Кибербезопасность

Приоритет — сохранить информацию | А3

Российский рынок информационной безопасности перестраивается на фоне участившихся хакерских атак и ухода зарубежных разработчиков ПО

ПРИЛОЖЕНИЕ К «РОССИЙСКОЙ ГАЗЕТЕ» | 18 мая 2022 среда | № 105 (8753)

РЕШЕНИЕ / Бизнес учится защите от нападений хакеров

Умей постоять за себя

Леонид Федоров

В России к 2024 году планируется открыть 15 опорных центров Национального киберполигона. На данный момент действует семь опорных и один образовательный центр. Создание Национального киберполигона началось в 2019 году. Это электронная тренировочная площадка, на которой компании и организации отрабатывают защиту от киберугроз в максимально реалистичных условиях. После хакерских атак в марте—апреле на сайты госорганов, федеральных СМИ и стратегических предприятий стало ясно, насколько такой центр необходим и как вовремя он был создан. Кто из бизнеса стал первопроходцем в этой сфере, как проходят учения на полигоне и можно ли прокачать здесь свой собственный бизнес, выяснил корреспондент «РГ».

Национальный киберполигон появился в рамках национальной программы «Цифровая экономика» на базе компании «Ростелеком-Солар».

—Говоря простыми словами, полигон—это «цифровые копии» предприятий. На этой площадке эмулируются процессы, которые происходят на предприятиях в реальной жизни. У нас есть оборудование и системы для отработки любых сценариев атаки,—рассказал «РГ» Александр Чечин, заместитель генерального директора компании «Ростелеком-Солар».—Эти сценарии разрабатываются на основе действий реальных злоумышленников. И они постоянно обновляются. Мы тесно работаем с экспертами крупнейшего в России Центра противодействия кибератакам SolarJSOC, который анализирует порядка 110 миллиардов событий безопасности в сутки. Это позволяет создавать условия, максимально приближенные к реальной жизни, и отрабатывать защиту без риска реального ущерба для предприятий.

> На сегодняшний день в Российской Федерации работает восемь центров Национального киберполигона

Сейчас на полигоне есть четыре «отраслевых» сегмента: корпоративный (имитируется типовая офисная инфраструктура), электроэнергетический (моделируются типовые объекты электрических сетей), нефтегазовый сегмент, а также банковский сектор, где эмулируется типовая ИТ-инфраструктура финансовой организации, в том числе система банковского обслуживания и процессинга. В этом году планируется расширить банковский сектор, а также запустить два новых сегмента—нефтепереработки и магистральных сетей связи. А к 2024 году их дополнят сегменты транспортной, металлургической и горнодобывающей отрасли.

Спрос на такие услуги есть не только в Москве и Санкт-Петербурге—активно развивается сеть опорных центров и в регионах. Им предоставляется полный доступ к инфраструктуре Национального киберполигона. И в этом смысле любая компания из самого отдаленного субъекта России получает тот же набор услуг, что и столичные компании первого эшелона.

Один из ярких примеров—корпоративные учения для сотрудников Трубной Металлургической Компании (ТМК) и Группы Синара, которые прошли в прошлом году. На них впервые в России специалистам удалось отработать все без исключения процессы служб информационной безопасности.

А2

СТРАТЕГИЯ / Россия принимает дополнительные меры для надежной работы информационных систем

Отбить атаку

РИА НОВОСТИ

Правительство РФ рекомендовало госорганам ограничить использование иностранных средств защиты информации.

Михаил Калмацкий

Количество кибератак на российские ресурсы в последние месяцы выросло в разы. Многим организациям и особенно госорганам пришлось держать настоящую оборону от хакеров. Логично, что в таких условиях в России стали принимать меры для повышения уровня кибербезопасности.

В начале мая президент России Владимир Путин подписал Указ «О дополнительных мерах по обеспечению информационной безопасности РФ». Руководителям ведомств, регионов, госкорпораций, стратегических предприятий было поручено создать структурное подразделение для обеспечения информационной безопасности, в том числе обнаружения, предупреждения и ликвидации последствий компьютерных атак. Глава государства также поручил правительству определить перечень ключевых органов (организаций), которым необходимо оценить уровень защищенности своих информационных систем. Помимо этого указ запрещает органам власти и ряду организаций с 1 января 2025 года использовать средства защиты информации, произведенные в недружественных странах.

АКЦЕНТ

ПЕРЕХОД НА РОССИЙСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОВЫСИТ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дополнительные меры потребовались после того, как на российские сайты обрушилась беспрецедентная волна кибератак. Только в начале этой волны, 26 февраля, было зафиксировано более 50 DDoS-атак мощностью более одного терабайта, а также ряд профессиональных целевых атак на портал госуслуг. Как пояснили «РГ» в Минцифры России, объектами киберпреступников становились сайты госорганов и СМИ.

В основном в отношении России использовались стандартные атаки, рассказал генеральный директор АНО «Цифровые платформы» Арсений Щельцин. «Первое, это были DDoS-атаки на сервера для повышения нагрузки на них. Второе—попытки взломов администраторских учетных записей различных сервисов. Цель—смена информации или ее скачивание и использование для чего-то незаконного,—пояснил эксперт.—Для кибератак привлекались разные компании, с разным уровнем экспертизы и инструментария. При этом, можно сказать, что задача была повысить скорее количество, а не качество атак».

Дополнительные сложности для кибербезопасности создало введение санкций в отношении России и уход с нашего рынка целого ряда иностранных разработчиков программного обеспечения. В результате само наличие иностранного ПО стало в определенной степени фактором риска. И с этим нужно было что-то делать.

Как сообщили «РГ» в минцифры, правительство ранее выслало госорганам рекомендации по обеспечению безопасности информационных ресурсов. «Были направлены следующие рекомендации: отключение автоматических неконтролируемых обновлений иностранного ПО, ограничение использования иностранных средств защиты информации, блокировка удаленного доступа иностранных подрядчиков в сети органов государственной власти, получение гарантийных обязательств от поставщиков и производителей по исполнению госконтрактов в сфере информационно-коммуникационных технологий»,—рассказали в министерстве.

«На время переходного периода к полному импортозамещению требование отказаться от обновлений все еще эксплуатируемого ПО—мера вынужденная,—отметил специалист департамента анализа защищенности Digital Security Александр Багов.—В результате сокращается риск отказа в обслуживании производителями, к которым нет полного доверия, однако значительное количество информационных систем окажется беззащитными перед новыми угрозами. Их несут постоянно выявляемые новые уязвимости, которые в отсутствии вендорских обновлений останутся неисправленными».

Проблема касается разных видов ПО, включая операционные системы. Если не обновлять ОС Windows, в ней возникают уязвимости и серьезно возрастают риски, связанные с безопасностью, рассказал «РГ» руководитель направления перспективных исследований ГК «Астра» Роман Мылицын. «Для рядовых пользователей это может не так важно, но для организаций—критичный момент,—считает он.—Думаю, сейчас компании постараются управлять этими рисками. Например, изолировать свой контур ИТ-инфраструктуры от внешнего интернета, чтобы сократить возможность попадания вредоносного ПО. Но это временная мера, ведь сидеть в закрытом контуре, выходя в Сеть через один компьютер, не очень удобно. Полагаю, что многие крупные компании это не устраивает, и они будут строить альтернативную инфраструктуру на российских ОС».

А2

СОБЫТИЕ / Эксперты обсудят новые вызовы ИТ-отрасли

Вирусы берут на прицел

Сергей Григорьев

Сегодня в Москве открывается ежегодный международный форум по практической кибербезопасности Positive Hack Days. Российские и зарубежные разработчики программного обеспечения, «белые» хакеры, представители бизнеса и госструктур, молодые ученые собираются вместе, чтобы обсудить новые технологические вызовы в сфере информационной безопасности и способы их решения.

В программе форума традиционно представлено три больших трека, посвященных отражению атак, защите через нападение и влиянию кибербезопасности на бизнес. Из выступлений докладчиков можно, например, узнать секрет обнаружения большинства кибератак. Оказывается, для этого достаточно знать ограниченный список техник, которые используют почти все злоумышленники независимо от квалификации.

А что если компьютер поражен руткитом—программой, позволяющей скрыть присутствие вредоносного ПО в системе? Появляются все новые семейства таких программ, и остановить их становится все сложнее. В одном из докладов предлагается рассмотреть наиболее яркие примеры руткитов последних лет и множество подходов к их обнаружению. Еще одно выступление посвящено фишингу. Обычно для него используются поддельные сайты, но может случиться и так, что сайт настоящий, просто имел место взлом. Как это происходит, ясно из примеров, показывающих, что жертвами таких атак становятся не только маленькие организации, но и крупные банки и авиакомпании.

> Для обнаружения кибератаки нужно знать ограниченный список техник, которые используют почти все злоумышленники

Важное место на форуме PHDays занимают также конкурсы. Их задача—не только развлечь, но и помочь получить полезные знания и ценный опыт. Так в программе запланирован конкурс, посвященный поиску уязвимостей в банковских системах. Он состоит из теории и практики. Сначала идет рассказ экспертов о работе и слабых местах различных платежных устройств, а затем участники могут испытать систему безопасности настоящего банкомата, кассовой системы и POS-терминала. Другой конкурс может приглянуться любителям испытать на прочность системы сетевой защиты. Перед ними ставится задача найти слабости в шести сервисах и добыть флаги за выполнение заданных условий, а также обойти IDS—систему обнаружения вторжений, которая пропускает через себя трафик и блокирует попытки сетевых атак.

Другие развлечения для гостей форума—фестиваль анимации HackerToon и финал первого Всероссийского конкурса open source проектов школьников и студентов по направлению «Кибербезопасность», организованного Кружковым движением Национальной технологической инициативы.

Как и год назад, на площадке PHDays проводятся крупнейшие открытые киберучения—The Standoff. В этот раз для них специально создано виртуальное государство F. Его инфраструктуру атакуют 17 команд белых хакеров, а пять команд защитников в режиме реального времени выясняют, как недопустимое стало возможным. Ситуации берутся из жизни, но масштаб возможных катастроф растет: представьте, что вирус-шифровальщик останавливает нефтепровод и создает дефицит топлива в стране или атаки на систему управления электроподстанциями вызывают перебои в подаче воды в жилые дома. Учения пройдут два дня, как и сам форум, который завершится 19 мая. ●

СИТУАЦИЯ / Российские компании обеспокоены безопасностью данных в облаках

Воздушная оборона

Анастасия Павлова

Расходы на облачные технологии в России до 2024 года, по оценкам Accenture, будут увеличиваться на 5,3 процента ежегодно. Треть компаний используют облака более пяти лет, а 47 процентов начали работать с ними в последние три-пять лет. При этом 67 процентов фирм обеспокоены сохранностью данных при выборе публичного провайдера. Впрочем, как отмечают эксперты, безопасность облачных сред в России находится на высоком уровне благодаря законодательной поддержке и жестким требованиям к обеспечению информационной безопасности.

Существует стереотип, что облачные технологии небезопасны и уязвимы. Но, по мнению экспертов, облачное хранение лучше серверного. Российские компании географически распределяют дата-центры, уровень защиты данных часто относится к высокой категории TIER 3, а внутри компании не существует «суперадмина», который имеет доступ ко всему пользовательскому контенту.

Цифра

67

процентов

фирм переживают за сохранность данных при выборе публичного провайдера

«В случае мошеннических взломов облачные компании могут оперативно заблокировать доступ к данным и быстро восстановить безопасность благодаря масштабируемости и налаженности системы. Если же взлом происходит с традиционной системой хранения данных на сервере, последствия будут намного серьезнее»,—говорит Артур Хасиятуллин, региональный директор TraceAir в России.

Часто угроза облаков лежит в плоскости цифровой гигиены пользователей, а не безопасности самой системы. Аналитики из Unit 42 проанализировали 18 тысяч облачных учетных записей и пришли к выводу, что причиной киберуязвимостей являются неправильные настройки аккаунта компании (65 процентов), ненадежный пароль (53 процента) или повторно использованный пароль (44 процента).

«Более половины успешных атак происходит по вине самих пользователей,—говорит независимый эксперт Кирилл Солодовников.—Если в корпоративном сегменте дела обстоят более-менее хорошо, так как вопросы безопасности обеспечивает внутренняя служба, то у физических лиц—существенно хуже. Люди не всегда применяют сложный пароль, используют облачные сервисы из публичных точек доступа, более подвержены социальной инженерии и фишингу со стороны злоумышленников».

АКЦЕНТ

БОЛЕЕ ПОЛОВИНЫ УСПЕШНЫХ АТАК ПРОИСХОДИТ ПО ВИНЕ САМИХ ПОЛЬЗОВАТЕЛЕЙ

Поэтому сейчас больше внимания стоит уделять обучению пользователей базовым правилам информационной безопасности и информационной гигиене при работе с онлайн-ресурсами.

Облачные технологии выгодны. Согласно исследованию Accenture, 96 процентов компаний уже сократили затраты на ИТ благодаря облакам. В среднем экономия составила 7,9 процента. При этом 83 процента респондентов считают облака компонентом гибкости и расширенных возможностей, а 73 процента полагают, что cloud-технологии помогают снижать риски и преодолевать неопределенности на рынке.

В России почти каждая организация стала использовать тот или иной тип облака за последнее десятилетие. Результаты впечатляют: почти три четверти добились экономии в среднем до 10 процентов. Но всего 12—15 процентов компаний не останавливаются только на миграции в облако, а рассматривают облака как среду возможностей для достижения гибкости бизнеса на турбулентном рынке, отмечают в Accenture.

«Мы как сервис, который переводит бизнес на работу в облаке, уверены, что облачные технологии в России безопасны. И продолжаем убеждать в этом компании, которые все еще хранят свои данные на локальных серверах»,—рассказывает Филипп Щиров, сооснователь и директор сервиса облачной автоматизации бизнеса Altapp. По его оценке, доверие к облачным технологиям растет, рынок увеличивается на 25—30 процентов в год.

Если бизнес хранит свои данные у публичного провайдера на аутсорсинге, то получает актуальную систему безопасности за небольшую цену подписки. При этом провайдеры постоянно модернизируют системы, обладая огромным опытом. Публичные провайдеры несут как материальную, так и уголовную ответственность за утечку персональных данных. Также у них должен быть аттестат соответствия сервиса требованиям безопасности информации.

И все-таки угрозы есть. Василий Степаненко, директор центра киберзащиты DataLine, рассказывает, что среди распространенных угроз можно выделить DDoS-атаки разных типов. При атаке на сайт злоумышленники автоматически направляют большое количество запросов с помощью специальных программ-ботов. Из-за резкого роста нагрузки веб-ресурс может выйти из строя, и пользователи не смогут на него зайти, а сотрудники компании могут потерять доступ к своим системам, например, к почте. Это один из самых распространенных типов атаки, и от него можно защититься с помощью AntiDDoS-решений, которые распознают трафик от ботов и блокируют его.

А4

УГРОЗЫ / Системы управления транспортным комплексом должны регулярно обновляться

Светофор под прикрытием

Ирина Фурсова

Организация движения различных видов транспорта все сильнее зависит от современных технологий. Внедрение интеллектуальных транспортных систем (ИТС) в агломерациях должно завершиться к 2024 году. В крупных городах как грибы после дождя появляются умные переходы, светофоры, остановки. И чем «интеллектуальнее» становится транспортный комплекс, тем удобнее и комфортнее он для пользователя услуг и тем уязвимее для различных видов кибератак—при отсутствии должной защиты, разумеется.

Сегодня для того чтобы создать транспортный коллапс достаточно вывести из строя светофор на пересечении улиц с плотным трафиком. Особенно если среди участников движения окажутся беспилотные ТС, ибо «живые» водители как-то смогут договориться о приоритетном проезде.

К счастью, наш транспортный комплекс пока не пропускал нокаутирующий удар на системы управления, хотя железнодорожники уже противостояли попыткам сбить график движения поездов. А вот в мире имеются примеры кибератак, достигших цели: выводились из строя автоматизированные системы управления (АСУ) в портах Барселоны и Сан-Диего, система пограничного контроля в аэропорту Стамбула и т.д.

Так какой защитой должны быть экипированы АСУ транспортным комплексом, и реально ли обеспечить их полную неуязвимость? Обратимся к экспертам.

«Средства защиты информации транспортной инфраструктуры прежде всего должны иметь сертификаты ФСТЭК, ФСБ и других регуляторов, и по возможности быть отечественного производства,—сообщил «РГ» директор по продуктам и технологиям Группы Т1 Александр Рожков.

А2

КАДРЫ / Учебную программу готовы корректировать под запросы бизнеса

Образовательный прогресс

Андрей Иванов,
заведующий кафедрой защиты информации НГТУ

ПРЕСС-СЛУЖБА НГТУ

Андрей Иванов: Мы стараемся показать студентам все многообразие нашего направления.

Информационная безопасность (ИБ) — направление относительно молодое. Первые профильные кафедры стали появляться 20–25 лет назад. Нашей кафедре 17 лет. Сейчас это направление развивается очень активно. Если в 2020 году набор на первый курс Новосибирского государственного технического университета НЭТИ составил 120 человек, то в 2021-м уже 150. Интересно, что в прошлом году впервые ребята, не добрав один-два балла при поступлении на бюджет, осознанно оставались на ИБ по контракту. Раньше в подобной ситуации они шли на другие специальности. Кстати, всегда есть шанс в дальнейшем перевестись на освободившееся бюджетное место.

Увеличение количества студентов, с одной стороны, хорошо, с другой — повышенная нагрузка на кафедру. Мы, как и ИТ-компании, стоим в очереди за квалифицированными кадрами, в нашем случае преподавательскими. Абсурдно думать, что, не имея хороших кадров в вузе, можно подготовить современного специалиста, обладающего знаниями мировых компетенций. Поэтому мы стараемся привлекать молодежь и создавать для них хорошие условия, в том числе финансовые (доход молодого специалиста в вузе должен быть соизмерим с рынком). Хотелось бы, чтобы недавно озвученные меры поддержки ИТ-сектора распространялись не только на бизнес, но и на образовательные учреждения.

Несколько лет назад, когда я только начал руководить кафедрой, задался вопросом: почему мы не так активно актуализируем содержательную часть наших образовательных программ с бизнесом, по сути, основным заказчиком? Вузам в первую очередь нужно ориентироваться на запрос рынка и пытаться угнаться за теми темпами развития, которые в этой области присутствуют. А они очень высокие — некоторые технологии развиваются и полностью уходят за 3–5 лет. Отрасль развивается стремительно, и бизнесу в кратчайшие сроки необходимо интегрировать новый запрос на знания тех или иных технологий в учебный процесс. Но образовательный стандарт невозможно так быстро изменить. Поэтому нужен механизм постоянной актуализации именно содержательной части образовательного процесса, чтобы эту повестку формировал в большей части потребитель наших кадров.

> Этот период может стать драйвером развития отрасли информационной безопасности

Мы провели большую работу с местными и федеральными компаниями из области ИБ (разработчики, интеграторы, регуляторы). На общедоступной онлайн-платформе был визуализирован наш учебный план. За пару месяцев порядка 30 экспертов — сотрудники компаний, а то и целые коллективы — прокомментировали содержательную часть, указали на слабые места, разрывы между образованием и реальной работой. Были внесены оперативные правки в учебные планы. Да, мы сами себе подняли планку, по некоторым вопросам у нас не было преподавателей или материальной базы, но проблему нужно решать исходя из запросов рынка и уже для их реализации искать возможности, а не наоборот.

По-хорошему, подобная онлайн-система не должна решать лишь задачи отдельного вуза, она должна быть представлена на федеральном уровне. В таком случае любой участник процесса — министерство, бизнес, государство, другие университеты — может включиться в повестку, предложить свой запрос, перенять или поделиться опытом и т.д. Но подобная система не должна превратиться в еще одну бюрократическую схему. Все должно быть гибко, понятно и связано информационной системой вуза.

Следует отметить, что большинство наших партнеров активно взаимодействуют с университетом, все понимают, что кадровую проблему можно решить только сообща. Эксперты компаний участвуют в проведении занятий, разработчики предоставляют свои продукты для изучения (в большинстве случаев бесплатно), преподаватели стажируются на предприятиях, студенты проходят практики — вот тот минимум сотрудничества, который должен быть.

В сфере ИБ за последнее время появилось много направлений, технологии усложняются, работники становятся все более узкоспециализированными. Если говорить об этом «крупными мазками», то специалистов по ИБ можно разделить по следующим направлениям: работа с нормативными документами (фактически специализированные юристы, которые хорошо разбираются в нормативном поле по информбезопасности и знакомы с аттестацией и аудитом объектов информатизации); специалисты по кибербезопасности на различных уровнях (программные продукты, аппаратная часть, работа с сетью или рабочими станциями); специалисты по техническим каналам утечки информации; разработчики подсистем безопасности программных продуктов и т.д. Каждую из этих групп можно разделить еще на множество специализаций.

> Многие после третьего курса подрабатывают по специальности, а на четвертом трудоустроены

Мы еще на начальном этапе обучения стараемся показать студентам все многообразие нашего направления. С третьего курса у них начинается специализация, на производственных практиках они ближе знакомятся с сутью будущей работы. Многие уже после третьего курса подрабатывают по специальности, на четвертом — практически все наши студенты трудоустроены. А по завершении учебы — 100-процентное трудоустройство. Причем пандемия научила работать дистанционно. Многие ребята, сидя в Новосибирске, работают на московские компании, в которых совсем другой уровень зарплат. С одной стороны, это помогает сохранить кадры у себя, с другой — делает переезд в другой регион более доступным и плавным.

В данный момент в плане развития системы подготовки кадров у нас есть идея перевести в вуз на постоянную основу ряд задач профильных партнеров (фактически взять на аутсорсинг). Мы организуем рабочие места, подразделения в расчете на студентов. У них появится возможность подрабатывать, решать реальные задачи партнера, не покидая территории университета. Партнерам это выгодно: им не придется расходовать ресурс на погружение наших выпускников в свои задачи на своей территории. Нам тоже выгодно — у студентов и выпускников не теряется связь с университетом, и они получают дополнительный доход, появляется перспектива построения полноценной карьеры в вузе с уровнем дохода, соизмеримым с рыночным.

Сейчас непростое время для ИТ/ИБ-отрасли. Но я считаю, что этот период может стать драйвером развития и по наполнению рынка специалистами, и по созданию отечественных разработок, систем, и по изменению отношения к информационной безопасности в целом. ●

Умей постоять за себя

А1

ПРЕСС-СЛУЖБА POSITIVE TECHNOLOGIES

На киберполигоне отрабатывается защита без риска реального ущерба для предприятий.

—Подобные киберучения очень полезны для промышленных предприятий, поскольку отрасль постоянно находится под прицелом злоумышленников, — говорит Александр Чечин. — Согласно нашему исследованию, более 92 процентов атак высокопрофессиональных группировок, зафиксированных в прошлом году, пришлось на объекты критической информационной инфраструктуры. Чаще всего атакам были подвержены госсектор, промышленность, энергетика и ВПК.

Большое внимание уделяется подготовке молодых специалистов. По словам Александра Чечина, отрасль испытывает дефицит квалифицированных кадров. Сейчас это примерно 20 тысяч специалистов ежегодно. Классическая модель образования часто не дает учащимся наработать практические навыки защиты от всех современных киберугроз, поэтому такие площадки — реальная возможность молодым ребятам «прокачивать» себя в этих нишах, отмечают опрошенные «РГ» эксперты.

— Мы развернули опорный центр Национального киберполигона на базе нашего вуза и очень довольны результатом, — говорит проректор по учебной работе Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ) Алексей Салмин. — Это позволит Самарскому региону заниматься подготовкой и переподготовкой кадров в сфере информационной безопасности, что важно и для студентов, и для работающих специалистов. Здесь они получат возможность отработать на практике важные навыки, научатся работать с современными средствами защиты информации. Мы планируем и дальше развивать киберполигон, ориентируясь на реализацию образовательных и научно-исследовательских программ в сфере кибербезопасности.

В этом году на Национальном киберполигоне впервые прошел финал Национальной технологической олимпиады для школьников 8–11-х классов по профилю «Информационная безопасность». Специально для финальных соревнований была смоделирована цифровая копия типовой ИТ-инфраструктуры энергетического предприятия. По легенде, на объект энергетики была совершена многоэтапная атака, и школьникам нужно было расследовать цепочку действий условного злоумышленника и устранить последствия атаки. Учащиеся получили уникальный опыт.

— Проводить подобные мероприятия очень важно, поскольку они помогают находить талантливых ребят и повышать их интерес к предметной области, — говорит Александр Чечин. — Примечательно, что в этом году заявки на участие в профиле подали более семи тысяч школьников, а в финал вышли порядка 100 человек из 23 регионов страны. Вообще же мы открыты к различным форматам сотрудничества и готовы создавать опорные центры не только на базе вузов, но и любых других заинтересованных организаций.

Еще один показательный пример — совместная инициатива с Минцифры России по проведению межвузовских олимпиад, на которых студенты различных инженерных вузов соревнуются друг с другом в решении одинаковых практических кейсов в формате киберучений. Студенты и ранее решали задачи по тематике кибербезопасности, но это происходило локально в каждом из учебных заведений. Теперь же на Национальном киберполигоне впервые воплощен формат, когда учащиеся вузов из разных регионов страны собираются вместе на одной площадке, чтобы побороться за первенство в режиме реального времени.

> АКЦЕНТ
> КИБЕРУЧЕНИЯ ПОЛЕЗНЫ ДЛЯ ПРОМЫШЛЕННОСТИ, КОТОРАЯ ПОСТОЯННО НАХОДИТСЯ ПОД ПРИЦЕЛОМ ХАКЕРОВ

— Такой формат мы впервые опробовали в прошлом году, когда провели первые в стране межвузовские киберучения, и продолжаем реализовывать в этом году, — рассказал Александр Чечин. — Так, например, в апреле прошла серия олимпиад среди студентов Северо-Западного, Центрального, Приволжского, Южного и Северо-Кавказского федеральных округов. В августе планируем провести аналогичные соревнования среди учащихся вузов Сибири и Дальнего Востока, а в октябре победители и призеры каждой из олимпиад смогут встретиться в суперфинале всероссийских киберучениях «OpenBonch 2022», которые состоятся на базе Северо-Западного федерального образовательного центра Национального киберполигона в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича. Мы считаем, что подобный формат мероприятий позволяет объективно оценить уровень подготовки студентов в разных регионах и определить наиболее талантливых ребят. И что не менее важно — это повышает интерес учащихся к предметной области за счет элемента состязательности. ●

СПРАВКА

В прошлом году на Национальном киберполигоне было проведено 78 киберучений, в том числе 16 мероприятий прошло на базе вузов. В этом году запланировано еще порядка 70 мероприятий, восемь из них уже состоялись. Среди участников мероприятий Национального киберполигона — представители государственных органов власти, специалисты по кибербезопасности, преподаватели образовательных учреждений и студенты.

Светофор под прикрытием

А1

— Однако высокая степень безопасности обеспечивается не только выбором конкретных решений, но и правильной организацией процесса. В соответствии с 187-ФЗ он должен включать, например, регулярную актуализацию моделей угроз и нарушителя и проведение учений в сфере кибербезопасности», — пояснил Александр Рожков.

Современные АСУ транспортных комплексов должны быть оборудованы межсетевыми экранами с функциями анализа трафика, также необходимо стойкое шифрование при использовании общедоступных сетей, рассказывает технический директор хостинг-провайдера Tendence.ru Александр Щукин. Для вычислительных мощностей должны применяться кластерные технологии в целях минимизации времени простоя в случае отказа.

«К сожалению, 100-процентную неуязвимость нельзя гарантировать ни одной неизолированной информационной системе, но можно приблизиться к идеалу. Для этого необходимо постоянно совершенствовать системы защиты, отслеживать найденные уязвимости в используемом программном обеспечении и своевременно обновлять его», — добавляет эксперт.

Впрочем, неприятности могут поджидать системы управления транспортом не только из-за стороннего вмешательства в их «мозги», но и из-за банального отключения света или интернета. Конечно, остановившийся на линии трамвай — это не трагедия, но вот пассажирам погруженной во тьму подземки или застрявшего в шахте небоскреба лифта будет уже явно некомфортно. Проблемы возникнут и у беспилотных ТС, которые рано или поздно заполонят дороги общего пользования. Кибератаки на беспилотники проводятся через их сенсоры и информационные системы, рассказал «РГ» ведущий научный сотрудник лаборатории навигационных систем НИУ МЭИ Илья Корогодин. Злоумышленник может подменять сигналы радара, навигационных спутников и дорожной инфраструктуры. Он может ослеплять камеры и искажать данные геосервисов. Компоненты комплекса защищаются шифрованием и дублированием. Но главная защита, уверен эксперт, — это избыточность данных, поскольку согласованно и одновременно исказить все потоки информации очень трудно.

Александр Рожков считает, что первыми шагами для поддержания бесперебойного функционирования транспортной инфраструктуры должно стать обеспечение кибербезопасности объектов ИТС, прежде всего узлов связи и энергообеспечения, с использованием ГЛОНАСС и современных информационно-коммуникационных технологий (межсетевой экран для контроля и фильтрации сетевого трафика, IPS — система предотвращения вторжений), а также переход к полной функциональной и технологической независимости от западных технологий, электронных навигационных карт и средств навигации (GPS) на всех видах транспорта.

> АКЦЕНТ
> ЗЛОУМЫШЛЕННИК МОЖЕТ ПОДМЕНЯТЬ СИГНАЛЫ РАДАРА, НАВИГАЦИОННЫХ СПУТНИКОВ, ОСЛЕПЛЯТЬ КАМЕРЫ

«Серебряной пули» против форс-мажоров не существует, но можно разумно дублировать наиболее критические узлы АСУ, говорит Александр Щукин. Везде, где возможно, стоит использовать источники бесперебойного питания, что позволит продолжить работу в случае кратковременного отключения электроэнергии. Каналы связи следует дублировать через разных операторов.

Группа компаний «Урбантех» провела исследования для выявления основных барьеров при внедрении ИТС в регионах. Основным препятствием оказалась нехватка специалистов, способных выявлять и решать проблемы с транспортным планированием, эксплуатацией ИТС и инфраструктурой транспортного комплекса.

«Максимальной эффективности от ИТС нельзя добиться только за счет установки оборудования и внедрения ПО. Нужно ежедневно и грамотно управлять системой. Важно не только поставить и единожды настроить светофор, но и проводить регулярные работы по адаптации режимов его работы к меняющейся ситуации, — говорит коммерческий директор «Урбантех» Даниил Хазов. — Именно поэтому мы исповедуем подход организации дорожного движения как комплексного сервиса, который в том числе включает ежедневную работу по управлению всей инфраструктурой. В качестве KPI ставится не только исправная работа системы, но и конкретные социальные показатели: снижение уровня пробок, аварийности на дорогах, увеличение пропускной способности улично-дорожной сети и соблюдение расписания общественного транспорта». ●

В тему

Мишенью злоумышленников может стать и личный транспорт, поскольку в большинстве своем современные тачки напичканы электроникой. Впрочем, в нашей стране уже дано добро на выпуск авто без АБС и системы курсовой устойчивости, в дальнейшем, может, и другие прибамбасы отменят и вообще не о чем будет переживать? «Наоборот! — парирует управляющий партнер MONTRANS Станислав Емельянов. — Цифровизация будет только расти. Автомобильная промышленность сегодня является одной из ключевых сфер мировой экономики. Ежегодно ассигнования на научные разработки и инновации превышают в отрасли сотни миллиардов долларов. Плюс еженедельные изменения и поправки правительства, касающиеся охраны окружающей среды, требуют от современного авто основываться на новейших разработках, отвечающих всем требованиям научно-технического прогресса. Стремительное развитие цифровых технологий во всех сферах жизни человека будет и дальше стимулировать производителей на создание высокоинтеллектуальных машин».

Отбить атаку

А1

Переход на отечественные операционные системы — один из шагов , способных повысить уровень кибербезопасности, соглашается доцент кафедры информационной безопасности киберфизических систем МИЭМ НИУ ВШЭ Антон Сергеев. Ведь сейчас нет гарантий, что при обновлении зарубежной ОС не появится какая-нибудь уязвимость. У других программных продуктов такие прецеденты были — есть целый список зарубежного ПО, в которое встраивались закладки. За операционными системами подобного пока не замечалось, но это не означает, что такого не будет никогда, предупреждает эксперт.

В этом смысле очень своевременно было решено не использовать зарубежное ПО на объектах критической информационной инфраструктуры (КИИ). Согласно мартовскому указу президента России, принадлежащие госорганам значимые объекты КИИ должны перейти на российское ПО до 1 января 2025 года. А с 31 марта этого года запрещается импорт зарубежного ПО для таких объектов. Это усилит их защиту от хакеров, считают эксперты.

«Основная цель кибератак — это прежде всего повреждение критической информационной инфраструктуры. Ведь ее выход из строя затормаживает нормальное функционирование общества и государства, — отмечает руководитель комитета по информационной безопасности АРПП «Отечественный софт», директор по стратегии и развитию BellSoft Роман Карпов. — Я уверен, что с переходом КИИ на отечественное ПО глобальных проблем не будет. А вот с тем, что не является КИИ, будут проблемы, потому что пока информационная система не ломается, организации не уделяют внимания повышению уровня информационной защиты».

Помимо замены общего программного обеспечения, требуются и специальные программы для защиты информации. С этим у России проблем нет. В нашей стране достаточно собственного софта, способного заменить зарубежные решения, заявляют в минцифры, приводя в пример реестр российского ПО, содержащий более 13 тысяч продуктов.

«На фоне многочисленных кибератак у нас выросла собственная отрасль информационной безопасности. Почти в каждом классе систем противодействия атакам есть национальные разработки, которые соответствуют мировому уровню, а и иногда даже его превосходят, — отмечает Антон Сергеев. — У нас есть свои антивирусы, межсетевые экраны, системы защищенных коммуникаций. Есть системы по выпуску ключей и сертификатов, системы сканирования, противодействия DDoS-атакам».

> Почти в каждом классе систем противодействия атакам есть отечественные разработки, которые соответствуют мировому уровню

В результате, несмотря на то что Россия, по статистике, одна из самых атакуемых стран в мире, по оценке ООН, она входит в топ-5 самых киберзащищенных государств, подчеркнул эксперт.

Помочь российским компаниям в поиске надежных программ может созданный Ассоциацией разработчиков программных продуктов (АРПП) «Отечественный софт» каталог с перечнем зарубежных программных продуктов и отечественных решений, готовых их замещать. «После модернизации каталога в нем появится и информация о том, является ли продукт средством защиты информации (СЗИ), что поможет компаниям подобрать альтернативы. Уверен, количество и качество разработки отечественных программных продуктов повысится», — заверил «РГ» Роман Карпов.

Чтобы поддержать процесс перехода с зарубежного ПО на отечественное, Минцифры России решило запустить маркетплейс российского программного обеспечения и в апреле стало принимать заявки от правообладателей на размещение там продуктов. «Маркетплейс должен стать удобной площадкой для взаимодействия правообладателей и заказчиков российского программного обеспечения. Страница продукта будет содержать данные о его функционале, стоимости, сферах применения и совместимости с операционными системами, а также информацию о том, какое зарубежное решение он может заменить», — пояснили в министерстве.

«Главное в этой задаче — создать естественные рыночные инструменты для получения информации. Чем быстрее заказчик понимает, что ему нужно, когда и за сколько, тем проще сделать нужную закупку, чтобы получить ожидаемый результат, — считает Арсений Щельцин. — Думаю, что в ситуации кризиса государство должно давать понятные ориентиры развития рынка для его участников. Чтобы все понимали, куда мы идем, что поддерживается, что нет. Второе, нужно давать инфраструктурные решения, то есть государству стоит создавать те инструменты, которые не может сделать частный бизнес. В этом плане работа уже ведется».

Между тем усиление кибербезопасности ожидается и для государственных информационных систем (ГИС). Как пояснили в Минцифры России, в рамках федерального проекта «Информационная безопасность» предусмотрены мероприятия, направленные в том числе на повышение защищенности этих систем. Например, планируется провести эксперимент по повышению уровня защищенности ГИС федеральных органов исполнительной власти и подведомственных учреждений.

Одновременно предполагается укрепить защиту персональных данных российских граждан. В Госдуму внесен законопроект, обязывающий операторов в случае утечки персональных данных сообщать об инцидентах в уполномоченные органы. Также Минцифры России прорабатывает вопросы борьбы с фишинговыми сайтами и телефонным мошенничеством. В частности, министерство разрабатывает систему, у которой будет широкий набор функций: от поиска фишинговых сайтов до подсистемы личных кабинетов по обмену данными о подобных ресурсах.

С первого взгляда порой сложно понять, что сайт — фишинговый, то есть сделан мошенниками с целью украсть чьи-то данные — логин, пароль к мобильному банку и т.д., отмечает Арсений Щельцин. По его словам, необходимо также обучать самих граждан, чтобы они не доверяли слепо всему поступающему к ним контенту. «Самая проблемная часть в России с персональными данными — это человеческий фактор. В основном эти данные сливаются, потому что у какого-то администратора был к ним доступ, и он сделал с персональной информацией что-то нехорошее. И здесь уязвимыми оказываются все категории граждан, не только пенсионеры и дети», — предупреждает эксперт. ●

Цифра

13 тысяч

программных продуктов содержится в реестре российского ПО

ТРЕНД / Рынку кибербезопасности прогнозируют небывалый взлет

Приоритет — сохранить информацию

Михаил Калмацкий

В 2022 году российский рынок информационной безопасности оказался в необычной ситуации. С одной стороны, резко возросло число цифровых атак, а значит, и потребность в защитных программных продуктах. С другой, зарубежные производители ПО решили свернуть свою деятельность в нашей стране. Все это, вкупе с дополнительной поддержкой от государства, открывает новые возможности для отечественных разработчиков систем кибербезопасности.

Всем нужна защита

Российский рынок информационной безопасности растет ежегодно на 15–20 процентов. На конец 2020 года его совокупный объем, по оценке аналитиков, превысил 140 миллиардов рублей.

Исследование PwC, проведенное в конце прошлого года, показало, что 65 процентов российских компаний ожидали роста расходов на кибербезопасность и в 2022-м. Однако реальность может превзойти самые смелые ожидания, ведь с конца февраля на госструктуры, компании, организации обрушилась беспрецедентная по масштабам волна кибератак.

«В прошлом году темпы прироста российского рынка кибербезопасности оценивали в 25 процентов. В условиях резко увеличившегося спроса он может вырасти на 50–100 процентов, — прогнозирует аналитик ФГ «Финам» Леонид Делицын. — Стало ясно, что ИТ-безопасность в сегодняшних условиях является одним из ключевых элементов национальной безопасности. Это обеспечивает спрос на услуги компаний отрасли со стороны государства».

По словам эксперта, в продуктах для информационной безопасности сейчас особенно нуждаются оборонный, энергетический, сырьевой и финансовый секторы. Там фактически идет оборона от кибернаступательных действий. В случае же связи и электронной коммерции информационная безопасность уже является внутренней, неотъемлемой частью этого бизнеса. К этому же идут и банки, отмечает Леонид Делицын.

«С конца февраля российские организации подверглись беспрецедентной по масштабам волне кибератак. Хакеры атакуют буквально все: ВПК и ТЭК, госучреждения и банки, СМИ и ИТ-сферу. В этих новых реалиях резко возрос запрос на сервисы и продукты нашей компании, разрабатывающей решения в области информационной безопасности, — рассказал «РГ» директор по продажам и развитию бизнеса Positive Technologies Максим Филиппов. — Число запросов от клиентов на наши сервисы всего за три недели сравнимо с третью заказов за весь прошлый год. Схожая картина и в количестве запросов на оперативную поставку наших продуктов — межсетевого экрана уровня приложений (PT Application Firewall), PT Network Attack Discovery — системы анализа трафика, MaxPatrol SIEM — системы выявления инцидентов в режиме реального времени, песочницы (PT Sandbox)».

«В марте мы отметили всплеск спроса на ИБ-решения в классах Web Application Firewall (WAF), Anti-DDoS, межсетевых экранов нового поколения NGFW/UTM, DLP-защиты, SIEM-систем, — рассказал «РГ» генеральный директор Axoft Global Вячеслав Бархатов. — А вот в апреле основной запрос был на инфраструктурные направления — системы виртуализации, ОС, офисные пакеты и коммуникационное ПО».

По словам гендиректора, изменения сегодня наблюдаются не только на рынке ИБ, но и в ИТ-ландшафте в целом. Спрос на отечественные решения существенно вырос, поэтому с одной стороны, для многих разработчиков появилось «окно возможностей», с другой — значительно выросла нагрузка на команды, что влияет на скорость обработки запросов.

«Стоит отметить, что российский ИБ-сегмент достаточно зрелый, в нем работает много серьезных игроков с большой историей, опытом, ресурсами и сильными решениями, — отмечает Вячеслав Бархатов. — На данный момент мы наблюдаем, как многие вендоры оперативно расширяют штат, вкладывают дополнительные средства в разработку инструментов или доработку функционала. А также готовы поддерживать на безвозмездной основе компании, которые попали под атаку, или предоставляют ПО, когда иностранный софт больше не работает, при наличии собственного железа».

ПРЕСС-СЛУЖБА POSITIVE TECHNOLOGIES

Минцифры планирует финансово поддержать разработку отечественных решений в сфере ИБ.

По словам Максима Филиппова, происходит практически полный исход иностранных вендоров из российского сегмента ИБ, а объем высвобождающегося рынка стремится к 80 миллиардам рублей. На этом фоне рынок кардинально перестраивается: от всех клиентов поступает запрос на реальный результат и защиту от недопустимых событий. При этом информационная безопасность стала приоритетом первых лиц компаний.

Гудбай, Америка

Уход целого ряда зарубежных разработчиков ПО действительно стал одним из главных событий для российского рынка кибербезопасности в этом году. Вендоры из других стран предоставляли софт, программно-аппаратные комплексы, а также услуги по проектированию, внедрению и т.д. К примеру, на рынке было более 100 продуктов в области информационной безопасности американского производства.

В списке иностранных разработчиков ПО, остановивших продажи и поддержку своих продуктов, несколько десятков компаний, включая Microsoft, Oracle, Cisco, Avast, Symantec и др. Как только зарубежные вендоры стали заявлять о своем уходе, в Минцифре России предложили срочно обсудить условия поэтапной передачи российским ИТ-компаниям технической поддержки компонентов информационных систем и объектов инфраструктуры, нарушения в работе которых могут привести к серьезным сбоям в системах жизнеобеспечения. При этом министерство выразило готовность оказать необходимую помощь в налаживании такого взаимодействия.

АКЦЕНТ

УХОД ИНОСТРАННЫХ ВЕНДОРОВ ПРИДАЛ ДОПОЛНИТЕЛЬНЫЙ ИМПУЛЬС РОССИЙСКИМ КОМПАНИЯМ

«От западного программного обеспечения сейчас освобождается весь корпоративный рынок, — отмечает Леонид Делицын. — При этом российские решения есть везде. Но поскольку глобальный рынок на порядок больше, значительно старше и компаний там в десятки раз больше, там активно продвигались такие комплексные решения, на которые наши корпорации пока не предъявляли спрос».

«Уход зарубежных вендоров создает предпосылки, чтобы российские компании увеличивали свои доли на рынке и свои показатели, — отмечает инвестиционный стратег УК «Арикапитал» Сергей Суверов. — К примеру, компания Positive Technologies по результатам первого квартала нарастила продажи примерно в три раза. Помимо общего роста востребованности средств защиты это произошло в том числе за счет освобождения ниши западных конкурентов, а также за счет ожидаемого роста самого рынка».

По словам Вячеслава Бархатова, для крупных российских игроков мало что изменилось. Такие компании, как Positive Technologies или «Лаборатория Касперского» давно успешно работают в направлении импортозамещения. Совсем другая ситуация у нишевых поставщиков. К примеру, если раньше они работали с госсектором, то теперь на них обращают внимание и коммерческие компании, поэтому приходится серьезно наращивать производственные мощности и человеческие ресурсы.

«Рынок ИБ в России достаточно развит, есть вполне зрелые продукты по ключевым классам — защита конечных точек, антивирусы, защита веб-приложений, защита от DDoS-атак, — отмечает эксперт. — Некоторое ПО иностранных вендоров нужно замещать не одним конкретным российским решением, а несколькими. Это также повод пересмотреть набор необходимого функционала, ведь многие покупали западный софт с огромным набором функционала, но использовали всего лишь его треть. Конечно, есть классы, для которых пока нет аналогов на российском рынке, например, защита контейнеров и облачных сред. Но это может быть хорошей возможностью для компаний, которые планируют расширить свои линейки».

При этом отечественные разработчики смогут рассчитывать и на помощь государства. Минцифры России предложило распространить меры господдержки на ИБ-специалистов и добавить ОКВЭД 74.90.9 (деятельность в области защиты информации) в перечень видов деятельности, на которые будут распространяться льготы. Это позволит ИБ-компаниям и их сотрудникам пользоваться всеми мерами поддержки, ранее представленными Минцифры РФ.

Критически важные объекты

Государство принимает активные меры для повышения уровня кибербезопасности и ускоренного перехода госструктур и частного бизнеса на отечественные программные продукты. Президент России Владимир Путин 1 мая подписал Указ «О дополнительных мерах по обеспечению информационной безопасности РФ». Согласно этому документу, главам регионов, ведомств, стратегических предприятий поручено создать структурное подразделение для обеспечения информационной безопасности, в том числе для обнаружения, предупреждения и ликвидации последствий компьютерных атак. Ранее другим указом президента госзаказчикам запретили закупать без согласования иностранное ПО (в том числе в составе программно-аппаратных комплексов) для использования на объектах критической информационной инфраструктуры (КИИ). А с 1 января 2025 года на этих объектах вообще нельзя будет использовать иностранный софт.

По действующему законодательству к объектам критической информационной инфраструктуры в России относятся информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, ТЭК, оборонной, ракетно-космической, металлургической промышленности, банковском секторе и др.

По данным Федеральной службы по техническому и экспортному контролю (ФСТЭК), в России насчитывается около 50 тысяч объектов КИИ, из которых около 10 тысяч отнесены к особо значимым. При этом в 55 процентах систем и сетей не применяются требуемые средства защиты от компьютерных атак.

Между тем российские объекты КИИ всегда были зоной повышенного внимания хакеров. Так, по словам генерального директора «Ростелеком-Солар» Игоря Ляпунова, абсолютное большинство (92 процента) попыток профессиональных кибератак, проведенных в России в 2021 году, было направлено именно на объекты КИИ. Чаще всего внимание хакеров с высокой квалификацией привлекали госорганизации, предприятия энергетики, промышленности и военно-промышленного комплекса.

Результативная кибербезопасность

В условиях участившихся кибератак особенную значимость получают принципы результативной информационной безопасности, которые предусматривают выстраивание защиты таким образом, чтобы недопустимые для каждого бизнеса, отрасли (или даже государства) события были невозможными. И некоторые российские разработчики предлагают технологии, которые позволят достичь этого результата с минимумом экспертизы и усилий со стороны специалистов на стороне компании. К примеру, один из метапродуктов Positive Technologies — MaxPatrol O2 — позволяет автоматически обнаружить и остановить хакера до того, как будет нанесен неприемлемый для компании ущерб, и сделать это можно в прямом смысле слова силами одного человека.

«На фоне сложной геополитической обстановки мы прогнозируем увеличение количества атак, поэтому рекомендуем компаниям перейти от типовых процессов ИБ к принципам результативной безопасности, — говорит аналитик исследовательской группы Positive Technologies Яна Юракова. — Мы настоятельно рекомендуем компаниям сконцентрироваться на защите ключевых и целевых активов и точек проникновения во внутреннюю сеть. Также следует обратить внимание на организацию процесса управления уязвимостями в компании».

Важную роль в концепции результативной безопасности играют практические киберучения, которые позволяют проверить эффективность системы защиты. Ведь реальный результат можно оценить только путем моделирования действий злоумышленников на киберучениях.

Крупнейшие открытые киберучения — The Standoff — проходят сегодня и завтра, 18 и 19 мая, на площадке ежегодного Международного форума по практической кибербезопасности Positive Hack Days. PHDays традиционно собирает всех, кто так или иначе связан с информационной безопасностью: от представителей отрасли, экспертов и лидеров мнений до молодых ученых и журналистов. Среди посещавших ранее форум хедлайнеров — легендарный криптограф Брюс Шнайер, один из разработчиков USB-эмулятора FaceDancer Трэвис Гудспид, соавтор концепции криптографии с открытым ключом Уитфилд Диффи.

В этот раз для проведения The Standoff создан макет небольшого государства, включающий в себя ключевые отрасли и свойственные им бизнес-процессы. Парализовать жизнь этого государства, найдя слабые места в защите виртуальных компаний из разных отраслей экономики, пробуют 157 «белых хакеров». А пять команд защитников отслеживают перемещения атакующих внутри инфраструктуры, изучают техники и тактики злоумышленников, чтобы в дальнейшем эффективно предотвращать подобные события в реальном мире.

The Standoff проводится не впервые, и, к примеру, в мае прошлого года атакующим на киберполигоне удалось реализовать 33 недопустимых события — больше половины запланированных. Они смогли сократить добычу нефти на 90 процентов, уронить контейнер в порту и полностью обесточить все предприятия, воссозданные в рамках киберполигона. В этот раз атакующие попробуют реализовать 100 недопустимых событий. На киберполигоне представлены три основные отрасли: энергетика, нефтяная промышленность и черная металлургия, а также сервисные сектора: ЖКХ, банковская и транспортная системы. Организаторы хотят показать взаимозависимость отраслей экономики, когда даже незначительное влияние на одну из систем может иметь непредсказуемые последствия для другой, казалось бы не связанной с первой.

«Этот эффект бабочки каждый сможет наблюдать в реальном времени, что и делает киберучения The Standoff актуальными как никогда. Знать, нарушение работы каких систем и объектов может привести к недопустимым последствиям, — одна из главных целей киберучений», — говорит руководитель продукта The Standoff Ярослав Бабин.

Кстати, недавно Минцифры России решило поддержать «белых хакеров» и предложило профессиональному сообществу обсудить новую инициативу прямой финансовой поддержки проведения пентестов (анализ системы на наличие уязвимостей) и Bug Bounty. В рамках оперативного штаба по обеспечению информационной безопасности крупным компаниям предлагается протестировать технологию и механику внедрения данных инициатив. А министерство готово софинансировать пилотные проекты. По мнению экспертов в области информационной безопасности, развитие программ Bug Bounty, в рамках которых «белые хакеры» смогут искать критические уязвимости в российском ПО и зарабатывать на этом, играет для практического развития идей результативной безопасности ничуть не меньшую роль, чем те же киберучения.

В целом российский рынок кибербезопасности ждет активное развитие и появление новых программных продуктов. Уход иностранных вендоров придал дополнительный импульс российским компаниям, отмечают эксперты. Разработкой технологий занимаются уже не только вендоры, но и интеграторы, у которых есть собственные лаборатории и центры разработки. Сложившаяся ситуация стимулирует всех игроков на рынке создавать собственные решения. ●

ДЕНЬГИ / У российских ИТ-компаний резко улучшились финансовые показатели

Притяжение инвесторов

Сергей Григорьев

Кибербезопасность стала необходимым условием ведения бизнеса. Рынок средств информационной защиты растет, а вместе с ним и финансовые показатели работающих в этом секторе компаний. Так в первом квартале 2022 года объем продаж компании Positive Technologies вырос в три раза — до 1,2 миллиарда рублей — по сравнению с аналогичным периодом прошлого года. Выручка прибавила 49 процентов год к году и составила 1,4 миллиарда рублей. Показатель EBITDA увеличился на 75 процентов и достиг 262 миллионов рублей, а чистая прибыль — 146 миллионов, по сравнению с убытком в 10 млн рублей годом ранее.

Напомним, по итогам 2021 года выручка Positive Technologies увеличилась на 28 процентов и достигла 7,1 миллиарда рублей. Скорректированный показатель EBITDA компании составил 2,9 миллиарда рублей, прибавив 35 процентов по сравнению с предыдущим годом. Рентабельность по скорректированной EBITDA достигла 41 процента — один из лучших показателей для этой отрасли. Что касается чистой прибыли, то в 2021 году она составила 1,9 миллиарда рублей — рост на 27 процентов.

В конце 2021 года Positive Technologies первой из российских компаний в сфере кибербезопасности разместила свои акции на Московской бирже. «Этот шаг стал точкой сборки для нашей общей стратегии нескольких последних лет, — отметил генеральный директор Positive Technologies Денис Баранов. — К этому моменту мы свели воедино все цели компании с точки зрения разрабатываемых технологий (мы сформировали наиболее полную на нашем рынке продуктовую линейку, отвечающую потребностям результативной кибербезопасности), развития бизнеса (успешно реализовали стратегические цели по увеличению продаж с 2019-го по 2021 год в объеме 4–6–8 млрд руб.) и публичности — нашими инвесторами стал широкий круг частных инвесторов».

По словам гендиректора, опыт последних месяцев показал, что ставка компании на частного инвестора и внутренний рынок была единственно верным решением. Это позволило полностью исключить зависимость от иностранного капитала и существенно повысить надежность акций для инвестирования. «Сегодня общее число наших инвесторов превышает 44 тысячи. Мы прилагаем много усилий к тому, чтобы сделать бизнес в сфере отечественной кибербезопасности максимально прозрачным и более понятным для широкого круга инвесторов, поэтому применяем лучшие мировые практики раскрытия финансовой отчетности — в частности, публикуем финансовую отчетность по стандартам МСФО», — подчеркнул Денис Баранов.

АКЦЕНТ

СТАВКА НА ВНУТРЕННИЙ РЫНОК ПОВЫШАЕТ НЕЗАВИСИМОСТЬ ОТ ИНОСТРАННОГО КАПИТАЛА И НАДЕЖНОСТЬ АКЦИЙ

Число частных акционеров компании быстро растет — в декабре их было 1391, а к середине апреля — более 44 тысяч человек. После возобновления торгов на Московской бирже в конце марта акции Positive Technologies оказались в списке топ-3 по темпам роста. За неделю их цена увеличилась в 2,3 раза. В начале апреля капитализация Positive Technologies превысила один миллиард долларов.

«Сейчас возможности покупки иностранных бумаг на бирже сильно ограничены. А так как рынку нужны быстрорастущие истории, то перспективы у акций Positive Technologies — единственной компании, которая представлена на бирже из этого сегмента, достаточно неплохие. Несмотря на то, что эта бумага является вторым эшелоном, обороты по ней в отдельные дни такие же, как по голубым фишкам, — отмечает инвестиционный стратег УК «Арикапитал» Сергей Суверов. — Компании в других отраслях сокращают бизнес, а Positive Technologies, наоборот, быстро растет, даже в условиях ожидаемой рецессии. К тому же эта компания уже 20 лет на рынке и ее продукты используют крупнейшие корпорации России, а значит, качество предлагаемых решений достаточно хорошее». ●

ПРОБЛЕМА / Количество «нападений» на компьютеры растет

Вредоносы не дают покоя

Михаил Курбатов

Количество кибератак в 2021 году увеличилось на 6,5 процента по сравнению с 2020 годом. Такие данные приводятся в исследовании компании Positive Technologies. Доля целевых атак в сравнении с 2020 годом выросла на 4 процентных пункта и составила 74 процента от общего количества. Среди вредоносного ПО доминируют шифровальщики. Также в 2021 году злоумышленники стали чаще атаковать системы хранения данных, пользоваться опасными уязвимостями и продолжают беспокоить частных лиц. Эти тренды будут актуальны и в 2022 году, говорится в исследовании.

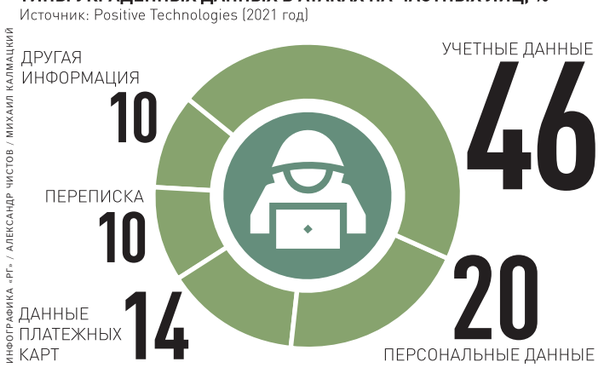
В 2021 году 86 процентов всех кибератак было направлено на организации. В тройку самых популярных у хакеров вошли госучреждения (16 процентов от всех атак), медучреждения (11 процентов) и промышленные компании (10 процентов). Далее следуют научные и образовательные организации (9 процентов) и ИТ-компании (7 процентов).

Самым популярным методом атак в 2021 году стало применение вредоносного программного обеспечения — 63 процента. На втором месте идет использование методов социальной инженерии (50 процентов) и хакинг — эксплуатация недостатков защиты и уязвимостей в ПО (32 процента). Среди вредоносного ПО, которое использовалось в атаках на компании, чаще всего встречались шифровальщики: по данным Positive Technologies, они были задействованы в 60 процентах случаев — на 15 п. п. больше, чем в 2020 году. На втором месте — вредоносное ПО для удаленного управления, использовавшееся в 27 процентах атак на организации. Третье место заняли загрузчики (16 процентов). Количество атак с использованием ВПО с 2018 года выросло на 137 процентов, и на текущий момент не видно оснований для снижения их числа в 2022 году, считают в Positive Technologies.

Также в прошлом году изменилась тактика вымогательства. В 2020-м киберпреступники, распространяющие программы-вымогатели, угрожали отказывающимся платить выкуп жертвам передать информацию об атаке их клиентам. В 2021-м злоумышленники пошли дальше и стали угрожать публикацией украденных у компаний данных, если жертва обратится за помощью в полицию или наймет переговорщика.

Что касается частных лиц, доля атак на них составляет 14 процентов от всех кибератак, зафиксированных за прошлый год. В 88 процентах атак на частных лиц киберпреступники использовали методы социальной инженерии. Популярными темами фишинга в 2021 году были пандемия COVID-19, премьеры фильмов и сериалов, инвестиции, корпоративные рассылки. ●

ТИПЫ УКРАДЕННЫХ ДАННЫХ В АТАКАХ НА ЧАСТНЫХ ЛИЦ, %
Источник: Positive Technologies (2021 год)



ИНФОГРАФИКА «РТ» / АЛЕКСАНДР ЧИСТОВ / МИХАИЛ КАЛМАЦКИЙ

ТИПЫ УКРАДЕННЫХ ДАННЫХ В АТАКАХ НА ОРГАНИЗАЦИИ, %
Источник: Positive Technologies (2021 год)

ИНФОГРАФИКА «РТ» / АЛЕКСАНДР ЧИСТОВ / МИХАИЛ КАЛМАЦКИЙ

Воздушная оборона

А1 Еще распространены попытки взлома аккаунтов пользователей облачных сервисов методом подбора паролей. Как правило, злоумышленники используют его, если получили в распоряжение логин пользователя, например, из-за утечки данных в интернете.

Затем начинается «угадывание» пароля с использованием любых возможных вариантов. Такие попытки редко становятся успешными, однако учетные записи блокируются, пользователи испытывают трудности с доступом к ним.

По мнению Александра Щукина, технического директора хостинг-провайдера Tendence.ru, распределенные атаки, вызывающие отказ обслуживания (DDoS), сейчас могут иметь мощность до нескольких терабит в секунду и способны хотя бы на время вывести из строя любой дата-центр. Высокая концентрация ресурсов в Центрах обработки данных (ЦОД) может привести к эффекту домино, когда атакуют соседа, а страдают и другие клиенты, не имеющие отношения к цели атаки. Поэтому лучше дублировать свои сервисы у нескольких поставщиков.

Другой угрозой, с которой сталкиваются пользователи, является вероятность спора хозяйствующих субъектов, которым принадлежит дата-центр. Например, в феврале-марте 2020 года продолжительное время пользователи одного из старейших российских хостинг-провайдеров сутками не имели доступа к своим ресурсам именно по этой причине. Работа сервиса восстановилась лишь несколько недель спустя, многие клиенты получили убытки.

> DDoS-атаки, вызывающие отказ обслуживания, могут иметь мощность до нескольких терабит в секунду

«Основными угрозами безопасности облаков стабильно остаются неправильная конфигурация, излишние или неверно настроенные права доступа к ресурсам и данным, использование небезопасных интерфейсов (API) и протоколов. Но если посмотреть на угрозы информационной безопасности традиционных инфраструктур, то они будут практически теми же», — резюмирует Денис Полянский, директор по клиентской безопасности Selectel.

Технологии злоумышленников не стоят на месте, поэтому информационная безопасность превратилась из проекта в непрерывно эволюционирующий процесс. «В ближайшие три-пять лет все больше традиционных сервисов перейдут на облачную схему. Эту тенденцию мы наблюдаем уже более трех лет. Развитие технологий безопасности, включая защиту облачных технологий и сред, идет в ногу с развитием методов злоумышленников, а местами даже опережают», — говорит Кирилл Солодовников.

По оценке Accenture, мировой рынок услуг в сфере кибербезопасности будет расти на 13 процентов в год и к 2025 году достигнет 94 миллиардов долларов. Эксперты прогнозируют, что вырастет востребованность услуг по развитию ИБ-компетенций, включая проведение киберучений и киберполигоны.

Согласно рейтингу Top-50 Global Security, традиционными лидерами по информационной безопасности в мире остаются компании из Юго-Восточной Азии. «Россия отсутствует в этом рейтинге, и это может говорить о том, что рост цифровой трансформации у нас опережает развитие информационной безопасности. По итогам 2021 года рынок ИБ в России прибавил, по разным оценкам, до 10 процентов. Скорее всего, этот рост продолжится, но ожидать более высокой динамики не стоит», — резюмирует Артур Хасиятуллин. ●

ПРАКТИКА / Основным инструментом для цифрового мошенничества остается сотовый телефон

Защита нападением

Алексей Стригин

Количество киберпреступлений в финансовом секторе за последние месяцы, согласно данным Банка России, выросло в 22 раза, а ИТ-сектор отмечает стократный рост DDoS-атак. На этом фоне регулятор выступил с инициативой возвращать клиентам похищенные мошенниками со счетов средства в течение 30 дней. Сейчас идет разработка этого механизма. Возникает вопрос: а есть ли у пользователей реальные возможности избежать обмана? Например, в Visa уверены, что доля россиян, способных к самозащите, сегодня не превышает 0,2 процента.

Основным инструментом мошенников по-прежнему является телефон — на звонки с подменой номера приходится 80 процентов случаев обмана. Помимо телефона, преступникам активно помогают знания основ социальной инженерии и способность убедить жертву самостоятельно перевести средства злоумышленникам.

— Современные компании используют мощные средства защиты, взломать которые сложно, и самым уязвимым звеном в системе защиты становится сам человек — сотрудник компании или пользователь, — предупреждает Александр Тарасов, управляющий партнер DIS Group.

Приемы у мошенников простые — это информация об отключении российских банков от международной платежной системы, слухи о полной блокировке банковских операций и запрете на снятие наличных. Нередки предложения услуг по открытию карт в иностранных банках, быстрому снятию наличных, валютному обмену «по выгодному курсу», перечисляет Иван Шубин, руководитель дирекции информационной безопасности РГС Банка. Кроме того, согласно опросу компании «Лаборатория Касперского», четверть пользователей получала вредоносные электронные письма на темы, связанные с COVID-19. Относительно новыми приемами, появившимися в последние месяцы, стали предложения о компенсации или выплате материальной помощи, о вознаграждении за опрос, об оформлении карты «Мир», подарках и бонусах от компаний, добавляет финансовый эксперт Александр Патешман.

СПРАВКА

В 2021 году был совершен один миллион операций без согласия клиента на сумму 13,6 миллиарда рублей. Рост составил 38 процентов. При этом доля возвращенных средств составила всего семь процентов, говорится в отчете Банка России.

Здесь важно отметить: перечисление известных приемов мошенников не защитит от обмана — преступники изобретательны, и каждый день появляются новые способы манипуляции. Например, в ВТБ отмечают, что каждый седьмой способ теперь носит гибридный характер и использует все возможные средства воздействия на жертву.

Самый простой способ борьбы с назойливыми звонками с неизвестных номеров — отключиться и перезвонить в банк по официальному номеру, указанному на банковской карте или сайте кредитной организации, советует Анастасия Громакова, гендиректор компании «ЭгроТрейд». И, конечно, не стоит никому сообщать данные карты или код из SMS. Определить же номер оппонента можно с помощью специального мобильного приложения.

Аналогичное поведение рекомендуют эксперты и в отношении сообщений от незнакомых абонентов. В этом случае можно провести поиск по номеру телефона отправителя, возможно, на него уже есть жалобы в Сети.

Сложнее понять подвох при общении в соцсетях. По последним данным, активность мошенников там выросла в три раза, причем в основном она направлена на людей в возрасте 18—22 лет — более легкую «добычу», чем опытные пользователи. Расчет преступников прост — они делают ставку на самонадеянность молодых, уверенных в том, что их никто никогда не проведет.

— Главный совет — не верить ничему, что пишут в интернете, даже если сообщения приходят со знакомых аккаунтов. Они ведь могут быть взломаны, — предупреждает Павел Коростелев, руководитель отдела продвижения продуктов компании «Код Безопасности».

Другая распространенная угроза — фишинг, то есть получение конфиденциальных данных с помощью поддельных сайтов. Чтобы избежать этого, пользователи должны проверять доменное имя и вводить свои данные только на официальных сайтах. Помогают бороться с фишингом специальные сервисы и приложения — любые антивирусные программы или встроенные в браузер системы защиты (например, Protect от «Яндекса»), поясняет Сергей Гребенников, член комиссии ОП РФ по развитию информационного сообщества, СМИ и массовых коммуникаций.

АЛЕКСАНДР КОРОЛЬКОВ

Не стоит никому сообщать данные карты или код из SMS.

АКЦЕНТ

ЧЕТВЕРТЬ ПОЛЬЗОВАТЕЛЕЙ ПОЛУЧАЛА ВРЕДОНОСНЫЕ ЭЛЕКТРОННЫЕ ПИСЬМА НА ТЕМЫ, СВЯЗАННЫЕ С COVID-19

Отличить подделку иногда бывает очень сложно — нередко мошенники в контактах сайта указывают телефоны и адреса оригинальной компании, при этом оставляя название и ИНН компании мошенника, напоминает Татьяна Сустина, руководитель комиссии по правовому просвещению Федерального союза адвокатов России.

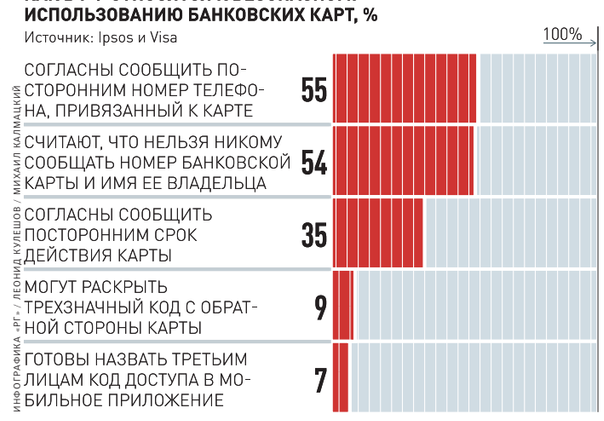
Есть еще несколько общих правил, исполнение которых является обязательным для каждого пользователя Сети. Так, онлайн-шопоголикам просто необходимо иметь отдельную карту для покупок с ограниченным объемом средств на ней. Использование незащищенных Wi-Fi сетей в публичных местах, использование неофициальных банковских приложений и простых паролей в сетях, пренебрежение антивирусами, хранение фотографий банковских карт на телефонах, а также использование неизвестных флешек на личном компьютере — все это легкие способы приобрести серьезные финансовые проблемы, уверен Григорий Ковшов, эксперт по информационной безопасности компании «Газинформсервис».

Важно вообще минимизировать личные данные, которые вы оставляете в Сети, напоминают эксперты. Ведь кибератака — вмешательство в информационную систему компании — всегда начинается со сбора данных о жертве. А чем физическое лицо в данном случае отличается от юридического? Только своей неподготовленностью. Поэтому главная рекомендация для тех, кто хочет сохранить свои средства, звучит очень просто.

— Совет для всех: постоянно учитесь. Финансовая грамотность — один из базовых навыков, необходимых в наше время. Пройдите обучающие курсы, почитайте специальную литературу или статьи в интернете. Тогда мошенникам будет гораздо сложнее вас обмануть, — резюмирует Александр Тарасов. ●

КАК В РФ ОТНОСЯТСЯ К БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ БАНКОВСКИХ КАРТ, %

Источник: Ipsos и Visa



ИНФОГРАФИКА «РГ» / ЛЕОНИД КУЛЕШОВ / МИХАИЛ КАЛМАЦКИЙ

РИСКИ / Киберстрахование позволяет снизить убытки компаний и частников

Возмещение ущерба

Андрей Крупнов,
директор по отраслевым решениям в страховании компании «КРОК»

Доля нематериальных активов у крупнейших компаний, входящих в индекс S&P500, в 2020 году составила 90 процентов, физических — лишь 10 процентов. Растет объем нематериальных активов и у домохозяйств. Речь идет о ценной информации, персональных данных, которые могут быть использованы для совершения юридически значимых действий, логинах и паролях от банковских и других аккаунтов. Соответственно и компаниям, и частным лицам приходиться думать о том, чтобы снизить риски утраты этих активов.

Общее количество кибератак в мире в первой половине 2021 года, согласно отчету компании Deloitte, выросло на 29 процентов по сравнению с тем же периодом 2020-го. В том числе на 93 процента выросло число атак вымогателей — хакеры пытались извлечь выгоду из вызванного пандемией массового перехода людей на удаленную работу.

Неудивительно, что на этом фоне одним из самых быстрорастущих сегментов страхового рынка стало киберстрахование. Оно покрывает как прямой экономический ущерб от инцидентов, произошедших со страхователями, так и их ответственность перед третьими лицами, наступившую в результате непреднамеренной утечки защищенных законом данных. Популярность новой услуги подтверждает статистика — совокупный мировой объем страховой премии по киберстрахованию в 2021 году достиг пяти миллиардов долларов.

Перечень актуальных киберрисков постоянно расширяется, а вслед за ним растет и количество вариантов страхового покрытия. Причем покупателями полисов киберстрахования становятся не только компании, работающие с персональными данными клиентов. Стремительно набирает популярность и розничное киберстрахование, в том числе благодаря удаленной работе, которая создала дополнительные риски и для компаний, и для их сотрудников, несущих ответственность за сохранность данных на своих компьютерах. Наконец, объектами атак кибермошенников чаще становятся именно частные лица, нежели компании, обладающие штатом специалистов по информационной безопасности и соответствующими протоколами.

Сегодня розничное киберстрахование включает в себя несколько видов страхового покрытия. Во-первых, это кража средств — покрываются убытки, возникшие в результате взлома банковского счета, кредитной или дебетовой карты, а также мобильного кошелька. Кроме того, можно получить компенсацию расходов на восстановление данных, поврежденных вредоносными программами, и покрыть финансовые потери от фишинговой атаки, включая расходы на судебное преследование преступников. Страхование кибервымогательства обеспечивает защиту от убытков, вызванных угрозами преступников, а страхование кражи личных данных покрывает расходы на защиту по искам пострадавших от мошенничества, связанного с кражей личных данных.

АКЦЕНТ

РОЗНИЧНОЕ КИБЕРСТРАХОВАНИЕ СТРЕМИТЕЛЬНО НАБИРАЕТ ПОПУЛЯРНОСТЬ

Средства массовой информации могут застраховаться и покрыть расходы на защиту по искам третьих лиц в связи с диффамацией или вторжением в частную жизнь в результате публикации или трансляции застрахованным лицом любого цифрового медиаконтента. То же касается и социальных сетей, к которым могут быть предъявлены претензии тех, кто пострадал от взлома аккаунта. В перечень киберрисков, для которых есть страхование, также входит несанкционированная онлайн-транзакция — здесь покрывается ущерб от мошеннического использования третьим лицом банковского счета, кредитной или дебетовой карты и электронного кошелька для совершения онлайн-покупок через интернет. А еще страхование предусматривает возможность атаки с помощью поддельной электронной почты и нарушение неприкосновенности частной жизни.

Каждый может примерить этот перечень рисков на себя и убедиться, что большинство из них вполне актуальны. Но у всех ли есть страховое покрытие на такие случаи? Если нет, стоит обратиться к страховщикам за киберполисом. Но прежде чем это сделать, следует запомнить несколько существенных моментов. Начнем с того, что киберугрозы все время изменяются, и любая оценка рисков, посчитанная на основании данных прошлых периодов, как это принято в традиционном страховании, совершенно ненадежна. Управление киберрисками реализуется на других принципах. Первый из них — упор на предотвращение или снижение уровня риска, а не на его оценку. Компании, занимающиеся киберстрахованием, работают в паре с ИТ-компаниями, предоставляющими услуги по кибераудиту и технологиям защиты от киберугроз. Такой ИТ-партнер обеспечивает определенный уровень безопасности, принимая на себя часть киберрисков и делая возможным более-менее корректную количественную оценку остаточного уровня риска, принимаемого на страхование.

Кроме того, киберинциденты могут быть остановлены, а наносимый ими ущерб минимизирован, даже если риск все-таки реализовался. Для этого существуют подразделения и технологические инструменты быстрого реагирования, позволяющие предотвратить худший для клиента сценарий.

Таким образом, киберстрахование работает не просто как покрытие на случай неблагоприятного события, а как комплексная услуга, включающая в себя набор мероприятий и инструментов по предупреждению киберинцидентов и снижению наносимого ими вреда. ●

ОТРАСЛЬ / Взломщики наступают на энергетический сектор

Под напряжением

Евгения Мамонова

Энергетическая отрасль имеет важнейшее значение для функционирования множества секторов экономики. Поэтому практически любой элемент энергетического комплекса — это стратегический объект. Это прекрасно понимают и злоумышленники, для которых данный сектор является одной из основных мишеней кибератак.

Стремительное развитие цифровизации не обошло и энергетический комплекс. Автоматизация различных процессов, возможность удаленного управления, несомненно, повышают качество и эффективность работы отрасли. С другой стороны, это дает возможность злоумышленникам заполучить контроль над важнейшими процессами. По данным исследования Kaspersky ICS CERT, во второй половине 2021 года на энергетическую отрасль пришлась почти треть (32,4 процента) от всех заблокированных кибератак на компьютеры автоматизированных систем управления (АСУ) в мире.

Одной из самых громких кибератак в энергетике в прошлом году стал взлом сайта Белорусской атомной электростанции. Хакерам удалось разместить фейковое объявление якобы от имени сотрудников АЭС. При этом технология, которая использовалась злоумышленниками, позволяла получить контроль над всем содержимым сайта, заменить имеющуюся там информацию или полностью удалить содержимое. Месяц спустя в США хакерская атака заблокировала работу крупнейшего оператора трубопроводов Colonial Pipeline. Из-за этого транспортировка по трубопроводам была остановлена на несколько дней. Результат — скачок цен на бензин и временный дефицит топлива на всем Юго-Востоке США.

> Во втором полугодии 2021 года на энергетическую отрасль пришлась почти треть от всех заблокированных кибератак на компьютеры АСУ в мире

Но самой масштабной кибератакой на объект энергетики, пожалуй, можно считать случай в Венесуэле, который произошел в 2019 году. Как сообщили власти страны, хакеры атаковали автоматическую систему контроля крупнейшей ГЭС «Эль-Гури». Правительство Венесуэлы решило временно остановить работу гидроэлектростанции, что привело к отключению электричества практически по всей стране. Почти сутки без света находился 21 штат из 23, в том числе социальные объекты: школы, больницы.

«Наиболее распространенными кибератаками являются, например, насыщение сетевого оборудования большим количеством внешних запросов или перехват управления системы в сети SCADA через украденные аккаунты, отправка команд на отключение систем бесперебойного питания, которые уже были реконфигурированы, — рассказывает доцент кафедры информатики РЭУ им. Г.В. Плеханова Александр Тимофеев. — После этого злоумышленники отключают систему безопасности, что приводит, например, к прерыванию подачи электроэнергии. Еще один способ, которым активно пользуются хакеры, — уничтожение информации на серверах и рабочих станциях, несанкционированное вмешательство в АСУ. С помощью удаленного доступа злоумышленник может перехватить управление устройством и вызвать сбои, например внести изменения в данные, передаваемые оператору, повредить оборудование или вызвать полный или частичный отказ устройства».

Несмотря на то что энергетический сектор является критически важной отраслью для любой страны и его безопасности уделяется должное внимание, он остается одним из самых уязвимых секторов для кибератак. Это связано с тем, что энергетическая отрасль довольно медленно обновляет инфраструктуру и программное обеспечение, что играет на руку хакерам. Устаревшее ПО — это идеальная мишень для DDoS-атак и эксплойтов (последовательность команд, использующих различные уязвимости в ПО для проведения атак).

> Российский энергетический сектор использует от 40 до 50 процентов иностранного ПО, а также иностранное оборудование — датчики, контроллеры, микроэлектронику

Помимо устаревшего ПО слабыми местами также можно назвать отсутствие безопасного удаленного доступа и регулярного контроля конфигураций, отсутствие разграничений прав доступа, контроля над запуском различных приложений из вне и многое другое. Все это делает энергетическую отрасль удобным объектом для нападений киберпреступников.

Сегодня из-за нестабильной геополитической ситуации российская энергетика становится более уязвимой для зарубежных хакеров. По разным оценкам, отечественный энергетический сектор использует от 40 до 50 процентов иностранного ПО, а также иностранное оборудование (датчики, контроллеры, микроэлектронику). Работая «на своем поле», зарубежным хакерам легче внедрить вирусные программы. «Сегодня в энергетической отрасли существует чрезмерная зависимость от импорта некоторых видов оборудования, технологий, программного обеспечения, усугубляющаяся монопольным положением их поставщиков», — отмечает Александр Тимофеев.

По словам экспертов, единственное решение для снижения риска хакерских атак извне, — это отказ от иностранного оборудования и ПО, а также развитие защиты. «Киберугрозы представляют серьезную опасность для энергетического сектора, поэтому компании, занимающиеся технической поддержкой, активно внедряют новые решения для противодействия этим угрозам, — говорит первый вице-президент «ОПОРЫ России» Павел Сигал. — Тренд на импортозамещение в ключевых отраслях активно развивается в последние годы, и многие госпредприятия и корпорации переходят на отечественные технологии. Это касается и инструментов защиты от кибератак». ●

Российская Газета

УЧРЕДИТЕЛЬ
ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ГАЗЕТА ИЗДАЕТСЯ С 11 НОЯБРЯ 1990 ГОДА

Главный редактор «Российской газеты»: В.А. Фронин
Адрес редакции и издателя: ул. Правды, 24, стр. 4, Москва 125993 ФГБУ «Редакция «Российской газеты»
Адрес в Интернете www.rg.ru
Телефон 8 499 257 5650,
Факс 8 499 2575892
Контакт-центр по вопросам подписки и доставки 8 800 100 1113 (звонок бесплатный по России)

Генеральный директор ФГБУ «Редакция «Российской газеты»: П.А. Негоица
Распространитель: ул. Правды, 24, стр. 4, Москва 127137 АО «Издательство «Российская газета»
Телефон 8 499 257 5362 Факс 8 499 257 5122
Подписные индексы:
на год — 10042, 17950, П5922
на полгода — 50202, 15588, 50201, 15589, П1107, П1261, П5921, П5919
Комплекты — 17991, 40913, 40942, 70458

Заказы на размещение рекламы в «РГ» и ее приложениях: телефон: 8 499 257 3752, 786 6787; факс: 8 499 257 5764, 8 499 257 5041, reklama@rg.ru

Справки по подписке и доставке: тел. 8 800 100 11 13 (звонок бесплатный); по розничным продажам 8 499 257 4023; Справки по вопросам экономики: тел. 8 499 257 5380, economic@rg.ru; политики: тел. 8 499 257 5970, politika@rg.ru; официальных публикаций: тел. 8 499 257 5396, oficial@rg.ru; международной жизни: тел. 8 499 257 5903, foreign@rg.ru; региональной сети: тел. 8 499 257 3603, chagina@rg.ru; телерадиопрограмм: тел. 8 499 257 5820, gpr@rg.ru; спорта: тел. 8 499 257 5045, sport@rg.ru; о публикациях: тел. 8 499 257 5256, biblioteka@rg.ru; общества: society@rg.ru; новостей: тел. 8 499 257 5348, hotnews@rg.ru; культуры: тел. 8 499 257 5113, culture@rg.ru

Отпечатано в типографии: АО «Прайм Принт Москва» 141707, Московская обл., г. Долгопрудный, Лихачевский проезд, д. 5В
Время подписания в печать: По графику: 18.00 Фактически: 18.00
Дата выхода в свет: 18.05.2022 г.
Приложение является составной частью «Российской газеты» и распространяется только в составе газеты
Свободная цена
ТИП. № 1274

Региональные филиалы ФГБУ «Редакция «Российской газеты» в городах:
Архангельск (8182) 20-78-37 arh@rg.ru; Барнаул (3852) 66-72-37 altai@rg.ru; Бишкек (10996312) 300-142 bishkek@rg.ru; Благовещенск (4162) 59-20-65 amur@rgfe.ru; Владивосток (4232) 22-34-89 prim@rgfe.ru; Волгоград (8442) 92-35-08 vlgr@rg.ru; Воронеж (473) 250-23-05 voronezh@rg.ru; Екатеринбург (343) 371-24-84 ural@rg.ru; Иркутск (3952) 28-83-82 irkutsk@rg.ru; Казань (843) 264-41-67 kazan@rg.ru; Калининград (4012) 53-10-10 zapad@rg.ru; Кемерово (3842) 35-40-59 kmr@rg.ru; Краснодар (861) 259-21-11 kuban@rg.ru; Красноярск (391) 274-60-49 rg@krasrg.ru; Мурманск (8152) 60-74-24 murmansk@rg.ru; Нижний Новгород (831) 216-05-95 nnov@rg.ru; Новосибирск (383) 223-80-29 sibir@rg.ru; Омск (3812) 25-80-15 omsk@rg.ru; Пермь (342) 236-56-55 perm@rg.ru; Ростов-на-Дону (863) 261-91-41 rostov@rg.ru; Санкт-Петербург (812) 449-65-45 sbp@rg.ru; Самара (846) 242-75-28 samara@rg.ru; Саратов (8452) 26-13-63 saratov@rg.ru; Симферополь (3652) 60-02-13 simferopol@rg.ru; Ставрополь (8652) 28-48-02 stavropol@rg.ru; Тюмень (3452) 35-24-94, (3452) 35-25-11 zs@rg.ru; Уфа (347) 276-42-60 ufa@rg.ru; Хабаровск (4212) 31-62-00 gazeta@rgfe.ru; Челябинск (351) 727-78-08 chel@rg.ru; Южно-Сахалинск (4242) 43-20-69 sakhalin@rgfe.ru; Якутск (4112) 42-20-54 sakha@rgfe.ru

© ФГБУ «Редакция «Российской газеты». Все права защищены.
— Любая перепечатка без письменного согласия правообладателя запрещена. Иное использование статей возможно только со ссылкой на правообладателя. Приобретение авторских прав: тел. 8 499 257-56-50
— Рукописи не рецензируются и не возвращаются.
— За содержание рекламных материалов редакция ответственности не несет.
— Материалы в рамке публикуются на коммерческой основе.
— За текст, опубликованный под знаком «Реклама», несет ответственность рекламодатель.
— В региональные выпуски газеты редакцией могут быть внесены изменения.

«Российская газета» печатается в городах: Апатиты, Архангельск, Астрахань, Барнаул, Бишкек, Благовещенск, Владивосток, Владимир, Волгоград, Воронеж, Екатеринбург, Иркутск, Казань, Калининград, Кемерово, Киров, Краснодар, Красноярск, Махачкала, Минеральные Воды, Москва, Нижний Новгород, Новосибирск, Омск, Оренбург, Пенза, Пермь, Ростов-на-Дону, Санкт-Петербург, Самара, Саратов, Симферополь, Томск, Тюмень, Ульяновск, Уфа, Хабаровск, Чебоксары, Челябинск, Чита, Южно-Сахалинск, Якутск, Ярославль

Заявки на электронную версию газеты, ее архивов, а также подписка на «РГ» и приложения: www.rg.ru/subscribe Газета зарегистрирована в Министерстве печати и информации Российской Федерации 28 сентября 1993 г. Регистрационный № 302

Подготовлено отделом деловых приложений «Российской газеты» и дирекцией по рекламе