ПРОМЫШЛЕННАЯ КИБЕРБЕЗОПАСНОСТЬ: ТЕНДЕНЦИИ, РЕШЕНИЯ И ВЫЗОВЫ

Киберугрозы в последние годы всё больше терроризируют промышленность. Хакеры видят в ней «золотую жилу» — представьте, на что готовы пойти ГЭС, если встанет вопрос остановки всей станции и лишения города или даже страны электричества. Конечно, в таком масштабе кибератаки происходят редко, но риски для промышленников только растут. Как предприятиям обезопасить производство, и что для этого предлагают разработчики?

Текст: Анастасия Семёнова. Фото: freepik.com

Промышленность разрастается, погружается в технологии и становится лакомым куском для хакеров, их действия становятся успешнее и сложнее. Жертвы взломов, пытаясь выявить кибератаки, долгие годы остаются в иллюзии безопасности, применяя неэффективные методы борьбы, считают эксперты.

Пандемия и связанный с ней переход на дистанционный бизнес тоже внёс свои коррективы, и помог хакерам найти новые пути давления. Сейчас руководство контролирует бизнес-процессы онлайн, также и управляет производством и организует работу через интернет вещей. Это уже потенциальное окно для внедрения на бизнес-платформу третьих лиц. Согласно статистике, в 2020 году по сравнению с 2019 годом прирост хакерских атак на промышленные компании составил 91%.

КИБЕРУГРОЗЫ — КАКИЕ ОНИ?

Весь мир перешёл в сеть, и тут-то хакеры почувствовали силу. Особенно уязвлёнными оказались те предприятия, которые только начали практиковать удалённую работу. Они не были готовы к такому объёму трудностей. Эксперты утверждают, что превалирующая часть предприятий до сих пор использует устаревшее ПО, из-за чего круг уязвимых для хакеров мест последние годы растёт с большей силой. Да, раньше АСУ ТП использовало собственную физическую изоляцию для защиты от взломов, но сейчас этот способ уже не сработает. Промышленники в большей степени стали цифровыми предприятиями, работающими за счёт интернета вещей, искусственного интеллекта, роботизации и дополненной реальности, благодаря этим модернизациям компании повысили свою производительность и привлекли к себе ещё больше киберугроз.

Перед службами информационной безопасности встала тяжелейшая задача — хотя бы просто сократить количество киберугроз, которые выливаются в шпионаж и денежное вымогательство, и минимизировать количество аварий на предприятиях. Для этого нужно определить основной вектор нападок хакеров.

ПРОМЫШЛЕННИКИ В БОЛЬШЕЙ СТЕПЕНИ СТАЛИ ЦИФРОВЫМИ ПРЕДПРИЯТИЯМИ, РАБОТАЮЩИМИ ЗА СЧЁТ ИНТЕРНЕТА ВЕЩЕЙ, ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, РОБОТИЗАЦИИ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ. БЛАГОДАРЯ ЭТИМ МОДЕРНИЗАЦИЯМ КОМПАНИИ ПОВЫСИЛИ СВОЮ ПРОИЗВОДИТЕЛЬНОСТЬ И ПРИВЛЕКЛИ К СЕБЕ ЕЩЁ БОЛЬШЕ КИБЕРУГРОЗ

Итак, руководитель отдела развития бизнеса продуктов ИБ компании АО «Аксофт» **Игорь Тюкачёв** делит наиболее интересующие кибертеррористов процессы на промышленном предприятии на две части. К первой относятся корпоративные сети и ресурсы, связанные с рабочими местами, это ERP-системы, «1С Бухгалтерия» и другие.

«Корпоративная сеть предприятий подвергается таким же киберугрозам, как и непромышленные компании — рабочие места, серверы, сетевое оборудование атакуются с помощью вредоносного и шпионского ПО, шифровальщиков и других средств», — заявил **Игорь Тюкачёв**.

Ко второй части относятся промышленные сети АСУ ТП, автоматизированные рабочие места и серверы АСУ ТП, которые совсем не связаны с корпоративной сетью. По словам г-на **Тюкачёва**, кибератаки на промсети — это проблема последних десяти лет. Согласно статистике «Лаборатории Касперского», на 39% АРМ в России, относящихся к АСУ ТП, была зафиксирована вредоносная активность. Наиболее популярный сектор для взломов — энергетический комплекс и нефтегазовая отрасль.

Отметим, что угрозам подвергаются не только АСУ ТП, но и платформы для связи с партнёрами, поставщиками и клиентами — ERP, PM и CRM-системы.

Ведущий системный инженер Varonis Systems **Александр Ветколь** добавил, что также атакам часто подвергается внешний периметр и программы аутентификации на открытых шлюзах. Атакуют, как правило, промежуточные платформы, открывающие доступ к конечной цели. Кибертеррористам интереснее разрушить объект промышленного предприятия или средства производства: внести изменения, которые остановят техпроцесс, или, если возможно, негативно повлияют на конечный продукт.

А В ЧЁМ СОЛЬ?

Чтобы понимать, как правильно подобрать системы защиты, лучше знать наверняка мотивы взломщиков. Немало хакеров, которые действуют по принципу: я это умею, так почему бы нет. Взломать информационную сеть предприятия для них, по мнению **Игоря Тюкачёва**, это как ночью разбить витрину в магазине.

Есть ещё один тип взломщиков — бывшие сотрудники, которые имели разногласия с руководством. А ещё взломщики затесались и среди специалистов по ИБ, которые не работают в компании, они находят уязвимое место в системе безопасности и проверяют, насколько далеко они могут зайти. Конечно, после всех проверок хакеры связываются с компанией и докладывают об уровне ИБ.

Самые опасные из взломщиков те, что устраивают спланированную хакерскую атаку с целью заработать денег. Во что выльется кибератака, зависит от уровня автоматизации предприятия, это может быть и исчезновение отчётности по производственному товару, и остановка про-

цессов на предприятии. На многих заводах в случае нарушения рабочих процессов запускается ручной режим работы, поэтому наибольшая вероятность, что после взлома завод просто останется «без глаз», то есть без статистики, аналитики, информации, которую предоставляют датчики.

В качестве примера вспомним остановку производства на заводе Honda, когда в корпоративную сеть был запущен один шифровальщик, а простой занял целый рабочий день.

БОЛЬШАЯ РАБОТА

Перед специалистами ИБ стоит серьёзная задача, тем более в нынешних условиях, когда через сеть можно проникнуть в самые глубины производства и достать оттуда самую конфиденциальную информацию.

Работа колоссальная — службе безопасности нужно оценить риски, рассмотреть возможные пути уязвления компании и потенциальные последствия кибератак. Эти данные позволят выбрать подходящую стратегию для защиты информационной системы компании. Большая работа связана с изоляцией базы данных, так как, согласно статистике, именно кража данных является основной целью взломщиков.

Для того чтобы в полной мере обеспечить безопасность АСУ ТП предприятия, по словам **Игоря Тюкачёва**, основная задача специалистов — организовать исполнение требований регуляторов в области защиты значимых критических информационных инфраструктур (КИИ), защиту АСУ ТП. Но это возможно только после процедуры категорирования КИИ и определения этих объектов. Сюда войдут организационные мероприятия по защите нормативной документации и внедрение программно-аппаратных ИБ-решений: антивируса для защиты рабочих мест и серверной инфраструктуры, SIEM — для сбора событий и логов, продукта по защите периметра, сетевого сенсора — решения класса NTA.

В случае если объект КИИ не такой уж значимый, то и жёстких требований по программно-аппаратной защите его не будет. Тогда обезопасить предприятие можно, исходя из представления об угрозах ИБ самим предприятием.

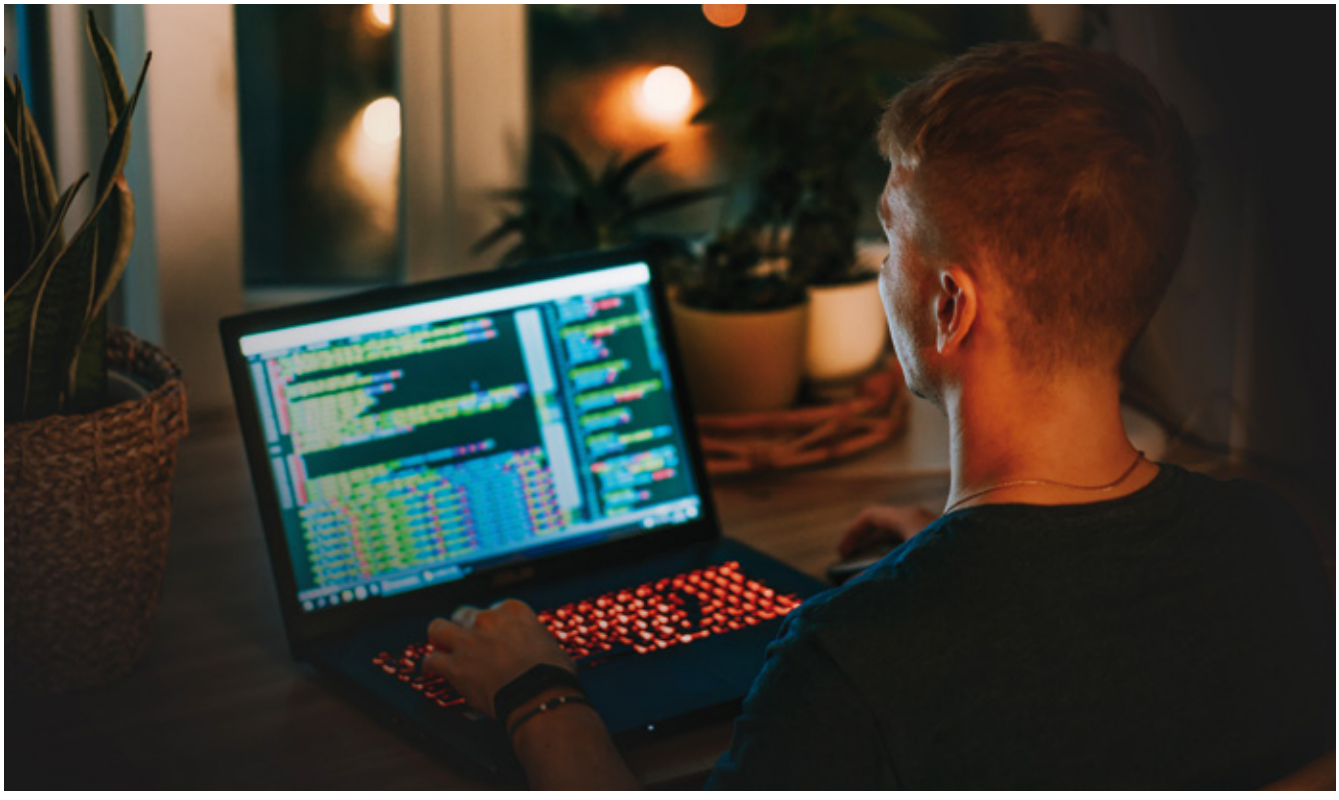
«Необходимо вести защиту ИС и АСУ ТП предприятия, ИТ и ИБ-инфраструктуры и периметра с учётом концепции «нулевого доверия», регулярно проводить мониторинг параметров работы и доступа ко всем системам, а также организовать исключительно однонаправленный доступ к внешним сетям», — подтвердил **Александр Ветколь**.

Если говорить о том, какие обязательные действия должны выполнить специалисты ИБ для защиты системы управления предприятием, то эксперты утверждают, что ничего мудрёного тут нет — это стандартный перечень мер любого подразделения ИБ: обеспечение безопасности рабочих мест и инфраструктуры (антивирусы, EDR), защита периметра (NGFW, proxy, SWG), защита от утечек информации (DLP), внедрение средств криптозащиты (СКЗИ/VPN).

В случае, когда предприятие опытное и уже сталкивалось с очевидной опасностью, то применяется ещё и управление учётными данными (IDM, PAM). А если нужно защитить данные с АСУ ТП, г-н **Тюкачёв** говорит, запускаются иные меры: начиная с разработки модели угроз, подготовки нормативной документации по системе обеспечения информационной безопасности и заканчивая внедрением средств защиты.

«Внедрение решений для кибербезопасности — это часть процесса повышения уровня защиты компании. В современных реалиях — это 100% необходимость, как, например, чистить зубы утром и вечером. Внедрение технических средств идёт рядом с организационными мероприятиями и повышением осведомленности персонала предприятий», — считает г-н **Тюкачёв**.

Необходимо создать воздушный зазор между корпоративной и промышленной сетью, защитить периметр промышленной сети, регламентировать работу сотрудников, чтобы они не подключали к сети 3G-модемы, регламентировать работу подрядчиков. Также важно обучить сотрудников правилам работы со входящей почтой и файлами, проинструктировать персонал, какие шаги необходимо сделать, если промышленную сеть взломали и основные процессы остановились. Чем лучше защищено предприятие, тем сложнее будет злоумышленникам его «взло-



В

2021

ГОДУ КОЛИЧЕСТВО КИБЕРАТАК НА КОРПОРАТИВНЫЕ СЕТИ ПО СРАВНЕНИЮ С

2020

ГОДОМ УВЕЛИЧИЛОСЬ НА

50%

мать», тем дороже будет стоить атака. И, возможно, взламывать станет экономически невыгодно, считает **Игорь Тюкачёв**.

ЧЕМ ЗАЩИТИТЬСЯ

С ростом количества киберугроз набирает обороты рынок платформ информационной безопасности. Среди самых эффективных решений контроля утечки данных эксперты отмечают мониторинг с помощью системы DAM/DBF — Data access management — управление доступом к данным/Data base firewall — межсетевой экран баз данных, к таким относится программа «Гарда БД». В её функции входит аудит действия администраторов, защита базы данных, выявление теневых баз на предприятии, обнаружение инцидентов и их расследование.

Кроме того, **Игорь Тюкачёв** отмечает — для киберзащиты промышленной сферы актуальны решения, обеспечивающие контроль сетевой активности внутри периметра промышленных сетей и защиту периметра. Например, такие задачи успешно решают Kaspersky KICS, Positive Technologies ISIM, промышленные фаерволы UserGate, InfoWatch ARMA и другие.

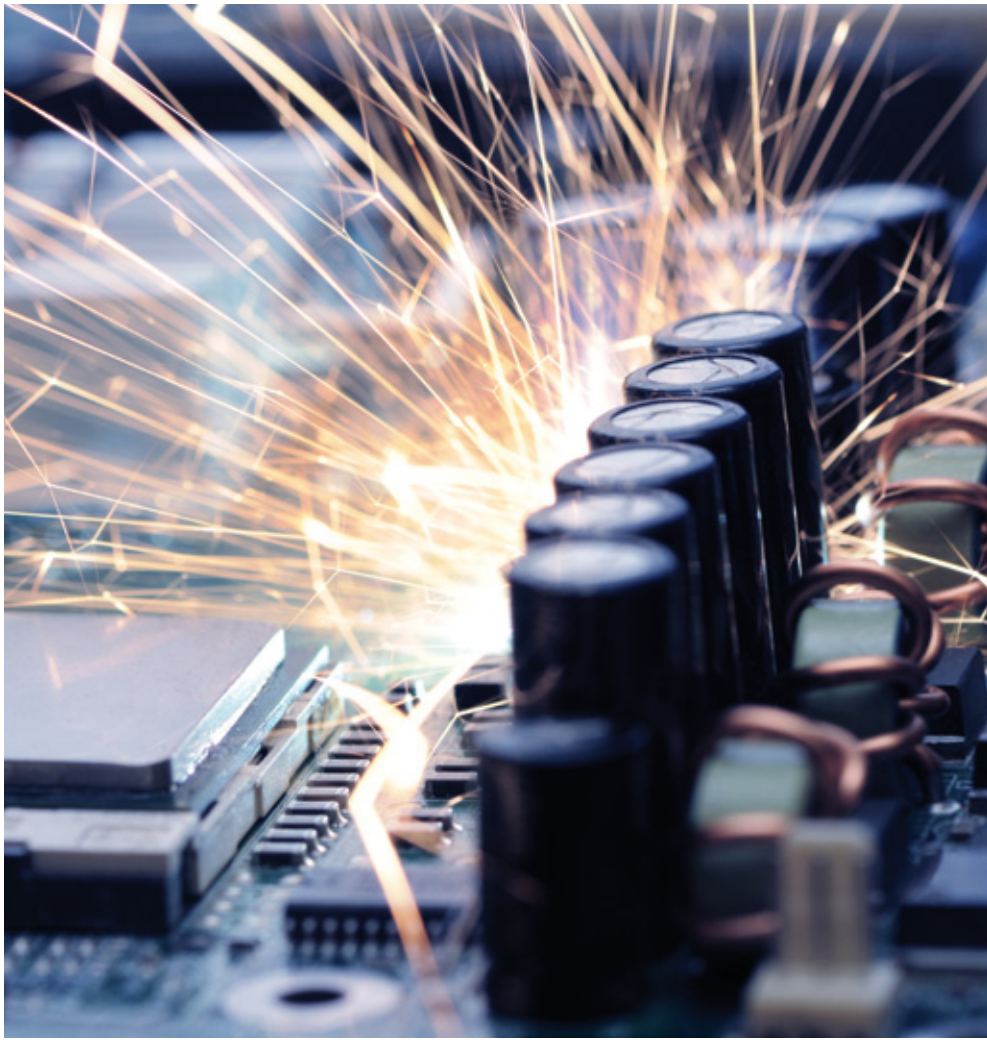
Готов ли российский рынок разработчиков дать необходимые инструменты защиты заводам?

По сообщению г-на **Тюкачёва**, ключевые игроки рынка ИБ либо уже выпустили решения по защите промышленных сетей и АСУ ТП, либо находятся в процессе разработки.

«Здесь нужно понимать, что средства обеспечения безопасности АСУ ТП отличаются от ИБ-решений для корпоративных сетей только тем, что защита АСУ ТП не должна вносить задержек в работу системы и влиять на работу защищаемых объектов», — заметил г-н **Тюкачёв**.

НАДЕЖДА НА ЛУЧШЕЕ

Информационная безопасность страны и промышленных объектов находится под угрозой, особенно в нынешнее время. То, как отечественные решения отреагируют и насколько смогут предотвратить и отразить взломы, покажет будущее российской отрасли кибербезопасности. Так или иначе, выбор невелик, и сильнейшие специалисты отрасли в стране будут развиваться с большей силой.



К СЛОВУ

Необходимо создать воздушный зазор между корпоративной и промышленной сетью, защитить периметр промышленной сети, регламентировать работу сотрудников, чтобы они не подключали к сети 3G-модемы, регламентировать работу подрядчиков.