Avec le soutien / при поддержке:

20 лет ans CCI FRANCE RUSSIE
CHAMBRE DE COMMERCE ET D'INDUSTRIE FRANCO-RUSSE
ФРАНКО-РОССИЙСКАЯ ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА

15 ans Le Courrier de Russie
www.lecourrierderussie.com
GROUPE NOVYI VEK MEDIA

Экономические отношения между Россией и Францией

L'économika

LES RELATIONS ÉCONOMIQUES ENTRE LA RUSSIE ET LA FRANCE

№11 (321), 2017

ТРЕТЬ РОССИЙСКИХ КОМПАНИЙ НЕ УМЕЕТ ЗАЩИЩАТЬСЯ ОТ DDOS-АТАК

31 % российских компаний не знает, как противостоять DDoS-атакам, а 15 % организаций никак не защищены от этой угрозы, следует из исследования, проведенного «Лабораторией Касперского» совместно с компанией B2B International.

При этом 62 % компаний, по данным «Лаборатории Касперского», полагаются на встроенные аппаратные средства защиты, которые бесполезны в случае сложных и масштабных DDoS-атак. IT-специалисты только из 21 % организаций в полной мере осознают потенциальную угрозу.

МИРОВАЯ ЭКОНОМИКА ПОТЕРЯЛА $ 450 МЛРД ИЗ-ЗА КИБЕРПРЕСТУПЛЕНИЙ

Исследование британской страховой компании Hiscox, в котором приняли участие более 3000 компаний из США, Германии и Великобритании, показало, что в 2016 году компьютерные преступления обошлись мировой экономике в $ 450 млрд. Преступники похитили более 2 млрд записей персональных данных. Средний размер ущерба от кибератак составил около € 22 000 для компаний малого бизнеса в Германии и до $ 100 000 для больших компаний в США.

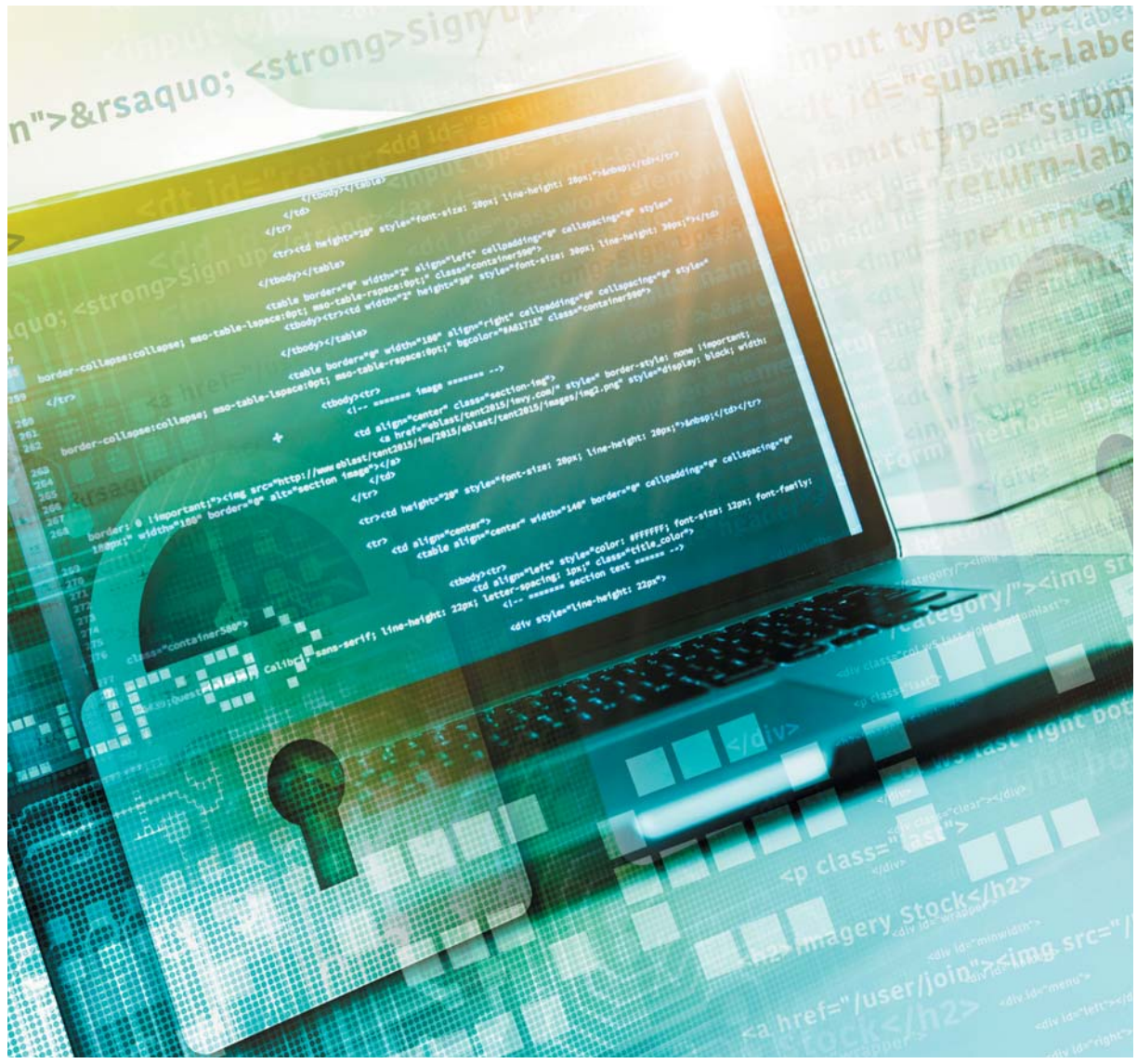
ХАКЕРОВ БУДУТ САЖАТЬ В ТЮРЬМУ НА 10 ЛЕТ

В конце января Госдума одобрила в первом чтении пакет правительственных законопроектов о повышении уголовной ответственности за кибератаки на критическую информационную инфраструктуру (КИИ). В качестве наказания для хакеров предусмотрено лишение свободы на срок от 5 до 10 лет или штраф в размере до 2 млн рублей.

Согласно новому законопроекту, к КИИ относятся информационные системы и информационно-телекоммуникационные сети госорганов, а также автоматизированные системы управления технологическими процессами в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, металлургической, химической и горнодобывающей промышленности.

ОХОТА ЗА ПЕРСОНАЛЬНЫМИ ДАННЫМИ: КАК НЕ СТАТЬ ДОБЫЧЕЙ ЗЛОУМЫШЛЕННИКОВ

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН РОССИИ ОХРАНЯЕТСЯ ФЕДЕРАЛЬНЫМ ЗАКОНОМ. НЕСМОТРЯ НА ЭТО, ОБЪЕМ ЧЕРНОГО РЫНКА БАЗ ДАННЫХ В РОССИИ ДОСТИГАЕТ 30 МЛН РУБЛЕЙ, А ЖЕРТВОЙ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ СТАНОВИТСЯ КАЖДЫЙ ДЕСЯТЫЙ РОССИЯНИН, ЧЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ПОПАЛИ В РУКИ ЗЛОУМЫШЛЕННИКОВ, – ТАКОВЫ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ «ЧЕРНЫЙ РЫНОК БАЗ ДАННЫХ» АНАЛИТИЧЕСКОГО ЦЕНТРА «МФИ СОФТ» ЗА НОЯБРЬ 2016 ГОДА. КАК В ТАКИХ УСЛОВИЯХ ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ КЛИЕНТОВ И СОТРУДНИКОВ КОМПАНИИ?



ПОДВОДНЫЕ КАМНИ

На сегодняшний день нет четкого определения понятия «персональные данные». Это может быть любая информация о физическом лице: Ф. И. О., дата рождения, адрес, семейное и социальное положение, образование, информация о доходах. Эксперты обычно выделяют три категории персональных данных: общедоступные, биометрические и специальные. Первые легко узнать из открытых источников, таких как, например, социальные сети. На основании биометрических данных устанавливают личность человека, его биологические и физиологические особенности: рост, вес, отпечатки пальцев, группа крови, результаты анализов и т. д. К специальной категории персональных данных относят информацию о расовой и национальной принадлежности, религиозных и политических убеждениях, интимной жизни и здоровье.

Современный человек щедро распоряжается персональными данными: при покупке билета в интернете, оформлении подписки на e-mail-рассылку, регистрации на мероприятие. Контролировать поток информации становится все сложнее. С развитием технологий компании внедряют специальные сервисы и CRM-системы для работы с большими объемами данных. Но из-за проблем с информационной безопасностью персональная информация нередко попадает в руки злоумышленников. При этом масштаб компьютерного преступления может варьироваться от безобидного спама до хищения многомиллионных сбережений.

Поэтому не стоит оставлять персональные данные в открытых источниках и на подозрительных интернет-ресурсах: кажущиеся безобидными онлайн-тест или игра могут оказаться ловушкой компьютерных преступников. Стоит позаботиться о надежности паролей к аккаунтам в социальных сетях и электронной почте. Также нежелательно пользоваться автосохранением в браузерах Ф. И. О., контактов и данных банковских карт.

Не стоит оставлять персональные данные в открытых источниках и на подозрительных интернет-ресурсах: кажущиеся безобидными онлайн-тест или игра могут оказаться ловушкой компьютерных преступников.

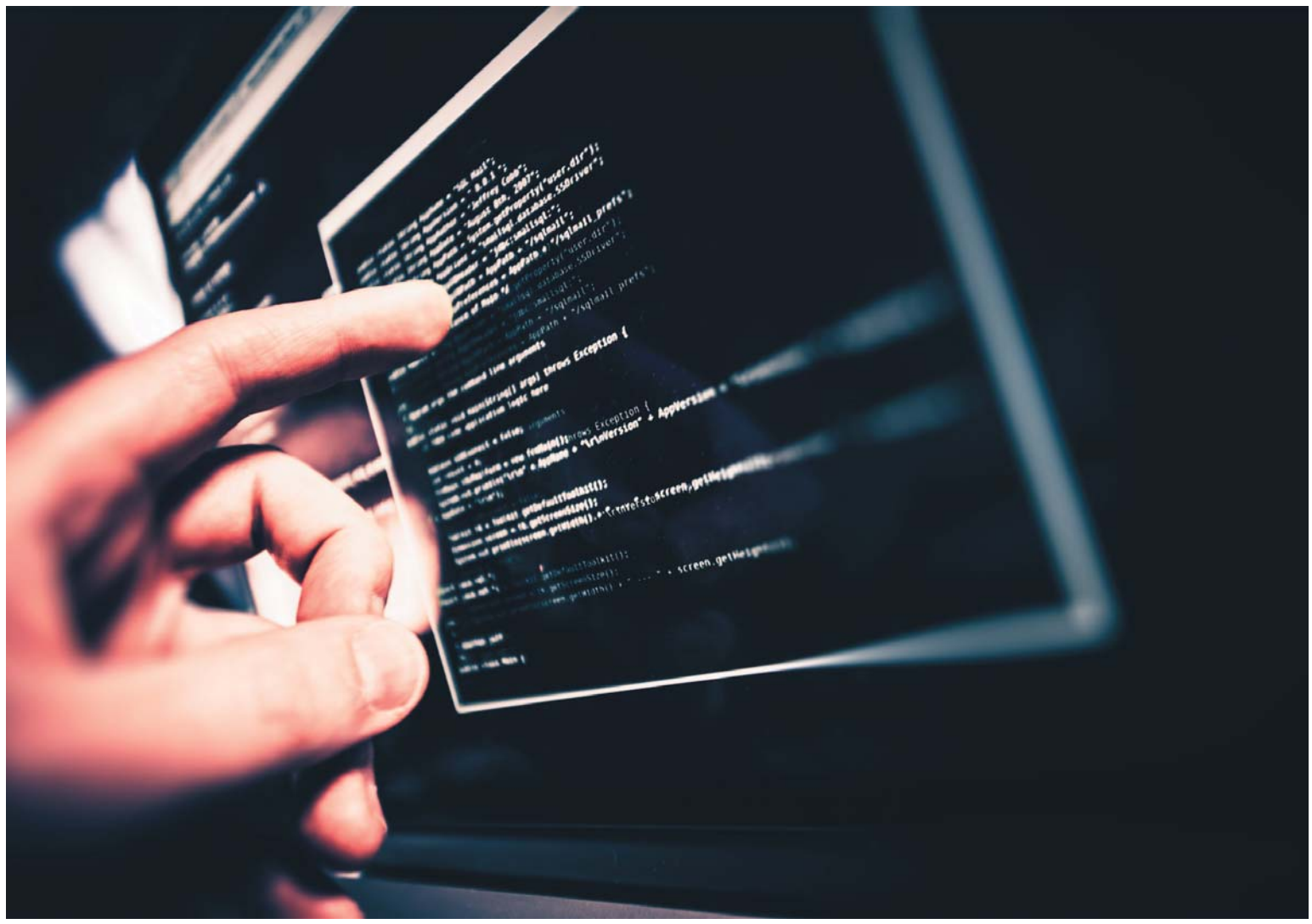
Компании наравне с физическими лицами тоже нередко становятся жертвами интернет-преступников. Только в этом случае последствия более масштабны: хищение персональных данных сотрудников приводит к взлому всей системы. А базы данных клиентов распродаются на черном рынке в среднем по 15 000 рублей за штуку. И то и другое наносит удар по репутации и вредит коммерческой деятельности.

ЗАКОНОДАТЕЛЬНЫЕ НОРМЫ

Обеспечение безопасности личных данных сегодня как никогда актуально и регулируется на государственном уровне. Персональные данные, как и неприкосновенность частной жизни, в России защищают Конституция РФ, Гражданский и Трудовой кодекс, Федеральный

ТАБЛИЦА 1. НАКАЗАНИЕ ЗА НАРУШЕНИЕ ЗАКОНА О СБОРЕ, ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

НАРУШЕНИЕ	ШТРАФ ДЛЯ ФИЗЛИЦА	ШТРАФ ДЛЯ ЮРЛИЦА	ШТРАФ ДЛЯ ДОЛЖНОСТНЫХ ЛИЦ
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЯХ, НЕ ПРЕДУСМОТРЕННЫХ ЗАКОНОДАТЕЛЬСТВОМ РФ, ЛИБО ОБРАБОТКА ДАННЫХ, НЕСОВМЕСТИМАЯ С ЦЕЛЯМИ СБОРА ТАКИХ ДАННЫХ	ПРЕДУПРЕЖДЕНИЕ ИЛИ ШТРАФ ОТ 1000 ДО 3000 РУБЛЕЙ	ОТ 30 000 ДО 50 000 РУБЛЕЙ	ОТ 5000 ДО 10 000 РУБЛЕЙ
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ ГРАЖДАНИНА	ОТ 3000 ДО 5000 РУБЛЕЙ	ОТ 15 000 ДО 75 000 РУБЛЕЙ	ОТ 10 000 ДО 20 000 РУБЛЕЙ
ОТКАЗ ПРЕДОСТАВИТЬ ЧЕЛОВЕКУ ИНФОРМАЦИЮ ОБ ОБРАБОТКЕ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ	ПРЕДУПРЕЖДЕНИЕ ИЛИ ШТРАФ ОТ 1000 ДО 2000 РУБЛЕЙ	ОТ 10 000 ДО 15 000 РУБЛЕЙ ДЛЯ ИП И ОТ 20 000 ДО 40 000 РУБЛЕЙ ДЛЯ ЮРЛИЦ	ОТ 4000 ДО 6000 РУБЛЕЙ



закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных». Однако в течение последних двух лет стали необходимы дополнительные законодательные меры, призванные обезопасить персональные данные граждан в интернете. Так, с 1 сентября 2015 года вступило в силу положение, обозначенное законом ФЗ-242, которое обязывает всех операторов персональных данных обрабатывать и хранить персональные данные россиян исключительно на территории РФ.

Причем перечисленные требования к обеспечению безопасности касаются практически каждого. К информационным системам персональных данных могут быть отнесены не только базы интернет-магазинов и онлайн-сервисов, но и кадровые и бухгалтерские системы, call-центры и даже автоматизированные системы бюро пропусков, которые есть почти в любой компании. Если проверка со стороны Роскомнадзора выявит нарушения, за этим последует административная ответственность предприятия и его руководителей по статьям «Нарушение установленного законом порядка сбора, хранения, использования и распространения информации о гражданах (персональных данных)», «Нарушение правил защиты информации», «Незаконная деятельность в области защиты информации».

Новый всплеск обсуждения защиты персональных данных произошел летом 2016 года. Тогда президент Владимир Путин подписал ряд антитеррористических поправок к законам, получивший в СМИ название «пакет Яровой» – по фамилии автора документа. По измененному законодательству операторы мобильной связи обязаны хранить все записи звонков и сообщений, которыми обмениваются пользователи в течение полугода, а информацию о фактах соединения – три года.

Кроме того, в начале 2017 года Госдума увеличила размеры штрафа за нарушение закона № 152-ФЗ о сборе, обработке и хранении персональных данных. Согласно принятым поправкам, теперь на устранение нарушений отводится три дня. За невыполнение предписаний грозят санкции: штрафы до 300 000 рублей, конфискация несертифицированных средств защиты или требование прекратить обработку персональных данных – в любом случае компанию ждут значительные издержки.

Юрист коллегии адвокатов «Новый Арбат» Алексей Пономарев уверен, что принятие ФЗ-152 – закона о хранении и обработке персональных данных – и дальнейшее ужесточение ответственности за его нарушение является необходимым шагом. «Конечно, все это звенья одной цепи – ужесточения контроля за интернет-сферой. Но анархия на просторах российской части интернета когда-то должна была закончиться. Для IT-сферы это означает дополнительные расходы, а также увеличение входного порога для начинающих компаний. Но подобные законы давно приняты в большинстве государств и считаются там нормой», – комментирует специалист.

Максим Лагутин, основатель и эксперт по защите персональных данных компании «Б-152», которая помогает организациям с юридическим оформлением документов по персональным данным, со своей стороны, считает, что у российского законодательства в области защиты персональных данных есть своя специфика. «За границей штрафуют за утечку информации, а в России – за отсутствие соглашений физлиц на обработку персональных данных, за несоответствие такого согласия целям, т. е. за отсутствие документов, а не за исполнение прав субъекта», – отмечает эксперт.

По его словам, раньше некоторые компании игнорировали закон, так как проще было заплатить штраф, чем соответствовать законодательным требованиям, тогда как недавнее увеличение санкционных мер заставит юридические лица быть более ответственными. «Соответствие закону не требует больших вложений, это, прежде всего, координация и дисциплина. Я надеюсь, что со временем во всех компаниях появится процедура саморегулирования или будет внедрена система регулярного аудита в этой области», – добавляет основатель «Б-152».

За границей штрафуют за утечку информации, а в России – за отсутствие соглашений физлиц на обработку персональных данных, за несоответствие такого согласия целям, т. е. за отсутствие документов, а не за исполнение прав субъекта.

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ

Однако обеспечить защиту персональных данных, как того требует закон, не так-то просто – можно быстро запутаться в многообразии средств защиты и количестве необходимых документов.

«Российское законодательство в этой сфере пока тщательно не проработано. Например, персональные данные, разнесенные по разным местам, перестают быть персональными: номер телефона – это набор цифр, а номер телефона и Ф. И. О. – уже персональные данные. Страница в социальной сети персональными данными не является, но если на такой странице указан телефон, то она сразу попадает под действие закона, даже если это досье вымышленного персонажа. И еще персональные данные нельзя хранить за рубежом, но бекап (резервную копию. – *Прим. ред.*) уже можно», – поясняет основатель системного интегратора Jack-IT Илья Яшин.

К тому же компьютерные преступники в технологиях стараются быть на шаг впереди систем безопасности, поэтому формальные методы защиты – от переноса информации на российский сервер до установления антивирусной программы – могут не сработать. Защита персональных данных требует комплексного подхода: как технического, так и организационного.

Универсального метода защиты нет, однако есть технологии, которые можно внедрить для защиты информации в любом виде бизнеса. Например, использовать биометрические. Принцип простой: доступ к инфраструктуре контролируется снятием отпечатка пальца, сканированием сетчатки глаза или аутентификацией по голосу. Важно, что система не хранит биометрические данные, а шифрует их. Такие технологии работают и когда нужно ограничить доступ сотрудников к кабинетам, компьютерам и отдельно взятым файлам, и когда пользователь входит в личный кабинет через мобильное приложение – после сканирования отпечатка пальца.

Еще один способ защиты – перенос всей информационной структуры в облако. Доступ к информации будет осуществляться только через защищенные каналы, а у каждого сотрудника появится персональный ключ доступа. При этом действия всех сотрудников можно контролировать в режиме реального времени: видно, кто чем занимается в данный момент, кто отошел от компьютера, кто скачивает подозрительные документы. При этом на самих компьютерах ничего не хранится, поэтому, даже если злоумышленники похитят технику, то данные не получат.

Для защиты интернет-магазинов и сайтов подойдут сервисы, которые контролируют трафик и оберегают от ddos-атак, предсказывают возможность нанесения вреда сайту и предупреждают о подозрительных действиях. Специальная программа фиксирует средние показатели: количество просмотров сайта, среднее число уникальных пользователей, время просмотра страниц и т. д. Если показатели начинают резко отличаться от нормы или кто-то начинает проявлять на сайте подозрительную активность, то программа сразу же отправляет сообщение с предупреждением.

«Используя данные об истории пользовательской метрики, мы прогнозируем ее ожидаемые значения. Если прогноз не совпадает с текущим значением, пользователь сразу же получает соответствующее уведомление», – поясняет принцип работы подобных программ сооснователь компании Statsbot Павел Тиунов.

Тем не менее, несмотря на то что существуют технологии, помогающие защититься от уловок компьютерных преступников, ни один код не спасет от человеческого фактора. Согласно исследованию компании по разработке систем информационной безопасности «МФИ Софт», базы данных попадают на черный рынок четырьмя способами. Причем добыча персональных данных путем взлома (2 %) и через незащищенные источники (7 %) – в меньшинстве. Главными причинами утечки остаются недобросовестные сотрудники: злонамеренный инсайд составляет 78 % случаев утечки данных, а оставшиеся 13 % приходятся на целенаправленное распространение данных клиентов на коммерческой основе.

ИЛЬМИРА ГАЙСИНА

ПАМЯТКА ДЛЯ РУКОВОДИТЕЛЕЙ

ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ ПРИ ВЫПОЛНЕНИИ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ:

- НАПРАВИТЬ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТРОЛИРУЮЩИЙ ОРГАН – РОСКОМНАДЗОР;
- ПОЛУЧИТЬ СОГЛАСИЕ КАЖДОГО СУБЪЕКТА (СОТРУДНИКА ИЛИ КЛИЕНТА) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ (СОГЛАСИЕ ДОЛЖНО СОДЕРЖАТЬ СОБСТВЕННОРУЧНУЮ ПОДПИСЬ СУБЪЕКТА ЛИБО ЕГО ЦИФРОВУЮ ПОДПИСЬ);
- ДОКУМЕНТАЛЬНО ОПИСАТЬ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ (НАЗНАЧЕНИЕ, СОСТАВ ДАННЫХ, ПРАВОВЫЕ ОСНОВАНИЯ ДЛЯ ИХ ОБРАБОТКИ), А ТАКЖЕ ОБОЗНАЧИТЬ КРУГ ЛИЦ, РАБОТАЮЩИХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ И ИМЕЮЩИХ К НИМ ДОСТУП;
- РАЗРАБОТАТЬ РЯД НОРМАТИВНЫХ ДОКУМЕНТОВ, ОПИСЫВАЮЩИХ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И СРЕДСТВА ЗАЩИТЫ ОТ НИХ;
- ОБЕСПЕЧИТЬ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТЕХНИЧЕСКИМИ (ПРОГРАММНЫМИ, АППАРАТНЫМИ) И ОРГАНИЗАЦИОННЫМИ МЕТОДАМИ;
- ПРОЙТИ НЕОБХОДИМУЮ ПРОВЕРКУ РОСКОМНАДЗОРА ДЛЯ ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА.

«БОЛЬШИНСТВО ХАКЕРОВ КОНЦЕНТРИРУЮТСЯ НА АТАКАХ БИЗНЕСА»

ЧИСЛО КИБЕРАТАК НА РОССИЙСКИЙ БИЗНЕС В 2016 ГОДУ ВЫРОСЛО ВТРОЕ. УЩЕРБ ОТ ОДНОЙ АТАКИ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОБХОДИТСЯ В СРЕДНЕМ В 6 МЛН РУБЛЕЙ, ДЛЯ КРУПНОГО – В 11 МЛН РУБЛЕЙ. L'ÉCONOMIKA ПОГОВОРИЛА О БОРЬБЕ С КОМПЬЮТЕРНЫМИ ПРЕСТУПНИКАМИ С ИЛЬЕЙ САЧКОВЫМ, ГЕНЕРАЛЬНЫМ ДИРЕКТОРОМ ОДНОЙ ИЗ КРУПНЕЙШИХ ЧАСТНЫХ КОМПАНИЙ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ GROUP-IB.

– Какие компании наиболее подвержены кибератакам?

– Компьютерная преступность на 99% связана с желанием злоумышленников получить деньги, поэтому любая компания попадает в группу риска. По данным нашего годового исследования, в 2016 году в России большую часть денег киберпреступники получили в результате целевых атак на финансовые учреждения.

Частные лица, безусловно, тоже часто являются мишенью хакеров. В последнее время получили популярность вирусы-шифровальщики. Смысл преступления в том, что программа зашифровывает ценные файлы, а преступники в обмен на ключ вымогают деньги. Также компьютерные преступники воруют персональные данные, связанные с банковскими картами.

Кроме того, злоумышленники могут использовать в своих целях популярные бренды. Создают мошеннические схемы, начиная от поддельных лотерей или конкурсов от имени бренда, призванных выманить личные данные пользователя, например данные по пластиковым карточкам, и заканчивая продажей контрафактных товаров под видом оригинальной продукции.

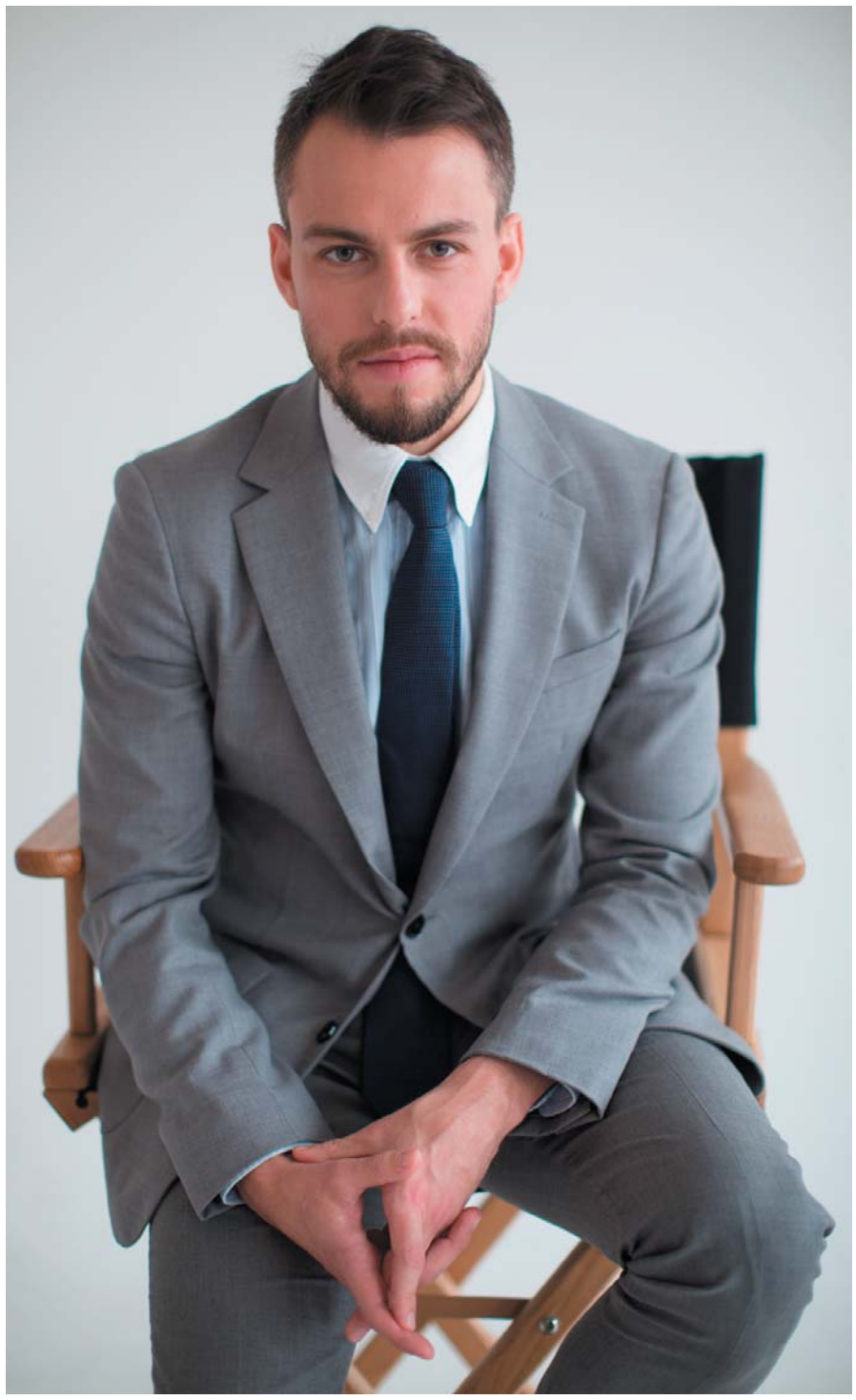
Критически важные объекты инфраструктуры, такие как атомные станции, электростанции и пр., классическую компьютерную преступность не интересуют, потому что атаки на эти объекты не приносят денег, а вызывают общественный резонанс. И, скорее всего, таких злоумышленников будут преследовать по закону. Поэтому подавляющее большинство хакеров концентрируется на атаках бизнеса и устройствах частных пользователей.

– Какие уловки используют злоумышленники?

– У злоумышленников две составляющих успеха. Первая – это технологии: сложносочиненные, не детектируемые антивирусами вредоносные программы и знание уязвимостей ПО. Вторая составляющая успеха – социальная инженерия, то есть знание аспектов психологии человека.

Вот простой пример социальной инженерии в действии из нашей практики: сотрудник банка получает письмо от клиента, который до этого позвонил по телефону и собирался открыть счет в банке. Письмо приходит с домена компании, о которой говорил клиент, с подписью и приложением в формате .doc. Естественно, сотрудник банка ждет это письмо и откроет вложение не задумываясь. Так злоумышленник получает доступ к сети организации.

Зачастую также применяется отправка вредоносных писем с текстом: «Ваш почтовый аккаунт будет заблокирован, подтвердите, что вы не робот», или «С вашего почтового аккаунта отсылался спам», или «Бесплатно получите 20 Гб места» и так далее. Стандартные человеческие слабости: страх и любопытство – вынуждают человека действовать быстро, что очень на руку компьютерным преступникам.



– Как снизить риски при хранении и передаче информации?

– Чтобы снизить риски, нужно о них знать. Большинство инцидентов происходит с людьми или компаниями, которые либо ничего не знают об информационной безопасности, либо неправильно оценивают свои риски.

Поэтому основа безопасности – правильная оценка рисков для вашей конкретной организации. Желательно искать информацию о возбужденных уголовных делах по компьютерным преступлениям в области вашего бизнеса, читать популярные статьи на тему информационной безопасности. Это построит фундамент, от которого зависит 99% безопасности. Ну и конечно, нужно соблюдать базовую компьютерную гигиену: не открывать ссылки и документы, отправленные незнакомыми людьми, регулярно обновлять компьютер, использовать сложные пароли и двухфакторную аутентификацию – запрос данных двух разных типов, например: логин и пароль в качестве первого типа данных и специальный код, который приходит по SMS или электронной почте, в качестве второго.

– Почему антивирусные программы не справляются?

– Современные организованные преступные группы обладают такими бюджетами и технологиями, которые способны конкурировать с антивирусными программами, установленными на конечных устройствах жертв. В 86% наших расследований на пострадавших компьютерах были установлены антивирусные программы.

Любой компьютерный преступник, запускающий в бой новый тип вируса, всегда проверяет вредоносную программу на всех антивирусных базах и в специальных средах, чтобы убедиться, что антивирусы ее не обнаруживают.

Антивирус необходим для защиты компьютера, но вот уже около пяти лет этого недостаточно. Чтобы быть в безопасности, нужно использовать также сетевые средства обнаружения и средства противодействия целевым атакам.

ПО ИТОГАМ 2015 Г., ХАКЕРЫ НАНЕСЛИ ЭКОНОМИКЕ РОССИИ УЩЕРБ В **203 МЛРД РУБЛЕЙ,** ЭТО 0,25% ВВП СТРАНЫ, ИЛИ ПОЛОВИНА БЮДЖЕТА, ЗАЛОЖЕННАЯ НА РАЗВИТИЕ ЗДРАВООХРАНЕНИЯ.

ИЗ НИХ **123,5 МЛРД –** УЩЕРБ БИЗНЕСА, 80 МЛРД – ЗАТРАТЫ НА ЛИКВИДАЦИЮ ПОСЛЕДСТВИЙ КИБЕРПРЕСТУПЛЕНИЙ.

92% ИЗ 600 РОССИЙСКИХ КОМПАНИЙ СТАЛКИВАЛИСЬ С КИБЕРАТАКАМИ. КОЛИЧЕСТВО АТАК ЗА ПОСЛЕДНИЕ ТРИ ГОДА ВЫРОСЛО НА 75%, ФИНАНСОВЫЙ УЩЕРБ ОТ НИХ – ВДВОЕ.

В РОССИИ ЕЖЕДНЕВНО СОВЕРШАЕТСЯ **СВЫШЕ 1000** ТОЛЬКО DDOS-АТАК.

ДАННЫЕ: ИССЛЕДОВАНИЕ ФРИИ, MICROSOFT И GROUP-IB

– Расскажите об основных тенденциях в сфере компьютерной безопасности. Какие появились новые способы пресечения преступлений?

– Сегодня существует несколько классов технологий предупреждения кибератак.

Первый класс представляет собой «киберразведку» и призван анализировать большие объемы данных, используя разного рода ловушки и мониторинговые системы, чтобы на раннем этапе предугадывать действия злоумышленника, когда тот только готовится к атаке. Необходимо выявить индикаторы, которые свидетельствуют о подготовке преступления. В интернете невозможно действовать незаметно. Злоумышленники, конечно, стараются не оставлять следов, но даже минимальной информации достаточно, чтобы предугадать атаку.

Второй класс связан с поведенческим анализом. Такие технологии используются, например, для проверки почтовых вложений. Программа запускает присланный файл в формате .pdf или .doc в различные виртуальные среды и проверяет, способен ли он нанести вред.

Появляются также технологии биометрической аутентификации пользователей. Это удобно, но тоже не обходится без рисков. Ведь при компрометации (взломе, краже данных. – *Прим. ред.*) своей учетной записи пользователь просто поменяет пароль, а при компрометации биометрических данных, по сути, потеряет свою личность.

Что касается пресечения преступлений, уже долго мы и наши коллеги в разных странах настаиваем на том, что сегодня бороться с киберпреступниками одними технологиями бесполезно, гонку вооружений наверняка проиграем. Борьба с преступностью должна совмещать применение технологий и юридического воздействия. Главный способ пресечения компьютерных преступлений – уголовное преследование преступников.

– Как оценить информационную защищенность компании?

– Создать службу компьютерной безопасности. Если ее нет, нужно обратиться к организациям, которые занимаются аудитом внешней и внутренней информационной безопасности бизнеса.

В качестве проверки можно симулировать действия злоумышленников – устраивать учебные атаки: проверять конфигурацию сетевого оборудования, оценивать подготовку сотрудников, в том числе методами социальной инженерии. Анализ защищенности – довольно популярная услуга. Такую проверку важно проводить хотя бы раз в квартал.

– Что делать, если обнаружена угроза?

– Если обнаружена угроза, главное, не пускать все на самотек. Важно помнить, что вас атакует организованная преступная группировка, задача которой украсть деньги либо информацию или саботировать вашу работу.

Я рекомендую, в первую очередь, написать заявление в полицию, потому что каждое преступление должно быть расследовано. Далее – привлечь внутреннюю службу безопасности или криминалистов для локализации инцидента. Если внутри компании обнаружен вирус, задача не просто его удалить, но и понять, как он попал в систему. Нужно исследовать функционал вируса, узнать, куда он передавал данные, с какой преступной группой связан. Понять, была ли это целенаправленная атака или случайное заражение.

Большому и среднему бизнесу нужно правильно выстраивать в компании политику реагирования на инциденты информационной безопасности, руководствуясь международными стандартами и прибегая к помощи специалистов в данной отрасли.

ИЛЬМИРА ГАЙСИНА

на правах рекламы

МАЛЫЙ И СРЕДНИЙ БИЗНЕС В КИБЕРСРЕДЕ

КИБЕРСРЕДА – ЭТО УСЛОВНАЯ СРЕДА, В КОТОРОЙ ПРОИСХОДИТ ОБМЕН ИНФОРМАЦИЕЙ ПОСРЕДСТВОМ КОМПЬЮТЕРНЫХ СЕТЕЙ. ПРИМЕР ТАКОЙ СРЕДЫ – ИНТЕРНЕТ. РАБОТА В КИБЕРСРЕДЕ НЕСЕТ ДЛЯ КОМПАНИЙ ОПРЕДЕЛЕННЫЕ РИСКИ, КОТОРЫЕ МОЖНО ПРЕДОТВРАТИТЬ ПРИ СОБЛЮДЕНИИ МЕР КИБЕРБЕЗОПАСНОСТИ.

ЗАЧЕМ НУЖНА КИБЕРСРЕДА?

Использование киберсреды позволяет упростить взаимодействия с партнерами и клиентами, а также увеличить производительность отдельных операций. Ряд компаний просто не могут существовать без киберсреды. Это, например, банки, финансовые корпорации и другие крупные компании.

Киберсреда также важна для малого и среднего бизнеса, так как обмен данными с помощью информационных технологий (далее – ИТ) позволяет бизнесу расти и приносить прибыль. ИТ – это и один из факторов конкурентного преимущества для бизнеса, поскольку в этой сфере постоянно появляются новые направления. Например, сегодня активно развивается технология EDI (Electronic data interchange – Обмен электронными данными), обеспечивающая оперативный обмен информацией между контрагентами. Использование EDI позволяет:

– оперативно получить, обработать и отправить заказ в магазин или в распределительный центр;
– минимизировать бумажный обмен;
– минимизировать количество ошибок при обмене информацией;
– контролировать качество, сроки исполнения заказа – как со стороны магазина, так и со стороны поставщика;
– соблюдать требование поставщика / сети магазинов об электронном обмене.

РИСКИ В КИБЕРСРЕДЕ

Но киберсреда – это не только преимущества. Она несет в себе множество ИТ-рисков, которые иногда не учитываются, так как лежат вне области рассмотрения стандартных рисков компании. В мире уже давно ведется борьба с причинами и последствиями реализации киберрисков, вырабатываются и обновляются стандарты и подходы по борьбе с их реализацией. Это, например, стандарт ISO/IEC 27032:2012 Информационные технологии – Методы обеспечения безопасности – Руководство по кибербезопасности (Information technology – Security techniques – Guidelines for cybersecurity[1]), в котором приводится список таких киберрисков, как проникновение в информационные системы, атаки на информационные ресурсы компании, использование программ-шпионов и вредоносного программного обеспечения (далее – ПО) и др.

ИСТОЧНИКИ КИБЕРАТАК

Распространитель кибератаки благодаря широкому развитию ИТ-инфраструктуры и разнообразию методов проведения кибератак может находиться в любой точке мира. Атака часто выполняется опосредованно через сотрудников компании или других участников электронного взаимодействия, которые могут не подозревать о своем участии. Фактически такими источниками может быть как один человек, так и целая команда, распределенная по киберсреде.

ПРИМЕРЫ ПОСЛЕДСТВИЙ КИБЕРАТАК

Информация о кибератаках на крупные компании регулярно появляется в прессе, тогда как новости об атаках на малый и средний бизнес практически не обнародуются. Это происходит потому, что, во-первых, компании часто не замечают атаки и ее последствий, а во-вторых, не хотят об этом заявлять открыто для сохранения репутационного имиджа. Последствия от кибератаки могут быть как незаметными в ближайшей перспективе (например, утечка информации к конкурентам, установка программ слежения за компьютерами), так и явными (блокировка приема заказов в интернет-магазине на сайте компании, несанкционированное исполнение платежей в «Клиент-Банке» компании).

ЗАЧЕМ НУЖНА КИБЕРБЕЗОПАСНОСТЬ?

Кибератаки не всегда идентифицируются установленным антивирусным ПО, так как могут создаваться для конкретного случая, в частности для атаки на определенную компанию. Пример – вирус, встроенный в сообщение электронной почты и созданный для хищения какой-либо информации у конкретной компании. Из-за его специфики антивирусная программа не идентифицирует вирус, что позволяет вредоносной программе приступить к осуществлению заложенной в нее функции. Таким образом, для выявления и предотвращения реализации киберриска нужны нестандартные методы и наличие отлаженного процесса кибербезопасности.

СПОСОБЫ БОРЬБЫ С КИБЕРАТАКАМИ

Кибератаки поястоянно видоизменяются, поэтому у компаний не всегда получается бороться с ними самостоятельно. Помочь в этом могут службы мониторинга и антивирусы, а также внутренние и внешние ИТ-службы. На уровне государств в последнее время также активно создаются и развиваются службы по борьбе с киберпреступностью.

Основной принцип борьбы с киберугрозами – это определение киберрисков и внедрение процессов, минимизирующих их, постоянный мониторинг новых ИТ-областей и методов кибератак, а также соответствующая работа с персоналом. Эти меры позволяют своевременно выявить и не допустить или минимизировать последствия кибератак на значимые активы компании. При этом новый процесс – это не обязательно новый персонал: кибербезопасности можно достигнуть и благодаря получению дополнительной компетенции имеющимся сотрудником.

Киберриск должен постоянно учитываться и пересматриваться при осуществлении компанией своей деятельности, благодаря уже внедренным процессам информационной безопасности и информационным технологиям. К киберрискам необходимо готовить не только ИТ-инфраструктуру, но и персонал компании посредством регулярного информационного оповещения, проверки знаний информационной безопасности. Таким образом создается подготовленная среда, которая поможет предотвратить и выявить кибератаки как можно раньше.

Анастасия Терехина, АССА, старший менеджер департамента аудита, сертифицированный аудитор
Лев Батищев, старший аудитор по информационным технологиям

1 https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.