# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ требует новых подходов

Л.Павлова

Для противостояния современным угрозам информационной безопасности государство, бизнес и общество вырабатывают адекватный механизм защиты, обновленный стратегически и технологически.

## По большому счету

О том, что назрела необходимость разработки и принятия новой редакции Доктрины информационной безопасности, заявил на "Инфофоруме-2015" Дмитрий Грибков, референт аппарата Совета Безопасности РФ. Напомнив, что действующая доктрина была утверждена 15 лет назад, он отметил, что сегодня требуется внести в нее корректировки, направленные на укрепление национального суверенитета России в глобальном информационном пространстве. По словам Д.Грибкова, в новой редакции Доктрина информационной безопасности должна быть согласована с представителями отрасли и определить национальные интересы в информационной среде (соблюдение прав человека и гражданина, развитие отечественных решений в сфере ИКТ, обеспечение безопасности национальной информационной критической инфраструктуры), а также тесно увязана с документами стратегического планирования, в частности, с принятой в мае 2009 года Стратегией национальной безопасности Российской Федерации до 2020 года. В документе планируется также прописать факторы, которые будут учитываться при оценке угроз информационной безопасности России, – активное использование информационных технологий зарубежными странами в целях разведки и достижения своих политических и военных целей, оказание давления на развитие российского сегмента интернета, слабая скоординированность деятельности органов власти по вопросам обеспечения безопасности на различных уровнях.

В необходимости выработки адекватного механизма реагирования на внешние угрозы информационной безопасности не сомневается и председатель комитета Госдумы по информационной политике, информационным технологиям и связи Леонид Левин. По его мнению, важной составляющей такого механизма может стать закон о хранении персональных данных россиян на территории РФ, который вступит в силу 1 сентября этого года. В то же время необходимо повышать грамотность в области информационной безопасности среди частных пользователей, особенно детей и подростков, считает Людмила Бокова, заместитель председателя Комитета Совета Федерации по конституционному законодательству и государственному строительству. По словам сенатора, возглавляемая ею временная комиссия Совфеда по развитию информационного общества подготовила технические требования по обеспечению безопасности детей в сети Интернет, проект методических рекомендаций по работе системы контент-фильтрации в образовательных учреждениях, а также инициировала проведение единого урока безопасности в интернете с подключением к обучению инфобезопасности родителей и школьных учителей (что, к слову, отражено и в принятой недавно Концепции информационной безопасности детей). "От уровня сегодняшней цифровой грамотности детей зависит завтрашний цифровой суверенитет страны, – уверена Л.Бокова. – В этом направлении должны действовать комплексные программы, и мы совместно с компаниями

отрасли будем обращаться с соответствующими предложениями в министерство образования".

## Человеческий фактор

Как сообщил Алексей Мошков, начальник Бюро специальных технических мероприятий МВД России, в 2014 году в России было зарегистрировано около 11 тыс. преступлений с использованием информационных технологий, причем на кражи денежных средств и мошенничество с целью извлечения материальной выгоды приходится 41% (в 2013 году – 30%). Важная тенденция последних лет – широкое использование компьютерными преступниками мобильных платформ в качестве средства получения конфиденциальной информации. Так, осенью 2014 года сотрудниками бюро была пресечена деятельность преступной группы, которая внедряла на смартфоны ПО, позволяющее удаленно получать полный контроль над устройством. "Большинство современных смартфонов и планшетов используют привязку к учетной записи, а зачастую еще и хранят конфиденциальные данные в облачных сервисах, – отметил А.Мошков. – Получив через интернет доступ к учетной записи пользователя, злоумышленники могут получить списки контактов, фото и видео, сведения о переписке, а в некоторых случаях и о перемещениях абонента. Иногда доступными становятся даже данные банковских карт владельца телефона, пароли и учетные записи в различных сервисах. Как правило, эти сведения впоследствии используются для хищения денежных средств и шантажа".

Зачастую жертвы компьютерных преступлений просто не знают о существующих в информационной среде угрозах. Поэтому, как сообщил А.Мошков, бюро подготовило своего рода дайджест угроз в сети, содержащий также рекомендации пользователям и советы по определению мошеннических ресурсов. В то же время, по его мнению, информирование пользователей о рисках и потенциальных потерях должно стать неотъемлемой частью работы операторов с клиентами.

Примечательно, что с точки зрения информационной безопасности человеческий фактор оказывается слабым звеном не только в частной, но и в деловой жизни, где уже прочно утвердился принцип использования личных устройств в рабочих целях BYOD (Bring Your Own Device). В этой ситуации о защите данных пользователей должны заботиться не только корпоративные ИБ-службы, но и производители мобильных устройств, считает Андрей Тихонов, директор по корпоративным продажам компании "Самсунг Электроникс Рус". По его словам, распространение рынка корпоративной мобильности тесно связано с растущим спросом на эффективные решения в области информационной безопасности, и компания Samsung Electronics уделяет этому направлению исключительное внимание при разработке устройств. Так, в 2014 году она представила российскому рынку Samsung KNOX – решение по разграничению информационного пространства в мобильном устройстве, полностью отвечающее требованиям ИТ- и ИБ-служб предприятий, без ограничений частной жизни персонала. А в 2015 году Samsung Electronics планирует вывести на российский корпоративный рынок открытую операционную систему Tizen со встроенными средствами безопасности и шифрования, контейнеризации приложений и данных, которая будет максимально соответствовать российским требованиям информационной безопасности.

## Вопрос доверия

Новые подходы к вопросам обеспечения информационной безопасности не отменяют их традиционной основы – доверия пользователей к устройствам и встроенному в них ПО. В свою очередь, как отметил Владимир Мамыкин, директор по информационной безопасности ООО "Майкрософт Рус", это доверие основывается на возможности государственных органов проверить и исследовать исходные коды программной продукции. За последнее десятилетие Microsoft предоставил ФСТЭК и ФСБ России возможность исследовать коды своих более чем шестидесяти продуктов для их сертификации на соответствие различным уровням требований к безопасности, напомнил В.Мамыкин. По его словам, к осени этого года компания готовит выпуск пакета новых продуктов, которые так же планируется сертифицировать в России.

Кроме того, в нынешнем году Microsoft запускает программу построения защищенных облачных инфраструктур на базе продуктов Microsoft и расположенных на территории России ЦОДов партнеров корпорации ("Ростелеком", "Электронная Москва", КРОК, Softline и др.). "В отличие от публичных облаков, партнерские облака позволят использовать российское шифрование, российские продукты и защищать данные в строгом соответствии с российским законодательством, – отметил В.Мамыкин. – Мы рассчитываем, что спрос на эти облачные сервисы будет большой". По его словам, процесс сертификации облачных решений Microsoft во ФСТЭК и ФСБ будет завершен в марте-апреле этого года. ■