Дмитрий РЫЧКОВ:

«Информационная безопасность – неотъемлемая часть общей системы безопасности предприятия»

На фоне импортозамещения и набирающей обороты цифровой трансформации промышленных предприятий все больше внимания уделяется обеспечению информационной безопасности. Поводами для этого служат не только ужесточение требований законодательства, но и повышение активности злоумышленников, многовекторность атак, которым подвергаются промышленные объекты. Огромное количество новых угроз провоцирует стремительное развитие беспилотных летательных аппаратов. Многие промышленные предприятия вынуждены создавать и совершенствовать свои системы безопасности в ускоренном темпе. Почему возникла такая необходимость, какие ИБ-риски наиболее актуальны сегодня, в том числе для предприятий оборонно-промышленного комплекса, насколько изменились требования к уровню квалификации ИБ-специалистов? Об этом и многом другом в интервью журналу Connect в преддверии форума по цифровизации оборонно-промышленного комплекса – «ИТОПК-2024» – рассказал директор Центра промышленной безопасности компании «Информзащита» Дмитрий Рычков.

– С 1 марта 2025 г. в отношении предприятий – субъектов КИИ, многие из которых являются промышленными объектами, ожидается усиление требований к замещению используемого ими иностранного оборудования и ПО. Эксперты считают, что не все организации успеют импортозаместить технологии к этому времени. Какие риски это несет для промышленности?

– В целом в России наблюдается значительная волна импортозамещения, что, конечно, затрагивает и промышленность. Для государственных (муниципальных) организаций, в банковской сфере сроки и требования были более жесткими. Но благодаря этому процесс начался раньше и достиг существенного прогресса. Для коммерческих организаций, владеющих промышленными предприятиями и опасными производственными объектами, обязательным является переход на 100%-ное использование на значимых объектах критической информационной инфраструктуры (ОКИИ) доверенных программно-аппаратных комплексов (ПАК) к 2030 г. Приобретение недоверенных ПАК запрещено с 1 сентября 2024 г. При этом предусмотрен механизм обоснования отсутствия аналогов ПАК посредством экспертизы.

Такие требования стали проблемой для некоторых предприятий, которые находятся на стадии закупки оборудования для долгосрочных проектов строительства (модернизации).

Следующие шаги по усилению регулирования импортозамещения в КИИ ожидаются после принятия законопроекта № 581689-8 «О внесении изменений в Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации”», который вступит в силу 1 марта 2025 г. Согласно документу к обязательствам Правительства РФ добавятся полномочия по установлению требований к использованию программного обеспечения и отечественной радиоэлектронной продукции, будет определен порядок перехода и его мониторинга.

Как показывает опыт взаимодействия с заказчиками из промышленности, многие нашли отечественные аналоги на уровне ПЛК и SCADA, и все новые проекты модернизации выполняются с их использованием. Для некоторых решений в промышленности пока объективно нет альтернативных вариантов замены – для таких случаев регулятор предусматривает механизмы отсрочки. На мой взгляд, продолжение использования оборудования и ПО из «недружественных» стран в критичных областях деятельности несет больше рисков, чем опасность столкнуться с трудностями при плановом импортозамещении.

> Специалисты считают, что к концу 2024 г. сегмент БПЛА увеличится до 13 млрд руб., а к 2028 г. превысит 80 млрд руб.

– Значимость информационной безопасности постоянно повышается. Это характерно и для промышленных предприятий? Какие инциденты – физические или в сфере ИБ – несут большую угрозу для промышленности?

– Информационная безопасность сегодня – неотъемлемая часть общей системы безопасности. Поэтому, наверное, разделять их не имеет смысла. Физические инциденты, т. е. сбои в работе оборудования, ошибки, допускаемые человеком, и т. д. происходят регулярно. Инциденты ИБ – более редкие явления для промышленного предприятия, но они крайне опасны.

> Информационная безопасность сегодня – неотъемлемая часть общей системы безопасности.

По данным «Информзащиты», около 17% всех атак с помощью программ-вымогателей приходится именно на промышленные предприятия, и это самый высокий показатель среди всех отраслей экономики. При такой атаке злоумышленники шифруют определенную часть данных компании и требуют деньги за то, чтобы снять блокировку и вернуть доступ к корпоративной информации. Подобные события крайне опасны для промышленных предприятий, часть которых являются градообразующими, часть работают по принципу непрерывного цикла. Остановка их работы представляет опасность для экономики, для жизни и здоровья людей, для функционирования целых населенных пунктов. Именно на это и рассчитывают хакеры, которым надо получить средства как можно быстрее, а у промышленности нет времени на то, чтобы найти альтернативные пути решения проблемы.

Не следует также забывать, что за последние два года серьезно возросла активность хактивистов, главная задача которых – нанести наибольший ущерб организации, разрушить

ее информационную систему. В первой половине 2024 г. по сравнению с аналогичным периодом 2023-го на 40% возросло количество деструктивных атак. Конечно, нападение на промышленные объекты – одно из приоритетных направлений для них, так как промышленность – одна из основ российской экономики, ее разрушение нанесет колоссальный вред.

Получается, что инциденты информационной безопасности ведут к физическому нарушению работы промышленного предприятия, а значит, в современных реалиях нам пора перестать выделять их в отдельную категорию, существующую, грубо говоря, параллельно. Их надо рассматривать как часть общей картины рисков промышленного предприятия.

– В последние годы беспилотники применяются государственными организациями, военными структурами, бизнесом и частными пользователями. Зачастую БПЛА используют для нанесения урона промышленным предприятиям, актуальность защиты от них также повышается. На каком уровне сейчас спрос на антидрон-системы? Какой процент промышленных предприятий оснащен такими системами? Какие угрозы для промышленных предприятий несет использование дронов?

– Действительно, рынок гражданских беспилотников развивается, одним из факторов, стимулирующих этот процесс, является снижение стоимости производства устройств. Специалисты считают, что к концу 2024 г. сегмент БПЛА увеличится до 13 млрд руб., а к 2028 г. превысит 80 млрд руб. Столь значительный объем указывает, конечно, на то, что и вероятность негативных событий, к которым ведет использование дронов, также увеличивается.

Спрос на системы борьбы с беспилотниками постоянно возрастает. Надо учитывать, что это достаточно молодой рынок, так как массовое применение БПЛА и их использование для нанесения вреда объектам инфраструктуры, промышленным предприятиям и т. д. – это явление, набравшее популярность в последние пару лет. Сегодня большие производственные компании хотят установить себе такие системы, чтобы избежать проблем в будущем. Малые и средние предприятия тоже проявляют интерес к данным средствам. Понятно, что у крупного и небольшого бизнеса разные возможности и, соответственно, разные запросы. Кому-то нужны стационарные системы, а кому-то достаточно иметь антидроновые ружья, с помощью которых можно нейтрализовать опасные БПЛА. Что касается сегментов, то самый большой спрос на такие устройства – в нефтегазовой отрасли, добывающей и тяжелой промышленности.

Не менее серьезной проблемой для промышленности могут стать

дроны, которые предприятия используют в собственных целях.

– Почему?

– Во-первых, недостаточная обученность персонала для управления ими может спровоцировать аварийные ситуации. Утратив управление, пилот повредит объекты на территории промышленного предприятия. Во-вторых, дроны, как и любую другую технику с подключением к сети, можно взломать. В этом случае злоумышленники могут получить доступ к управлению беспилотником и устроить диверсию либо шпионить за работой промышленного предприятия с помощью захваченного БПЛА. Иными словами, дроны могут применяться для внешней атаки на предприятие и представлять опасность при внутреннем использовании. Важно принимать превентивные меры: обучать персонал грамотно использовать беспилотники, устанавливать на БПЛА современные средства защиты информации, регулярно проверять их надежность. В противном случае инструмент, который должен приносить предприятию пользу, станет «троянским конем».

– Промышленные предприятия, как и все организации, стремятся к максимальной автоматизации производства. Сколько времени, на ваш взгляд, потребуется для достижения такого уровня систем, чтобы они работали без помощи человека?

– Мне кажется, автоматизация производства – это процесс, который начался много лет назад и никогда не закончится. Человек всегда будет разрабатывать технологии, которые должны его заменить, интегрировать их, а потом осознавать, что в соседнем цехе замены ему нет, и снова создавать очередную инновацию.

Конечно, автоматизация несет пользу, ускоряет производство, экономит промышленному предприятию ресурсы. Такие решения, безусловно, надо внедрять. Однако вопрос о том, когда системы смогут работать без управления человеком или как минимум без контроля с его стороны, скорее, философский. Не думаю, что нас в ближайшее время ждут полностью автономные предприятия. Более того, интеграция новых технологических решений зачастую требует наличия специалистов, которых ранее не было в штате. То есть автоматизация еще и создает новые рабочие места.

Мне кажется, автоматизация производства – это процесс, который начался много лет назад и никогда не закончится.

В сфере информационной безопасности тоже возникают новые задачи: чем больше технологий, тем больше людей должны заниматься обеспечением их защищенности от теоретических взломов, атак злоумышленников и т. д. Иными словами, дорога к автономности производства намечена, мы движемся по ней, впереди очень долгий путь.

– Насколько надежны автоматические системы оповещения об инцидентах, можно ли на них положиться, или специалисты должны продолжать следить за аварийными ситуациями на производстве?

– Автоматические системы оповещения об инцидентах – крайне важная технология. Человек не может находиться в нескольких местах одновременно. Такая система за счет разных датчиков собирает информацию, находит аномалии в том или ином месте на промышленном предприятии и тем самым вносит огромный вклад в безопасность.

Может ли такая система существовать автономно, без наблюдения человека? На мой взгляд, нет. Дело в том, что автоматическая система способна ошибочно определить аномалию, например, объявить тревогу и остановить производство, когда этого можно было избежать. Остановка предприятий – весьма опасное мероприятие. Кроме того, теоретически система может быть взломана, т. е. злоумышленники могут в своих целях включать ее или, наоборот, выключать. Поэтому необходим человек, который следит за тем, как работает автоматизированная система, какие аномалии она выявляет. Тандем специалиста и технологии – это вклад в максимальное обеспечение безопасности на производстве.

– С 1 сентября вступило в силу распоряжение «Ростехнадзора», который обновил вопросы для тестирования по общим требованиям промышленной безопасности и требованиям по отраслям. Зачем и насколько изменились вопросы? Сложнее или проще теперь будет проходить аттестацию? Существует ли риск, что большое количество специалистов не будут аттестованы, и что ждет в таком случае промышленную сферу?

– Основными причинами такого решения, на мой взгляд, являются изменения в технологиях и используемом оборудовании, а также накопленный опыт и обратная связь по применению прежней редакции. Изменились области аттестации (объединение, разделение, появление новых). По одним тематикам вопросов стало больше, по другим – меньше.

В целом изменения в вопросах ощутимые, поэтому специалистам и учебным центрам (им, наверное, в большей степени) необходимо подготовиться. По поводу количества специалистов, которые не смогут пройти аттестацию, прогнозировать трудно. Но аттестация

специалистов, работающих на ОПО, не должна быть слишком легкой или условной.

– У каждого сегмента промышленности свои особенности и обстоятельства, поэтому у разных предприятий разные риски и уровень защищенности. Предприятия какой отрасли сегодня защищены лучше всего? В каких сферах вложения в безопасность требуются незамедлительно?

– На мой взгляд, чем более новая отрасль, тем лучше она защищена. Это ключевой фактор. Многие промышленные предприятия, даже отрасли достаточно консервативны в подходах к технологическому развитию, интеграции новых технологий и т. д. Поэтому новейшие предприятия, занимающиеся производством передовых технологий, обычно защищены лучше других.

На более высоком уровне промышленная безопасность и кибербезопасность находятся в сферах микроэлектроники, робототроения, в атомной отрасли. На этих сложных производствах используется огромное количество современных технологических решений, цифровых инноваций и т. п. Все это подразумевает применение продвинутых инструментов и всеобъемлющих систем безопасности, наличие большой ИБ-команды.

Для таких традиционных сфер, как черная металлургия, горнодобывающая отрасль и т. д., характерны самые большие проблемы с безопасностью. В этих отраслях значительно меньше сложных современных технологий по сравнению с микроэлектроникой или атомной сферой. Соответственно, в представлении руководителей этих предприятий обеспечение промышленной безопасности, информационной безопасности – задача не первоочередная. Конечно, это ошибочное мнение. Мы живем в эпоху, когда любая организация может быть атакована в любой момент времени, поэтому уделять внимание ИБ нужно повсеместно. К счастью, новое поколение руководителей классических промышленных предприятий это осознает и внедряет решения для обеспечения безопасности.

Многим промышленным предприятиям приходится развивать свои системы безопасности в ускоренном темпе. Здесь на помощь приходят такие компании, как наша. Мы предоставляем услуги, охватывающие все их потребности в информационной безопасности, что дает время на создание всеобъемлющей, а главное, отвечающей современным требованиям системы безопасности. ■