Фото: freepik.com

ОТЕЧЕСТВО НА СТРАЖЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Последний год принёс государству и промышленникам множество новых вызовов. Санкции жёстко ударили по всем сферам бизнеса и на время лишили предпринимателей возможности крепко стоять на ногах. В это же время пробудилось большое число интернет-злоумышленников, и уровень кибербезопасности в стране пошатнулся. Геополитические факторы изменили ландшафт угроз со стороны хакеров. Способен ли российский рынок информационной безопасности противостоять атакам?

Текст: Анастасия Семёнова

Рынок информационной безопасности (ИБ) в России динамично развивался до 2022, в котором столкнулся с чередой вызовов из-за введения санкций и ухудшения международных отношений. Именно это послужило ростом количества кибератак, считает руководитель отдела информационной безопасности ООО «Цифроматика» **Алексей Винниченко**. Бизнесу в новых реалиях повышенных киберрисков остаётся только адаптироваться.

ХАРАКТЕР КИБЕРАТАК

Что собой представляют кибератаки в 2022–2023 годах? Часть экспертов считает, что текущие угрозы не очень отличаются от тех, что были в 2021-м и ранее: DDoS-атаки, фишинг, вредоносные программы и инсайдерские угрозы. Руководитель отдела продвижения продуктов ООО «Код безопасности» **Павел Коростелев** отметил, что первую очередь злоумышленники атакуют не сами промышленные предприятия, а корпоративные ИТ-системы, которые обеспечивают поддержку бизнеса. К таким угрозам относятся, например, атаки на цепочки поставок, хакерские операции с инфраструктурами контрагентов и другие.

А это, в свою очередь, негативно влияет на производительность заводов, которые, например, недополучают какие-то ресурсы, необходимые в производстве.

Что касается уровня сложности атак, то тут мнения спикеров расходятся. На-

пример, **Алексей Винниченко** считает, что киберпреступникам стало проще действовать. Это может быть связано с ростом рынка продажи доступов к корпоративным сетям и уменьшения их стоимости, а также развития рынка программ-вымогателей по подписке, что делает их доступными для неподготовленных злоумышленников. При этом г-н **Коростелев** уверен: несмотря на то, что ландшафт кибератак практически не изменился, их качество и интенсивность выросли. «Видно, что за дело взялись не любители, а профессионалы», — заявил **Павел Коростелев**.

По мнению CEO и управляющего командой разработчиков ООО «Степ Ап Лаб» **Романа Саркисова**, в последние несколько лет киберзлоумышленники сосредоточились на проникновение в сеть с использованием социальной инженерии: хакеры убеждают сотрудника установить приложение или выполнить иные действия, которые приведут к получению доступа в локальную сеть, домен или почтовый сервер. Эти действия образуют массу проблем на предприятиях. Например, в результате захвата ERP-системы или её модуля чужаки, получившие несанкционированный доступ, могут повредить оборудование или устроить сбой производственного цикла. А хищение персональных данных сотрудников позволяет преступникам использовать шантаж или запугивание с целью получить критическую коммерческую информацию.

«Надо понимать, что попасть в ИТ-систему компании или тем более предприятия довольно непросто, это требует серьёзных навыков, времени и денег, поэтому наибольший риск — в социальной инженерии. Человек — по-прежнему самое слабое звено любой системы защиты, поэтому компаниям нужно проводить постоянную работу по повышению киберграмотности», — поделился мнением г-н **Коростелев**.

Впрочем, импортозамещение ПО оказалось не на руку злоумышленникам, которым приходится получать новые навыки. Г-н **Винниченко** предположил, что основной удар в этом году стоит ждать на операционные системы Linux. Спикер уверен, именно из-за трудностей в замещении ПО системы иностранных вендоров будут наиболее уязвимы к атакам. Причиной тому могут быть сложности процесса установки обновлений или необходимость тщательной проверки и тестирования каждого обновления.

Спикеры отметили и выросший в 2022–2023 году уровень хактивизма. Хакеры с невысокими навыками, но жёсткой гражданской позицией стали массово атаковать ИТ-инфраструктуры различных компаний, от частных до государственных. Невзирая на то, что они не смогут нанести серьёзного урона, огромное количество попыток это сделать доставляет определённое беспокойство.

УРОВЕНЬ КИБЕРБЕЗОПАСНОСТИ

В основном с большими киберрисками столкнулись компании, которые используют программы, глубоко интегрированные в бизнес-процессы, а также специализированные отраслевые решения, построенные на базе инфраструктурных продуктов иностранных вендоров. **Алексей Винниченко** отметил среди них SAP, а также разнообразные АСУ ТП.

«Зачастую такие продукты не имеют поддержки отечественных решений, и импортозамещение может сопровождаться заменой большей части оборудования и технологий или изменением бизнес-процессов компаний. К такому бизнесу можно отнести в основном организации — субъекты критической информационной инфраструктуры: от банков и финансовых организаций, предприятий промышленной сферы до клиник и региональных перевозчиков», — объяснил спикер.

Оценить то, что сейчас происходит с информационной безопасностью на заводах, довольно сложно. Эксперты говорят, что такие данные, как правило, являются коммерческой тайной. **Роман Саркисов** рассказал, что в профильных телеграм-каналах то и дело публикуется информация о новых шантажах и утечках, новых и повторных взломах, однако поток сообщений гораздо меньше, чем в 2022 году. Спикер предположил два варианта, объясняющих такую перемену: либо безопасность сетей и систем улучшилась, либо фокус внимания хакерских группировок вернулся к привычному: к обману частных лиц, хищению и подделке личных данных и т. п.

Преподаватель департамента «Программной инженерии» в Научно-исследовательском университете «Высшая школа экономики» (НИУ ВШЭ) **Лев Немировский** уверен, что уровень кибербезопасности промышленных предприятий с 2021 по 2023 год улучшился благодаря активному внедрению новых технологий и решений, а также осознанию важности ИБ среди руководителей.

Прошедший год задал тренд на импортозамещение, вследствие которого

ЭКСПЕРТ

РОМАН САРКИСОВ,
CEO и управляющий командой разработчиков ООО «Степ Ап Лаб»

«С точки зрения экономической мощности или ёмкости рынок вскоре увеличится. Компании будут развивать имеющиеся продукты безопасности, разрабатывать и выпускать замещающие аналоги ПО ушедших западных компаний. Это позволит отказаться от параллельного импорта «недружественных решений» и увеличит долю ИБ компаний на мировом рынке подобных услуг. Внимание хакеров «всего мира» в 2023 году будет сосредоточено на России и российских компаниях, поэтому отечественные эксперты в области безопасности будут и дальше получать много практического опыта в отражении атак и расследованию последствий. Популярность темы ИБ привлекает в отрасль креативную молодежь и карьеристов, что даёт богатую почву для создания новых компаний-стартапов, в которые охотно вкладываются и спонсируют государственные корпорации, например «Ростелеком». К 2024 году мы ожидаем новостей о замене ПО уходящих брендов аналогами и даже более совершенными и продвинутыми разработками в силу наличия нескончаемого потока опыта и накопления больших объёмов информации о методах организации и проведения атак».

бизнес начал адаптацию с планирования мероприятий и бюджетирования проектов. Согласно указам президента № 166 от 30.03.2022 года и № 250 от 01.05.2022 года процессы импортозамещения необходимо завершить к 2025 году. Отсюда и возникла повышенная активность: заводы, которые подвергались кибератакам, начали стремительно внедрять российские продукты ИБ. Однако это ещё не значит, что иностранные системы совсем отошли на второй план. **Алексей Винниченко** уверяет, что в разработках широко используются и opensource-решения. Например, лидирующие позиции кейсов импортозамещения в ООО «Цифроматика» занимают проекты перевода систем, функционирующих на операционных системах семейства Microsoft Windows, на Astra Linux под ключ.

Г-н **Коростелев** считает, что уровень киберзащиты промышленности существенно вырос за последние годы, благодаря закону 187-ФЗ, который регулирует безопасность критических объектов инфраструктуры.

«За счёт этого ещё до ухода западных вендоров у нас был налажен переход на отечественные средства защиты, которые если и уступали в чём-то заграничным решениям, то за пятилетний срок существенно подтянулись. Конечно, российские вендоры по-прежнему отстают, например, в защите АСУ ТП, но как показывает прошлый год, безопасность у нас на высоком уровне. Несмотря на небывалую волну кибератак, мы не слышали о серьёзных инцидентах на предприятиях», — заявил **Павел Коростелев**.

В КАКОМ СОСТОЯНИИ РЫНОК ИБ?

События, которые произошли за последние 12 месяцев, перевернули не только обычный строй бизнеса, но и отношение к информационной безопасности. По мнению г-на **Винниченко**, теперь многие поняли: формальный подход к защите сетей не может защитить бизнес от реальных угроз.

Что касается рынка ИБ, то **Павел Коростелев** считает, что сейчас он находится в переходной стадии, которая характеризуется скачкообразным ростом.

«Прошлый год поставил перед частными компаниями и государственными организациями ряд серьёзных вопросов, поскольку, во-первых, с рынка ушли крупные западные вендоры, чьи решения составляли костяк ИТ-инфраструктур большинства предприятий, во-вторых, существенно вырос уровень враждебности киберсреды», — поделился наблюдениями г-н **Коростелев**.

Игроки рынка уже начали подстраиваться под другие условия и стремятся заменить ИТ-инфраструктуру. Освободившиеся после ухода западных компаний места активно занимают российские вендоры, которые наращивают объёмы поставок и компетенции.

Роман Саркисов уверен, что в целом IT-компании, специализирующиеся на безопасности, выигрывают от введённых санкций и угроз со стороны западного финансово-технического лобби. На фоне отсутствия возможности приобретения альтернативного ПО и роста количества/качества угроз российские продукты стали ещё более востребованы.

Таким образом, кажется, что ситуация под контролем и в целом информационная безопасность переживает, возможно, непростой, но важный для развития период. Однако значительной проблемой в отрасли остаётся недостаток специалистов, связанный с отъездом части ИТ-общества за границу. По словам г-на **Саркисова**, на оставшихся специалистов распределилась текущая нагрузка всего сектора и обрушилась масса новых вызовов от атак, что вызывает физическую и эмоциональную перегрузку и приводит к депрессиям.

ИХ БОРЬБА

Пусть виды и характер угроз особенно не изменились, способы защиты от них, очевидно, стали другими. Привычные зарубежные инструменты уже не работают, а в редких случаях даже становятся проводниками для злоумышленников. Как предприятия справляются с натиском кибератак в условиях санкций? По мнению экспертов, ответ на этот вопрос можно получить, исходя из количества инцидентов в информационной безопасности. Например, в прошлом году на всю страну прогремело несколько серьёзных случаев, но в общем числе угроз это не так много.

ЭКСПЕРТ

АЛЕКСЕЙ ВИННИЧЕНКО,
руководитель отдела информационной безопасности ООО «Цифроматика»

«С проблемами столкнулась большая часть бизнеса, использующая западные решения для построения ИТ-инфраструктур и защиты внешнего периметра. В основном речь идёт о продуктах компаний Microsoft, Cisco, WMware, Oracle, так как зачастую защитные механизмы именно этих решений составляют базу систем ИБ. Волны атак, обрушившиеся на бизнес за прошедший год, до сих пор не утихают, и мы в ближайшее время не ждём смены этой тенденции».

При этом **Павел Коростелов** отметил, что зарубежные инструменты, хотя и высокого качества, не являются «мечом-кладенцом», ведь российские решения во многих сегментах им не уступают.

«Проблема безопасности заключается том, что с уходом западных вендоров ИБ-инфраструктура отечественных компаний превратилась в своеобразный винегрет. Раньше для обеспечения ИБ нужно было привлечь двух вендоров с десятью решениями, а сейчас — пять с двадцатью. Решать возникающие проблемы с защитой проще с одним-двумя партнёрами, чем с пятью, но эта ситуация не критична», — поделился г-н **Коростелов**.

Кроме того, в условиях участившихся кибератак растут и бюджеты предприятий на защиту. Российские ИБ-компании всё чаще стали внедрять или модернизировать СОИБ, аудиты защищённости и пентесты. Г-н **Винниченко** выделил сферы, которые особенно сильно наращивают инвестиции в кибербезопасность — это субъекты КИИ и госсектор, так как общедоступные ресурсы и инфраструктуры являются основными целями злоумышленников.

Спикеры считают, что 2022 год подарил специалистам по ИБ колоссальный опыт, и уже сейчас не ощущается нехватки ПО из недружественных стран. Предприятия находятся под защитой российских сертифицированных разработок. На рынке широко представлены межсетевые экраны следующего поколения (NGFW). Кроме того, в России есть SIEM-системы высокого качества, поэтому эти продукты легко замещаются.

Роман Саркисов отметил, что за счёт ухода с отечественного рынка таких компаний, как Cisco, Eset, Norton, Avast, освободилось 2/3 рынка. Высвободившиеся места кратно увеличили продажи для уже устоявшихся на рынке компаний, а также привели к росту стартапов и независимых команд, специализирующихся на защите информации и отражении кибератак. Также в 2022 году прошла всероссийская программа DeepTech Cybersecurity от Фонда «Сколково», которая привлекла свыше ста участников. Победителями отобраны 6 команд со стартапами, 4 из них — резиденты «Сколково». Эти команды стали успешны благодаря разработанным и внедряемым методам и комплексам защиты данных.

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ

Исходя из комментариев экспертов, подытожим: ИБ страны проходит важный этап в развитии, при этом в багаже у ИТ-компаний уже есть достаточное количество отечественных решений, которые могут в полной мере обеспечить промышленности и другим сферам качественную защиту от хакерских атак и утечек данных. Также на рынке появляется всё больше стартапов, которые готовы занять места ушедших иностранных разработчиков. **Лев Немировский** уверен, что к концу 2023 — началу 2024 года рынок ИБ будет ещё более крепок за счёт инноваций и сотрудничества между компаниями и госорганами. Однако угрозы кибербезопасности также продолжат эволюционировать, и предприятиям необходимо активно адаптироваться к изменяющемуся ландшафту угроз.

Роман Саркисов аккумулировал опыт ИБ в небольшую рекомендацию по защите для бизнеса. Таким образом, при подходе к обеспечению ИБ нужно обратить внимание на все типы рисков, не выделяя что-то одно.

- Важно установить «железную» защиту от DDoS-атаки или подключится к интернет-провайдеру, который предоставляет такую для своих клиентов.
- Обратить пристальное внимание на обучение сотрудников безопасному поведению в интернете и безопасным методам работы с входящей почтой и файлами. Это связано с тем, что основным каналом атак является социальная инженерия.
- Установить все возможные обновления на сетевые устройства, а также обновить ПО на компьютерах и модулях ERP, которые непосредственно контактируют с автоматизированными линиями, датчиками и устройствами безопасности в закрытом контуре.
- Убедиться, что критически важное для обеспечения безопасности людей и непрерывности производственного цикла оборудование не контактирует с интернетом и не может быть подключено к серверам злоумышленников с использованием «человеческого фактора».
- Установить сложные пароли в локальных сетях предприятия и на доверенных узлах, а ключ корневого сертификата хранить на защищённом токене в надежном сейфе.

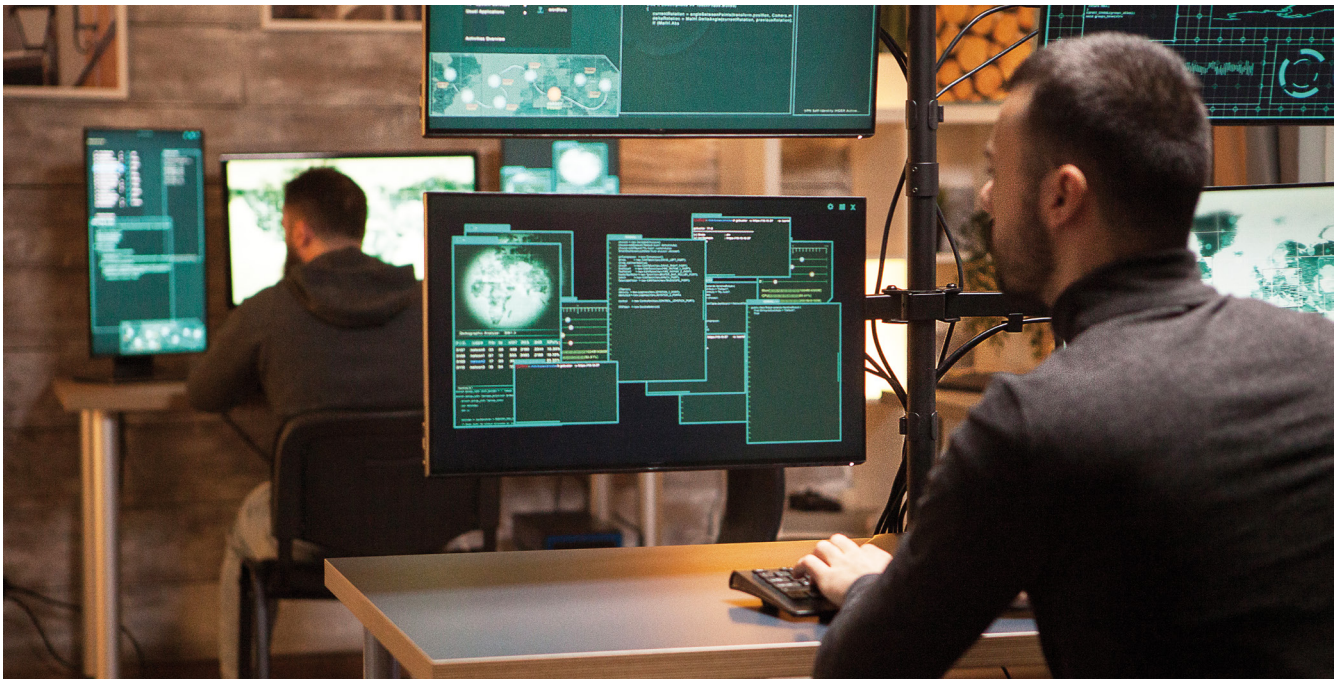

Фото: freepik.com