

## ПОСТ-РЕЛИЗ

**В Москве состоялся бизнес-бранч «Код безопасности. Защита от киберугроз в бизнес пространстве. Итоги года и прогнозы на 2017 год» при поддержке BISA.**

*Москва, 31 января 2016 года.* — В бизнес-бранче «Код безопасности. Защита от киберугроз в бизнес пространстве. Итоги года и прогнозы на 2017 год», организованной ИД «Коммерсантъ» при поддержке BISA, приняли участие представители органов государственной власти, руководители ИТ- и ИБ-компаний. В ходе дискуссионной панели участники подвели итоги года, обсудили сложившиеся тенденции развития рынка информационной безопасности, законодательные изменения, роль импортозамещения в сфере ПО, тренды кибербезопасности.

Модераторами мероприятия выступили **Владислав Новый**, руководитель отдела телекоммуникаций, ИД «Коммерсантъ» и **Олег Седов**, главный редактор, Ассоциация по вопросам защиты корпоративной информации BISA.

В дискуссии участвовали: **Людмила Бокова**, председатель временной комиссии Совета Федерации по развитию информационного общества, **Сергей Демидов**, директор по информационной безопасности Московской биржи, **Наталья Касперская**, президент ГК InfoWatch, соучредитель компании «Лаборатория Касперского», **Алексей Лукацкий**, бизнес-консультант по информационной безопасности Cisco Systems, **Муслим Меджлумов**, директор Центра кибербезопасности и защиты «Ростелеком», **Марат Гуриев**, Директор по работе с государственными учреждениями GR Advise, Samsung Electronics, **Кирилл Ермаков**, технический директор QIWI, **Василий Окулесский**, начальник управления безопасности НСПК, **Илья Сачков**, генеральный директор Group-IB, **Андрей Голов**, генеральный директор компании «Код безопасности», **Игорь Ведехин**, заместитель генерального директора IBS, **Владимир Лебедев**, директор по развитию бизнеса Stack Group.

«Если оценивать год с точки зрения законодательного регулирования в сфере информационной безопасности у нас появился ключевой документ, - начала свое выступление **Людмила Бокова**. - 5 декабря 2016 года была подписан Указом Президента РФ Доктрина информационной безопасности. Это документ стратегического назначения, где четко обозначены границы обеспечения информационной безопасности, показаны направления взаимодействия всех структур, в том числе и отрасли, на реализацию мероприятий в сфере ИБ. Ключевой лейтмотив Доктрины — защита персональных данных граждан, а также реализация их прав на доступность информации, на использование имеющихся технологий. В следующем году нам предстоит ее предметно осмыслить, обсудить направления реализации вместе с отраслью и ведомствами, наполнить Доктрину содержательно с точки зрения нормативной базы.»

**Наталья Касперская** представила последние данные о количестве утечек за 2016 год, которые удалось собрать: число утечек выросло незначительно, однако значительно (на 300%) увеличилось количество утекших записей персональных данных, 3,1 млрд. записей было потеряно в прошлом году. Число мегаутечек (свыше 10 млн. записей) в прошлом году составило 44 шт., а в 2015 всего 21. «Становится популярнее воровать и использовать огромные базы данных, чтобы потом их монетизировать. Это очень тревожащая тенденция, потому что бороться с этим довольно сложно.» - заключил спикер.

При этом **Наталья К.** положительно оценила развитие отечественного рынка информационной безопасности. «Год закончился по позитивной ноте. Что касается оценки объема, то, что мы ее не имеем, говорит о его закрытости, а не о его неструктурированности, потому что, на мой взгляд, рынок ИБ один из самых четких и структурированных рынков, на котором российские разработчики закрывают все ниши, у нас область ИБ развита лучше, чем другие области ИТ, нам есть чем гордиться.»

**Марат Гуриев** уверен: «Для создания защищенной корпоративной мобильной инфраструктуры, в том числе для госучреждений, важны три ключевые составляющие: сертифицированная операционная система с открытым кодом, сертифицированное корпоративное MDM-решение и сертифицированное решение по защите канала передачи данных. В настоящее время решением, отвечающим этим требованиям, является программно-аппаратная платформа Tizen на базе смартфона Samsung Z3. Специализированный смартфон Samsung Z3 в сочетании с доверенной мобильной платформой Tizen, MDM SafePhone и приложением VipNet по защите канала передачи данных создают комплекс с надежной системой управления устройством, защищенными каналами связи и обмена информацией. Решение исключает наличие каких-либо секретных кодов или недокументированных возможностей, а также обеспечивает блокировку установки приложений из недоверенных источников. Операционная система Tizen полностью сертифицирована на соответствие требованиям ФСТЭК России, а VPN VipNet также имеет сертификат соответствия требованиям ФСБ. Подобное универсальное решение способно не только решить важнейшие задачи кибербезопасности внутри страны, но и может стать конкурентоспособным продуктом на внешних рынках.»

**Владимир Лебедев** отметил, что «сегодня для крупного бизнеса актуален вопрос защиты данных в облаке с определенным уровнем защищенности, в том числе персональных данных, так как стремление повысить общую эффективность бизнеса требует и оптимизации ИТ-инфраструктуры, путем перемещения ее в облако. И этот вопрос относительно новый для рынка.»

Партнёрами бизнес-бранча «Код безопасности. Защита от киберугроз в бизнес пространстве. Итоги года и прогнозы на 2017 год», организованной издательским домом «Коммерсантъ» 31 января, выступили Samsung, Cisco, «Код Безопасности», IBS, Stack Group.