О ПРОБЛЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОИЗВОДСТВЕ

Д.В. Рычков (АО НИП «Информзащита»)

Стремительное развитие вычислительной техники и информационных технологий породило одну из глобальных задач начала XXI века – обеспечение защиты АСУТП и создание эффективных систем безопасности производственных активов предприятий. Рассмотрены современных проблемы в области информационной безопасности, характерные для промышленных предприятий.

Ключевые слова: информационная безопасность, кибербезопасность, АСУТП, средства коммуникации, сервисная поддержка технологического оборудования.

Киберугроза — любое незаконное вредоносное проникновение в информационный периметр компании (и некорректные действия, и злонамеренные атаки), которые наносят предприятию значительный ущерб. Последствия остановки работы управляющей компании или линии производства, похищения конструкторской или тендерной документации — это прямые убытки. Тем не менее, мало кто рассказывает о своей беде в открытую, поэтому о компьютерных инцидентах осведомлены только компании, специализирующиеся на оказании услуг в области информационной безопасности (ИБ).

Защита информации на производстве имеет свою специфику и сложность. Во-первых, атакуемые предприятия — это, как правило, объекты критической информационной инфраструктуры (КИИ). Они зачастую являются градообразующими, их остановка может привести к социальному урону, экологической катастрофе, недополучению бюджетом страны налоговых отчислений, невыполнению обязательств по размещенным заказам. Во-вторых, это технологические объекты с дорогостоящим оборудованием, работающим в режиме 24х7. И в третьих, это территориально распределенные организации с разным уровнем информатизации и автоматизации.

Существует два типа сетей: офисная сеть, где сотрудники работают за компьютерами, и промышленная сеть. Если в бизнес-сегменте акцент сделан на обеспечении конфиденциальности, то в сетях АСУТП главное — доступность: необходимо, чтобы все работало без сбоев, учитывая высокий уровень автоматизации производства и современное оснащение сетей предприятий серверами и сетевым оборудованием.

Производство должно работать безостановочно, следовательно, продукты киберзащиты не должны мешать и в то же время должны гарантированно защищать. Такая комплексная задача решается в производственных сетях, которые на порядок сложнее, чем офисные, и имеет ряд специфических проблем.

Информационные процессы на усредненном промышленном предприятии не являются определяющими, на первом месте всегда безотказная работа производственного оборудования. Самый главный принцип при разработке системы и методов киберзащиты на производстве — не навреди. Отсюда возникает несколько проблем.

1) Проблема ограничения возможного контроля угроз ИБ в промышленной сети предприятия в силу особенностей эксплуатации технологического оборудования. Иностранные разработчики производственных линий (механизмов, агрегатов, прокатных станов, станков) превалируют почти во всех типах современного производства. Оборудование стоит дорого и имеет сложную и закрытую цифровую «начинку», часто находится на гарантийной и сервисной поддержке производителя.

2) Проблема совмещения компетенций в области ИБ и технологических процессов, что приводит к необходимости задействования квалифицированных кадров. Такие работы обязательно должны выполняться специалистами, имеющими компетенции одновременно в сетевых технологиях, информационных системах, АСУТП, а также понимающих особенности подходов крупных производителей технологий к вопросам безопасности.

3) Невозможность рассмотрения мероприятий ИБ без учета мероприятий собственно промышленной безопасности (транспортной, энергетической и др., в зависимости от отрасли). Последний пункт может показаться спорным. Но, если вспомнить, что объекты КИИ определяются именно по степени возможного ущерба для окружающей среды и социума (что прописано в ФЗ № 187-ФЗ и приказах ФСТЭК России), то без учета влияния угроз ИБ на поведение систем промышленной безопасности средств противоаварийной автоматической защиты (ПАЗ), систем взрывопожаробезопасности и, конечно, человеческого фактора, то есть в том числе и систем охраны труда, наверное, всерьез рассматривать эффективность мероприятий ИБ в сегодняшнем цифровом мире смартфонов и повсеместного Internet неправильно.

Таким образом, проект ИБ в промышленном сегменте — это наведение порядка. Хотя не следует под зонтик ИБ тянуть вообще все системы. Как минимум, уже заявляемые связки с ТОиР и корпоративными бизнес-процессами на даже очень продвинутых промышленных предприятиях РФ, даже в начале 2020 г — это перебор.

При этом на горизонте уже засвечиваются новые проблемы. Например, из-за осложнения с 2014 г. общеполитической ситуации некоторые руководители подразделений ИБ крупных предприятий очень правильно озаботились вопросом контроля процессов гарантий-

ной и сервисной поддержки основного технологического оборудования. Мало того, что собственно первые линии поддержки находятся в неизвестных географических точках, но и само обращение (заведенный «тикет») может обрабатываться и Бразилии, Индии или на Гонолулу (страны названы из реальных кейсов).

Приведем несколько реальных примеров:

— одна крупная российская компания была очень «взбудоражена», когда сотрудники департамента ИБ обнаружили и доложили руководству, что сеансы удаленного доступа к системе управления технологическим оборудованием основного производства ведутся не из сети производителя в Германии (как должно было быть по сервисному контракту), а с адреса IP сети Internet-кафе в дальнем областном центре России;

— не единичный, но в данном случае конкретный пример: полная остановка на несколько дней систем с группой компьютеров, подцепивших вирус-шифровальщик. Производственные процессы были переведены на ручное управление, по агрегатам назначили внеплановое профилактическое обслуживание. С проблемами после безуспешных попыток борьбы справились только полными переустановками систем, что потребовало, в том числе и привлечения иностранных специалистов производителя (соответствующие счета на оплату услуг были выставлены);

— на пограничных сетевых устройствах одного российского завода постоянно присутствует активность с IP-адресов из региона Юго-Восточной Азии. Ситуация не может быть как-то разрешена полностью, так как места источников меняются. Адекватным ответом ИБ службы на данный момент является только укрепление периметров и сокращение возможных поверхностей атак;

— инцидент в крупной энергетической компании: отключение технологического оборудования принудительно через средства удаленного доступа;

— несколько блэкаутов в 2019 г., в том числе Венесуэла — просто отключили свет.

Перечни хакерских атак опубликованы в аналитических материалах специализированных российских и зарубежных компаний. Хакеров стало еще больше. Но интереснее другое — появился новый тренд: хакеры в 2018–2019 гг. обратили свое внимание на промышленные компании. Среди причин этого можно назвать развитие технологий промышленного Internet вещей. Стоимость взлома промышленного предприятия ниже, чем, например, банка. Сама атака безопаснее. И если дойти до подмены транзакций, то можно затеряться в субподрядных юридических лицах (особенно, если это строительство крупных промышленных объектов), и направить часть денежных средств в свой адрес. При этом злоумышленники «ломают» не управляющую компанию, которая, как правило, защищена и технологически, и организационно, а какую-нибудь IP-камеру на заводе или стройплощадке, что повышает вероятность не быть пойманными до 99%. Вот такие новые метаморфозы киберпреступлений.

Цифровое предприятие — это автоматизированное и роботизированное предприятие, где большинство процессов выполняются без участия человека. Таких производственных участков уже и сейчас много почти на каждом успешном предприятии. Например, на территории завода на современном автомобилестроительном или пивоваренном предприятии люди присутствуют только в зоне разгрузки/погрузки. На современном промышленном производстве специалисты также находятся вблизи оборудования и контролируют процесс либо в операторских. Важный нюанс: на предприятиях используются производственные линии иностранного производства. И дальше возникают все те проблемы ИБ, о которых говорилось выше.

С другой стороны, в России есть предприятия, где ручной труд очень мало автоматизирован, например, это характерно для литейного производства, механосборочных цехов и т. д.

Но и те, и другие предприятия имеют свои угрозы ИБ, которые значительно отличаются и по масштабам возможного ущерба, и по компенсирующим мероприятиям.

Рычков Дмитрий Валентинович *– директор Центра промышленной безопасности АО НИП «Информзащита».*
Контактный телефон +7(495) 980-23-45.
Http://www.infosec.ru

Разработка технологического процесса проверки кабельных жгутов

Компании Electro Magnetic Applications, Inc. (EMA) и Ansys (NASDAQ: ANSS) объединяются, чтобы предоставить усовершенствованный рабочий процесс для сертифицированных моделей кабельных жгутов и сборок в самолетах и автомобилях. Он существенно снизит риски электромагнитных помех для кабельных жгутов, сократит время на разработку, ускорит сертификацию и поможет продвигать новые продукты на рынок быстрее, чем когда-либо.

Кабельные жгуты, передающие электроэнергию и сигналы электронике в самолетах и автомобилях, должны быть защищены от внешних источников электромагнитных помех, таких как электромагнитные поля высокой интенсивности (HIRF) и удары молнии. Для защиты транспортных средств от электромагнитных помех на физических прототипах нужно проводить длительные и дорогостоящие сертификационные испытания электромагнитной совместимости (ЭМС).

Новый рабочий процесс EMA и Ansys Ansys EMA3D Cable является надежным платформенным решением для анализа параметров электромагнитной совместимости кабельных линий. Использование EMA3D Cable на ранней стадии проектирования позволяет повысить точность прогнозов производительности изделий инженеров, сократить стоимость разработки и необходимость физического прототипирования, а также использовать результаты испытаний в качестве основы для финального согласования и сертификации.

Http://www.ansys.com https://www.cadfem-cis.ru