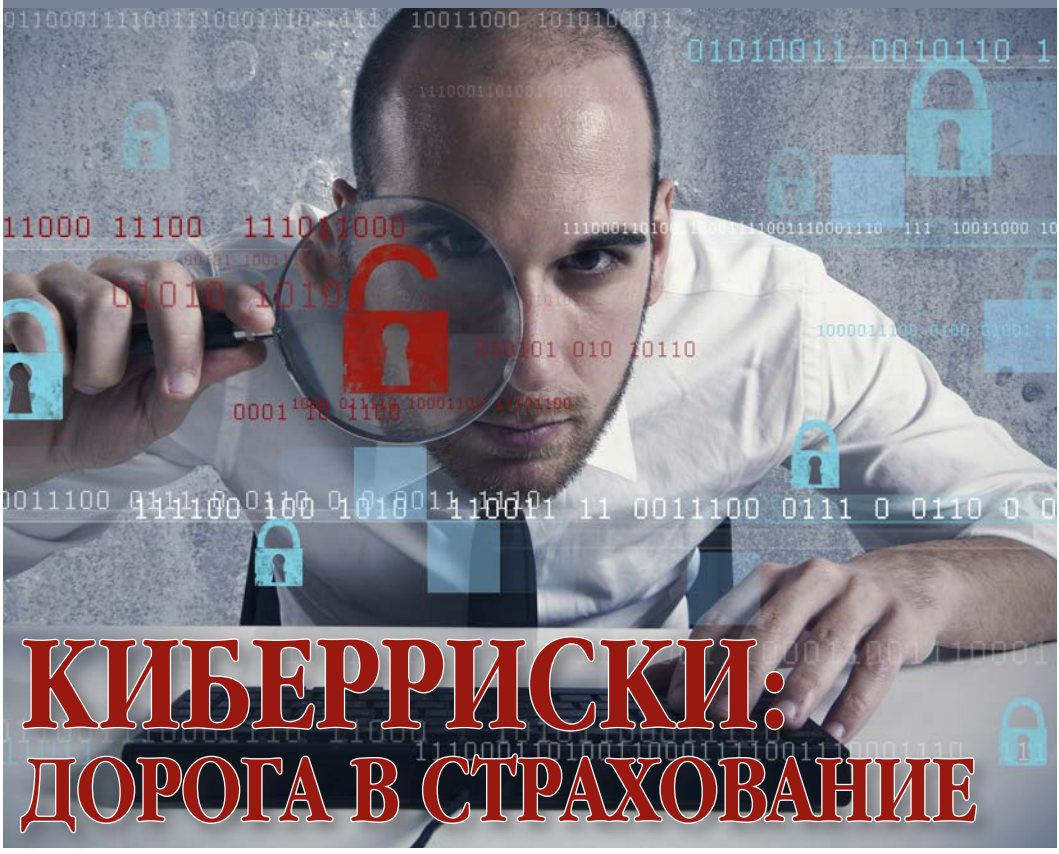
Среди окружающей природы человек находится под влиянием бесчисленных сил, то полезных, то вредных и разрушительных для его существования, в зависимости от условий, при которых наступает действие этих сил, и от их интенсивности.

А. А. Шахт. 1899 г.



КИБЕРРИСКИ: ДОРОГА В СТРАХОВАНИЕ

Кибермошенничество стало повседневной реалией в нашей стране. В ситуации, когда граждане и предприятия несут убытки, страховое сообщество может и должно доказать эффективность передачи киберрисков в страхование.

Развитие науки и техники, значительно увеличивая производительность труда и способствуя росту благосостояния людей, одновременно рождает и новые риски. Взрывы газов, падение летательных аппаратов, загрязнение окружающей среды, радиация — явления, появившиеся как результат прогресса всего за сто лет.

К сожалению, всегда находятся те, кто использует свои знания и достижения человечества для быстрого и незаконного обогащения. Так, с развитием информационных технологий появился абсолютно новый вид правонарушений — кибермошенничество.

Высокотехнологичная преступность динамично развивается в ногу с современной наукой и техникой, независимо от того, что мы про это думаем. В ответ на это нашему обществу пред-

стоит разработать и внедрить в ежедневный обиход организационные, технические и информационные системы защиты.

Малые предприятия и физические лица считают, что они не представляют интереса для киберпреступников. Крупные предприятия, имеющие полноценные департаменты безопасности и информационных технологий, полагают, что надежно защищены от кибермошенников. Ошибаются и те, и другие.

Почти ни у кого нет продуманных планов по реагированию на киберугрозы и проникновения, хотя четкие и незамедлительные действия могут если не предотвратить негативные последствия полностью, то минимизировать их в значительной степени.

Взломы информационных систем происходят как в незащищенных, так и в самых надежных местах. Киберпреступники постоянно совершенствуются, меняют методы и инструментарий атак после каждого обнаружения и раскрытия.

На каждый уровень защищенности системы находится мошенник более высокого уровня подготовки.

Кибератаки происходят с применением самых последних технологий и имеют гораздо более серьезные последствия, чем обычные кражи. Почти в любом виде деятельности используются компьютерные системы и электронные базы данных. Когда они подвергаются воздействиям компьютерных вирусов или кибератак, возникает опасность раскрытия или потери важной информации, непосредственно влияющей на оперативную работу предприятий или содержащей конфиденциальные данные третьих лиц. Более того, деятельность предприятия может быть полностью заблокирована.

Особо уязвимы предприятия малого и среднего бизнеса, которые зачастую имеют ограниченные ресурсы как аппаратных средств защиты, так и программных систем безопасности. Урезанная система безопасности делает их легкой добычей злоумышленников.

Взлом развитой системы безопасности, регулярно перенастраиваемой под активные виды угроз, умеющей распознавать и реагировать на сами атаки, менее вероятен. А заранее спланированный алгоритм ответов на проникновение зачастую позволяет предотвратить негативные последствия даже в случае успешной атаки. Тем не менее, внедрение в информационные банки данных — повсеместное явление в наши дни. Факт проникновения и наличия уязвимости может оставаться нераскрытым более года. Современные средства защиты могут лишь снизить вероятность проникновения в систему или минимизировать возможные негативные последствия типа потери или повреждения данных.

Андрей Богачев

Президент ООО «ЛЭББ»

Профессионалы говорят: «Ваша база данных уже вскрыта, вы просто об этом еще не знаете».

Россия пока далека от стран — лидеров по количеству киберпреступлений, но число атак, так же, как и размеры убытков их сопровождающих, растут год от года.

По данным открытых источников, совокупный убыток от зарегистрированных киберпреступлений в России за 2015 год составил порядка 200 млрд рублей или более. При этом надо понимать, что многие учреждения, оберегая свою репутацию, стремятся не афишировать такие случаи, поэтому реальные цифры значительно больше. В то же время, в мире годовые убытки от киберпреступлений исчисляются в сотнях миллиардов долларов.

Виды атак против компаний и граждан:
- Нецелевые атаки (фишинг, кардинг, sms-мошенничество)
- Целевые атаки (финансовое мошенничество, хищение баз данных, промышленный шпионаж, DDoS-атаки, вымогательство)
- Атаки изнутри (хищение, уничтожение информации, содействие целевой атаке)

Потенциальные виды убытков:
- Прямой ущерб (хищение средств, утрата информации, повреждение программного обеспечения, поломка оборудования и т. п.)
- Убытки от перерыва в коммерческой деятельности
- Ответственность перед третьими лицами (за нанесенный вред, разглашение информации)
- Ущерб вследствие хищения интеллектуальной собственности
- Ущерб репутации компании
- Дополнительные расходы (PR, юридические услуги и т. д.)

Принимая во внимание, что количество устройств, соединенных между собой посредством глобальной сети, увеличивается год от года, можно однозначно прогнозировать как развитие информационных технологий, так и рост преступлений в этой отрасли.

Возможность завладения огромными денежными суммами, отсутствие неотвратимости наказания и его относительная легкость будут дополнительно стимулировать рост киберпреступности в ближайшем будущем. Злоумышленники охотятся как за деньгами, так и за персональными и конфиденциальными данными как отсроченным средством получения денег.

Информационные технологии как эффективный инструмент влияния и устрашения всё чаще используется и террористами. Отключение всех светофоров, мобильной связи, утеря контроля над телевизионным эфиром, сбой движения транспорта, отключение электроэнергии и начало полного разрушения инфраструктуры всей страны красочно показано в «Крепком орешке–4», вышедшем на экраны еще в 2007 году. О возможности массового страхования киберрисков в нашей стране тогда вообще не говорили.

Чем больше мы доверяемся информационным технологиям, чем шире компьютеры и «умные» устройства внедряются в нашу жизнь, тем значительнее могут быть потери от кибератак.

Гарантированной защиты от кибермошенничества нет — это факт. Такое мошенничество обладает признаками непредсказуемости, внезапности, случайности и независимости от воли владельца риска. Это позволяет использовать страхование как эффективный инструмент уменьшения негативных финансовых последствий от таких событий. Кроме того, разрабатываемые в ходе создания страховой программы меры защиты в значительной степени предохраняют от таких рисков.

Ввиду специфичности киберрисков и особенностей расследования убытков, связанных с кибермошенничеством, профессиональных консультантов целесообразно привлекать уже на этапе заключения договора страхования, не говоря уж об урегулировании убытков.

Предстраховой аудит включает:
- Оценку рискозащищенности объекта
- Определение возможных угроз
- Разработку сценариев наиболее вероятных убытков
- Рекомендации по повышению уровня защищенности и предотвращению возможных убытков
- Разработку инструкций по действиям в случае чрезвычайных ситуаций
- Определение возможного влияния киберрисков на производственную деятельность
- Расчет финансовых показателей и возможных убытков

Тесты для оценки рискозащищенности объекта:
- Сетевая разведка аффилированных сетевых ресурсов
- Автоматизированное сканирование уязвимостей
- Ручная эксплуатация выявленных уязвимостей
- Нагрузочное тестирование критичных ресурсов и др.

Компания ЛЭББ, работая совместно с международными компаниями, лидирующими в области предотвращения и расследования киберпреступлений и высокотехнологичных краж, проводит предстраховую экспертизу объектов в части киберрисков при заключении договора страхования (pre-risk), а также расследование и урегулирование убытков в период действия полиса.

Предстраховой отчет содержит выводы об уровне защищенности информационных активов компании, описание рисков, советы по улучшению системы безопасности, а также финансовые показатели, необходимые для создания соответствующей конкретным конфигурациям информационной системы страхователя эффективной страховой программы.

Системы безопасности требуют постоянной доработки, так как методы злоумышленников все время меняются. В крупных организациях необходимость модификаций вызвана еще и постоянным появлением новых пользователей, устройств и программных продуктов, увеличивающих вероятность появления новых уязвимостей.

Контроль системы безопасности необходим не только внутри компании, но и в границах всех связей компании с партнерами, исполнителями, поставщиками. Так, взлом информационной системы партнера может быть предвестником атаки на вашу компанию. Поэтому помимо уменьшения собственных киберрисков и их страхования встает вопрос о защите поставщиков и агентов от аналогичных угроз, так как нарушение их работы может и косвенно, и прямо влиять на результаты деятельности вашей компании.

Процедуры расследования и урегулирования:
- срочное реагирование на возникающие угрозы (пресечение действий, рекомендации по минимизации ущерба);
- расследование обстоятельств и причин убытка, поиск виновника;
- юридический анализ, определение факта наступления страхового случая;
- расчет размера понесенных убытков;
- оценка перспектив суброгации и содействие в реализации требования.

В страховых убытках, связанных с киберпреступлениями, довольно часто есть возможность для суброгации, так как большинство событий вызываются умышленными действиями. В отличие от других видов преступлений, обнаруженные киберпреступления могут быть раскрыты

довольно быстро. Во многих случаях злоумышленник может быть опознан и арестован до того, как он успел потратить украденные средства. Следовательно, возврат украденных средств становится реальным и перспективным направлением работы при условии проведения четких, своевременных и профессиональных мероприятий.

Различные виды страхования от киберрисков существуют в мире и развиваются уже более 10 лет, но в России самые передовые страховщики заговорили о таком страховании лишь недавно. На прошедшей в апреле 2016 года конференции по перестрахованию ведущие российские и европейские перестраховщики отнесли киберстрахование к самым перспективным направлениям развития страхового бизнеса завтрашнего дня.

! *Бизнес завтрашнего дня — это работа всех участников процесса страхования сегодня.*

Сегодня ощущается недостаток достоверных данных о киберпроисшествиях и их последствиях, отсутствует понимание выгоды от страхования этих рисков, так как отсутствует четкий алгоритм оценки этих рисков. Именно поэтому полисы, на сегодня представляющие собой унифицированные «коробочные» продукты, мало интересуют страхователей.

А тем временем, киберриски уже сейчас могут достигать размеров, позволяющих отнести их к катастрофическим. Если потеря базы данных одного предприятия может надолго вывести его из строя, то нарушение в работе «облачного» сервиса или обрушение сети Интернет может привести к коллапсу с тяжелейшими экономическими, экологическими и социальными последствиями на значительных территориях.

Примеры киберпреступлений, расследованных в России

(информация предоставлена компанией Group-IB, одной из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничества с использованием высоких технологий)

Группа Germes
Крупнейшая в России бот-сеть, объединившая 4,5 млн зараженных компьютеров. Объем хищений, организованных с ее помощью, оценивается более чем в 150 млн рублей. Организатор преступной группы, действовавшей на территории нескольких стран, **найден и арестован**.

Группа Hameleon
Первая в России бот-сеть, предназначенная для хищения денег с банковских счетов физических лиц. Преступники осуществляли атаки на клиентов банков с использованием поддельных SIM-карт. Организатор преступной группы **найден и арестован**. Предотвращено хищений на сумму более 1 млрд рублей.

Dragon
Создатель бот-сети для организации заказных DDoS-атак. Жертвами группы стали несколько британских и российских компаний, в том числе один из ТОП-10 крупнейших российских банков. Организатор преступной группы **найден и задержан**.

PumpWaterReboot
Хакер, стоящий за DDoS-атаками на «Тинькофф. Кредитные Системы», «Альфа-Банк», «Промсвязьбанк», «Лабораторию Касперского» и крупные интернет-порталы. Вымогал деньги за прекращение атак. **Найден и арестован**.

Зона наибольшего риска:
- финансовые компании;
- социальные сети;
- организации здравоохранения;
- операторы связи;
- промышленные предприятия;
- телекоммуникации;
- энергетика.

Наиболее подвержены киберрискам компании, опирающиеся на оцифрованные базы данных и информационные технологии. Страхование киберрисков начинается именно с таких крупных предприятий, распространяясь затем на малые и средние.

Ускоряется развитие киберстрахования и с появлением связанного покрытия от перерыва в производстве, так как для многих предприятий потеря самих данных и ответственность за такую потерю может быть материально менее значима, чем финансовые убытки от простоя.

Растущий ежедневно поток информации о киберпреступлениях, а также осведомлённость общества о значительных финансовых последствиях таких преступлений способствует развитию страхования от киберугроз. В странах с законодательным требованием о раскрытии информации о кибератаках и с высоким уровнем ответственности за несохранность данных киберстрахование развивается ускоренными темпами.

Приходится признать, что случаи кибермошенничества в нашей стране стали ежедневной реалией, население страны и предприятия несут убытки. Задача страхового сообщества — подсказать решение проблемы, аргументированно продемонстрировав эффективность передачи киберрисков в страхование.

Очевидно, что высокие премии, узкое покрытие и огромный перечень исключений вряд ли убедят страхователя в выгодности нового продукта. Необходимы разумные, ясно сформулированные правила страхования. Так что дело за страховщиками.