчеркнул, что крайне важно быстро найти информацию, чтобы проанализировать её и сделать выводы о вредоносности. **Артем Бычков**, Банк «Открытие», в своем выступлении «Hack yourself» пропагандировал "хакерский" взгляд на жизнь в защите и подход "сделай сам" и рассказал, как защитить бренд с помощью подручных средств. На примере реальных фейков Артем доказал, насколько важны раннее обнаружение и анализ трафика.

В технологическом потоке **Артем Феоктистов**, КРОК, выступил на тему «DLP: чтобы защита не превратилась в тыкву», где рассказал, что мало кто доволен DLP, но это совсем не значит, что не нужно работать в этом направлении. Для упрощения работы нужно разделить атаку на шаги: доставка, инсталляция, распространение, выполнение действий, устранение угрозы. При внедрении DLP часто возникают организационные проблемы: далеко не все сотрудники знают о DLP. Чтобы избежать в работе этих ошибок, стоит вовлекать бизнес в процесс и учитывать его потребности. **Михаил Кадер**, Cisco, в своем кейсе «Использование сетевой телеметрии для обнаружения инцидентов безопасности» привёл примеры реальных угроз и рассказал, как обнаружить аномалии по поведению. «Главная задача – это понять, что из себя представляет аномалия», - заключил Михаил. **Михаил Романов**, «Новые технологии безопасности», представил кейс «Белые пятна привилегированного доступа. Как их решать?» поднял вопрос решения глобальной системы доступа. Михаил рассказал, как работает система (постоянный анализ и выявление ключей и доверительных связей, мониторинг, защита, управление) и как работать с привилегированным доступом. Рассмотрел варианты интеграции и особенности работы в распределенной

инфраструктуре. «Самое главное - сделать систему безопасности консистентной», - подчеркнул Михаил.

Психологический поток **Олег Кузьмин**, «Концерн ВКО «Алмаз-Антей», открыл мастер-классом «Психология информационной безопасности. Психология принятия решений». «Чтобы понять сотрудника, нужно поработать на его должности», - высказал свою точку зрения Олег. Далее были рассмотрены основные проблемы руководителя отдела информационной безопасности: недостаток знаний в области ИБ, маленький опыт работы, восприятие его окружающими, плохие поставщики, маленький бюджет, нет связи с руководством (медленное решение вопросов), провальные проекты. Олег поделился собственным опытом борьбы со всеми перечисленными проблемами.

Андрей Бажин, ВТБ Капитал, выступил модератором дискуссии «Как сейчас справляются с дефицитом квалифицированных сотрудников?», в которой приняли участие **Мона Архипова**, Acronis, **Елена Петрова**, «Экономикс-Банк» и **Андрей Дроздов**, ISACA. Все спикеры подтвердили, что сейчас по всей России присутствует кадровый голод в сфере информационной безопасности. Андрей Дроздов отметил, что HR-рынки Москвы и Санкт-Петербурга различны. Москва имеет возможность нанимать высококлассных специалистов и предлагать им соответствующую оплату. А в Санкт-Петербурге меньше спрос и меньше предложение. «Согласно мировым исследованиям по всему миру огромная нехватка кадров в сфере ИБ», - сказал Андрей. Мона Архипова сделала акцент на том, что не все специалисты, которые учатся в ИБ, потом идут работать по специальности. Но при этом на рынке много и таких сотрудников, у которых нет профильного образования, что не мешает им быть сильными безопасниками. Также Мона констатировала возобновившуюся утечку мозгов из России. Елена Петрова согласилась с коллегами в том, что основные источники информации находятся в Москве и все кадры выращиваются в Москве, поэтому зачастую у хороших специалистов просто нет стимула двигаться в регионы. К тому же по мнению Елены сотрудник из Москвы будет в регионе белой вороной с другой зарплатой и другим опытом. Важно и нужно менять систему имеющуюся на данный момент систему образования, чтобы люди не ждали, когда им спустят что-то сверху, а учились сами – пришли к общему мнению все участники дискуссии и слушатели в зале.

Во время последнего перерыва состоялся розыгрыш призов от Тайгер оптикс. Для участия достаточно было отдать свою визитку на стенд. Победителем стал Александр Леонов, Mail.ru.

В заключение деловой программы уникальный доклад «Анализ трафика в киберпространстве» представил специальный гость форума **Кеннет Гирс**, постоянный представитель Киберцентра НАТО, Comodo. Кеннет рассказал, что в первую очередь нужно найти информацию и проанализировать ее. Существует много способов защиты от внешнего анализа: отправка одновременно большого количества различных сообщений, чтобы не было понятно, какой именно сигнал вы реально хотите передать; использование разных частот; применение людей как передатчиков информации без использования телефонов и Интернета. «Анализ трафика - это очень быстро и дешево», - сделал акцент Кеннет. Также в ходе доклада слушатели еще раз убедились, что анализ контента - очень сложная работа, а анализ трафика крайне в этом помогает. «Прочитав 30 ваших постов в социальных сетях можно с точностью сказать, за кого вы будете голосовать», - сказал Кеннет, т.к. написанные посты имеют свои особенности и неповторимы, как отпечатки пальцев. «Если я знаю вас и знаю, с кем вы говорите, я с большой долей вероятности могу сказать, о чем вы говорите. И это предоставляет огромные возможности», - завершил Кеннет.

В конце Юбилейного CISO форума состоялся парад спикеров. Два дня слушатели могли проголосовать за того эксперта, который был наиболее полезен и который затронул самые наболевшие и важные темы информационной безопасности. По итогам голосования были награждены: независимый эксперт Алексей Лукацкий, Дмитрий Мананников, SPSR express, Александр Хегай, Cross Technologies, Андрей Акинин, Web Control, независимый эксперт Рустэм Хайретдинов, Евгений Климов, НИП «Информзащита», Игорь Булатенко, QIWI, Федор Горловский, ГК «Интеллектуальная безопасность», и Михаил Емельянников, "Емельянников, Попова и партнеры".

Компания **infor-media Russia** благодарит всех спикеров, партнеров и слушателей, которые приняли участие в мероприятии. До новых встреч!