уровня уверенности высшего руководства заказчика в обеспечении заданного уровня ИБ на всех объектах.

Список литературы

1. *Лившиц И.И.* Методика оптимизации программы аудита интегрированных систем менеджмента // Труды СПИИРАН. 2016. № 5. С. 52 - 68. DOI 10.15622/sp.48.3.
2. *Соколов Б.В., Юсупов Р.М.* Неокибернетика в современной структуре системных знаний // Робототехника и техническая кибернетика, 2014, вып. 3, стр. 3 -11.
3. *Юсупов Р. М., Шишкин В. М.* О некоторых противоречиях в решении проблем информационной безопасности//Труды СПИИРАН. Вып. 6. - СПб.: Наука, 2008. С. 39-59.
4. *Andrew Jaquith.* Security Metrics: Replacing Fear, Uncertainty, and Doubt 1st Edition. Addison-Wwsley, 2007, ISBN 0785342349986.
5. *Bohme R. and S. Koble.* On the Viability of Privacy-Enhancing Technologies in a Self-regulated Businessto-Consumer Market: Will Privacy Remain a Luxury Good?, Proc. Workshop on Economics of Information Security (WEIS 07), 2007.
6. *Livshitz I. I., Yurkin D.V., Minyaev A.A.* Formation of the Instantaneous Information Security Audit Concept. Distributed Computer and Communication Networks. V. 678 of the series Communications in Computer and Information Science pp 314-324, DOI 10.1007/978-3-319-51917-3_28, ISBN: 978-3-319-51916-6.

***Лившиц Илья Иосифович** – канд. техн. наук, доцент кафедры БИТ Университет ИТМО,*
***Неклюдов Андрей Валерьевич** – ведущий инженер ООО «Газинформсервис».*
Контактный телефон +7 921 934-48-46.
E-mail: Livshitz.il@yandex.ru nav7ad@mail.ru

Кибербезопасность АСУТП: взвешенный подход

А.В. Корнев (Компания Group-IB)

Кибербезопасность сегодня — один из ключевых процессов любой компании. Промышленные предприятия, содержащие в своей инфраструктуре системы автоматизации производства, не только не являются исключением из этого правила, но и должны задавать тренды в деле защиты информации. Одним из подтверждений этому является то внимание регуляторов в сфере информационной безопасности (ИБ), которое уделяется как ключевым системам информационной инфраструктуры в формате требований, так и широкому кругу производств, не включенных в соответствующие перечни в виде рекомендаций. В настоящей статье мы обсудим важность не только соблюдения требований отраслевых стандартов ИБ, но и проактивных действий по оценке и усилению защищенности промышленных объектов от киберугроз.

Ключевые слова: кибербезопасность, ключевые системы информационной инфраструктуры, информационная безопасность, киберугрозы.

Кибербезопасность — больше чем «модный» тренд

Согласно статистике, собранной с помощью сервиса Intelligence компании Group-IB (http://www.group-ib.ru/intelligence.html), в 2016 г. более 700 различных российских ресурсов были атакованы хакерами. Жертвами успешных атак стали не только банки, но и предприятия строительной сферы, заводы и государственные предприятия. Причем, учитывая цели атак на промышленные системы (скрытное внедрение и закрепление на атакованных системах для получения информации об особенностях производства и при возможности оставление средств удаленного управления для будущих воздействий), атаки на производства, как правило, остаются незамеченными в отличие от воздействий на компании финансовой сферы, где целью злоумышленников является быстрое обогащение.

Мы прогнозируем, что в текущем и последующем годах число атак на АСУТП будет только расти, и связывается это в первую очередь с ростом числа доступных из сети Internet систем SCADA (зачастую не защищенных должным образом) как общее следствие автоматизации и информатизации промышленности.

Отметим, что предприятия начали гораздо серьезнее подходить к вопросам информационной безопасности (ИБ), ведь стимулом этого процесса выступает государственное регулирование: нормативная база обязательных требований по ИБ постоянно расширяется и дополняется, что вполне очевидно и закономерно: современные АСУТП управляют сложнейшими и опасными технологическими процессами, где даже единичный сбой может привести к авариям, техногенным катастрофам, причинению вреда жизни и здоровью персонала, экологическим бедствиям, не говоря уже о прямом финансовом или репутационном ущербе предприятию, отрасли и государству в целом. На фоне напряженности во внешнеполитических вопросах и общемирового курса на усиление кибервойск как оборонительного, так и наступательного характера позиция государства более чем понятна.

Кибербезопасность в своем современном выражении является свойством информационных систем обеспечивать свою работоспособность и эффективность в решении наложенных на них функциональных задач [1,2]. Применительно к АСУТП, это характеристика всей информационно-технологической инфраструктуры, определяющая способность обеспечивать свою целостность, стабильность и непрерывность работы. То есть это не отдельно взятое требование к одной или группе систем иметь «определенную» конфигурацию, которая трактуется как «безопасность», а наоборот —

обширный и регулярно пополняемый комплекс мер, призванный обеспечить безотказность, безостановочность и корректность технологического процесса всесторонне: начиная от требований к безопасности аппаратной составляющей и конфигураций программных средств, заканчивая регламентными политиками для персонала по работе и обслуживанию систем.

Сегодня прослеживаются довольно положительные тенденции в подходе к вопросу ИБ АСУТП: пропадает былой консерватизм во взглядах на саму конфигурацию систем (принцип «лишь бы все работало»); сами компоненты АСУТП активно совершенствуются производителями не только в плане функциональных возможностей, но и в аспектах ИБ; сформирован и развивается рынок готовых специализированных решений и услуг по обеспечению безопасности сегментов АСУ и отдельных устройств. Но, к сожалению, не все инфраструктуры даже сейчас готовы продемонстрировать высокий уровень защищенности как корпоративного, так и промышленного сетевого периметра.

С чего начинается кибербезопасность в целом, как она интегрируется с АСУТП — на все эти вопросы постараемся дать ответы с практической (как наиболее эффективной на наш взгляд) точки зрения.

С чего начинать?

С детального изучения стандартов и анализа текущего состояния ИТ-инфраструктуры. Большинство уязвимостей инфраструктур промышленных объектов обусловлено тем, что при проектировании и эксплуатации нарушается то или иное предписание стандарта по обеспечению безопасности АСУТП. В первую очередь это касается приказа ФСТЭК № 31, который тесно перекликается с зарубежным аналогом NIST-800-82. Сюда также следует относить семейство IEC 62443 как новое направление универсального международного стандарта.

Другая сторона ИБ АСУТП начинается с формирования модели угроз, которая должна полностью отражать все потенциальные и наиболее реальные риски. Важно понимать, от чего и от кого следует защищать свою инфраструктуру. Модель угроз должна предполагать и описывать способы воздействий, которые приведут к нарушению функционирования систем или их компрометации. Только после анализа всех рисков следует предпринимать целенаправленные активные действия.

Важно прямо и однозначно ответить на вопрос: «Кто является актуальным для предприятия злоумышленником?». Это может быть конкурент в рамках отрасли, привлекающий в качестве атакующих единиц сторонних киберпреступников, сотрудников-инсайдеров или подрядчика, имеющего легальный доступ на территорию предприятия или в его сетевую инфраструктуру, или кибеpармия государства-конкурента, получившая приказ подготовить удар по ключевой инфраструктуре на случай возможного конфликта. Также нельзя исключать халатность со стороны сотрудников и потенциальный вред вследствие увольнений.

Для более детального изложения рисков необходимо иметь на руках подробную и актуальную карту всей локальной сети, используемого на хостах ПО, участников работы сети, их привилегий и доступов, а также описание особенностей архитектуры самих систем для грамотного планирования возможных сценариев развития атак.

Уровни безопасности АСУТП

Безопасность АСУТП вытекает из ее общей архитектуры, которая представляется в форме небезызвестной пирамиды отдельных инфраструктур и взаимодействий внутри нее и с внешними объектами. Информационная безопасность в своих мероприятиях и требованиях выстраивается в схожем порядке, дополняя собой вышеуказанную архитектуру, но со своим специальным делением по уровням. Перечислим основные из них:

- уровень полевых устройств — здесь рассматривается безопасность функционирования среды низкоуровневого оборудования: в модель угроз вписываются вероятные способы воздействия на полевые устройства таким образом, чтобы они вышли из строя, вызвав, например, аварийный останов в результате передачи им некорректных команд, параметров или инструкций по оперированию в той или иной ситуации;
- уровень физической безопасности, который предполагает любые возможные ограничения физического доступа к полевым устройствам и управляющим системам, помещениям, интерфейсам и любым другим отдельным компонентам, а иногда и вплоть до самой информации, относящейся к данной инфраструктуре;
- уровень безопасности отдельно взятых программно-аппаратных средств: настройки ОС и системного ПО, служб распределения доступов для отдельного хоста, настройка средств мониторинга состояния хоста и его взаимодействий и др. Сюда включаются не только технические меры, но и регламентная техника безопасности обращения персонала с рабочими станциями;
- уровень безопасности серверных станций (куда включаются также базы данных, Web-сервисы, отдельные OPC и др.) рассматривается как уровень более ужесточенных политик по сравнению с простыми хостами, расширяемых безопасной практикой администрирования;
- уровень безопасности приложений — это контроль целостности самого ПО (сюда относятся SCADA и HMI, ERP и MES, то есть любое ПО независимо от площадки применения), механизмы используемых средств авторизации пользователей, журналирования событий, распределения прав доступа учетных записей и др.;
- уровень сетевой безопасности подразумевает соблюдение правил сегментации и настройки сетевого оборудования, решает задачи взаимодействия сетей

АСУ и других сетей внутри инфраструктуры, обеспечивает безопасность процессов передачи данных, распознает потенциальные угрозы и т. д.;

• уровень мониторинга — отдельная независимая среда, которая призвана детектировать и локализовывать возможные инциденты ИБ, аномалии и потенциальные угрозы;

• административный уровень — нормативные документы, которые регламентируют процесс работы персонала с системами, что рассматривать исключительно с технической точки зрения недопустимо.

Такое деление не случайно — оно систематизирует весь перечень планируемых мероприятий и помогает оценить общий ход их выполнения на каждом этапе и в любом направлении. Рассмотрим основные принципы обеспечения безопасности АСУТП на каждом из уровней подробнее.

Среда полевых устройств — это среда низкоуровневых устройств, таких как датчики температуры или давления, контроллеры включения/выключения двигателей, насосов, генераторов, клапанов и др. Как правило, это ПЛК или распределенные системы с одним или несколькими управляющими микропроцессорами, где взаимодействие строится на таких протоколах, как HART, WHART, Modbus, Modbus TCP, Profibus и т. д. Важно контролировать, что доступа к данной среде нет ни у кого, кроме непосредственных операторов рабочих станций, которые отдают команды данным устройствам или следят за их состоянием, а также инженеров, занимающихся их подключением, настройкой и конфигурированием. Очевидно, что здесь недопустима ситуация, когда к SCADA-системе или ее драйверам для общения с полевыми устройствами имел бы доступ ERP-модуль из корпоративного сегмента сети, или чтобы MES имела возможность отправки команд на SCADA наравне с операторами. Необходимо постоянно отслеживать, что среда полевых устройств изолирована сама по себе и общается только с операторами или инженерами через управляющие интерфейсы, без любых возможных воздействий извне, — это важно. Не менее важно регулярно подвергать сомнению текущее распределение доступов и проводить инвентаризацию и пересмотр прав.

Отдельно выделим другой немаловажный момент, который тяжело отнести к тому или иному уровню: большинству предприятий страшен не столько сам факт угрозы хакерских атак или вредоносного ПО, сколько риск нестабильности новых прошивок для низкоуровневых устройств, установка которых зачастую действительно необходима и неизбежна. «Сырой» продукт может привести к любым неблагоприятным последствиям, если в нем содержатся ошибки конфигурации или может проявиться несовместимость с аппаратной составляющей. В данном случае специалистами АСУТП должны приниматься все необходимые меры для безопасного тестового запуска нового ПО на стенде, чтобы предусмотреть все возможные последствия установки новых патчей. Информационная безопасность должна содействовать данному процессу и отслеживать, чтобы новые прошивки не создавали аномалий на уровне работы локальной сети сегмента АСУ, а интерфейсы управления не конфликтовали с ПО и не создавали дополнительных угроз.

Уровень физической безопасности отдельно взятого хоста в сегменте АСУ должен формировать отказоустойчивое и корректно изолированное окружение, для которого внешнее воздействие исключено либо сведено к возможному минимуму (при условии компенсирующих мер, принимаемых на других уровнях). Рабочие станции непосредственных операторов, к которым подключаются напрямую полевые устройства, должны быть максимально закрытыми — системные блоки рекомендуется заключать в контейнеры под замок, кабели при необходимости защищать от механических воздействий или скрывать.

На аппаратном уровне следует запретить весь доступ к неиспользуемым физическим портам, в частности USB. Загрузка рабочей станции должна быть разрешена только с основного жесткого диска, а на BIOS следует устанавливать пароли. Для обновления или переконфигурации инженер временно получает доступ на подключение зарегистрированного и предварительно проверенного внешнего накопителя, о чем производятся записи в журналах доступа.

Поднимемся еще выше — до уровня программно-аппаратной безопасности хоста. Сюда ко всему уже вышесказанному добавляется безопасное конфигурирование ОС, настройка прав доступа, прав взаимодействия с самой системой и используемое специальное программное обеспечение. Здесь важно соблюдать принцип white-listing — проще определиться с тем, что нужно, а все остальное — отключить. Операторам рабочих станций, как правило, не нужны пакет офисных приложений, командная строка, средства работы с электронной почтой, многочисленные браузеры, учетная запись с правами локального администратора, доступы к настройкам оборудования, реестра или самой ОС. Если хостов много, то проблема решается созданием отдельного дистрибутива ОС с отключенными сторонними службами и программами. Конфигурации самой ОС и ПО — самые базовые и типовые можно устанавливать с помощью заранее подготовленного скрипта (шаблоны CIS).

Требования к безопасности серверных станций практически полностью сохраняются такими же, как и для всех остальных хостов обычных операторов, хотя функциональные возможности серверов гораздо шире. В рамках обеспечения ИБ серверная станция — это не только опосредующее работу операторов звено, но и центр наблюдения за всем выделенным сегментом инфраструктуры АСУ. Базы данных и другие хранилища на серверах должны быть защищены от несанкционированного редактирования или просмотра, все легитимные операции, способные повлиять на защищенность объекта автоматизации, долж-

Тот, кто видит со стороны, смотрит восемью глазами.
Цунэтомо Ямамото

ны журналироваться. Серверные компоненты SCADA недопустимо включать в корпоративный, даже отделенный программно сегмент корпоративной сети, так как формируется определенный риск удаленного воздействия. Серверные станции OPC/DDE рекомендуется дублировать для их взаимной заменяемости друг с другом на случай сбоев или неполадок в работе. Это характерно для OPC любого уровня: как тех, что общаются с полевыми устройствами, так и тех, что могут работать на уровне всего цеха. Клиент-серверное взаимодействие чаще всего строится на основе классических протоколов и технологий обмена данными и является одним из основных предметов ИБ. На каждом сервере должен поддерживаться как минимум один инструмент журналирования всех событий, чтобы в случае инцидента было проще выявить его своевременно, остановить развитие инцидента и после устранения возможных причин восстановить хронологию произошедшего. В нашем понимании, серверная станция — это не пылящийся годами ящик, который должен «просто работать», а инструмент для совместной работы инженеров и специалистов ИБ.

Безопасность уровня приложений несколько выходит за рамки сегмента АСУ и представляет комплекс мер по сохранению работоспособности и целостности всех программных средств. Сюда относятся различные DLC, парольные менеджеры, антивирусные средства, инструменты восстановления критически важных систем, призванные обеспечивать безотказность производственных процессов при любых обстоятельствах. Информационная безопасность на данном уровне призвана изучать сам программный продукт и его исходный код (что далеко не всегда возможно, но не упомянуть об этом нельзя), чтобы приложения не обладали свойствами аномального недекларированного поведения и не содержали излишней доступной функциональности. Тут же рассматриваются разграничения доступа и соблюдение сохранности учетных записей пользователей; ведение строгой парольной политики; безопасная настройка интерфейсов управления, исключающая любые возможные подключения из недоверенной среды; отслеживание анонсов обновлений и их своевременная установка.

На сетевом уровне работают «классические» принципы ИБ, которые на сегменте АСУТП необходимо соблюдать и интегрировать, допуская компромиссы только в исключительных случаях и закрывая возникающие риски на других уровнях. Здесь коснемся лишь тех моментов, которые так или иначе затрагивают безопасность АСУТП. Наиболее эффективным решением является выделение всей инфраструктуры АСУ в отдельный сегмент, у которого отсутствует полностью связь с офисными сетями: воздушный зазор невозможно реализовать гарантированно при фактическом подключении разных сегментов к одному маршрутизирующему устройству). В то же время бизнес не может находиться в отрыве от производства, это очевидный факт — эффективное планирование, прогнозирование и анализ зависят от информации с производственных цехов, которая должна быть предоставлена максимально оперативно. В связи с этим обратимся к имитации гальванической развязки сегментов с помощью шлюзов/диодов, которые обеспечивают однонаправленную передачу информации из сети АСУ на корпоративные рабочие станции, не позволяя обратный обмен. При корректном тестировании подобных систем до закупки, во время внедрения и после ввода в эксплуатацию информационные потоки невозможно развернуть в опасном направлении. Возникает некоторая свобода самовыражения: транслируемый от сегмента АСУ трафик можно шифровать при отправке и обратно интерпретировать после получения мониторинговыми и аналитическими системами так, чтобы сделать невозможной эффективную прослушку канала связи. Готовые решения такого рода уже существуют и могут помочь предприятиям, для которых классическая гальваническая развязка сетей невозможна. Один из немногих минусов подобных решений достаточно очевиден: интеграция такого решения с учетом всех стендовых проверок занимает достаточно много времени.

Не всегда управление процессами в АСУТП строится, исходя из требования физического присутствия персонала за рабочей станцией (в некоторых случаях это просто невозможно) — и зачастую требуются удаленный доступ и управление, который одновременно должен быть сам по себе безопасен. В этом случае необходимо отслеживать, чтобы интерфейсы SCADA не были доступны напрямую: между отправителем и получателем трафика всегда должно присутствовать промежуточное звено, которое:

- реагирует только на один или несколько разрешенных IP-адресов из доверенной сети;
- расшифровывает трафик перед отправкой команд на целевой интерфейс (если применимо);
- входит в группу устройств постоянного мониторинга состояния;
- обладает функциональной простотой;
- умеет реагировать на критические инциденты в автономном режиме.

Аутентификация в данном случае должна являться требованием, а не «рекомендацией». Допустимы и рекомендованы методы сокрытия и вышеупомянутых промежуточных интерфейсов, например, так называемый port knocking.

В случае распределенной системы управления производством правило изоляции сегмента АСУ сохраняется, а средства удаленного доступа размещаются внутри него с использованием современных технологий туннелирования. Для этого можно выделить несколько рабочих станций вне сегментов АСУ и офиса или внутри только сегмента АСУ, которые размещены за корректно настроенным межсетевым экраном и контролируют работу удаленных объектов. Следует убедиться, что даже у привилегированных пользователей корпоративного сегмента нет доступа к удаленным сетям АСУ. Также необходимо проверить, что сам канал передачи данных безопасен и проходит через наименьшее число промежуточных сетевых каналов. Главные задачи — обеспечить надежный канал поверх трафика с «полезной нагрузкой АСУТП», защитить удаленный интерфейс надежными механизмами аутентификации и настроить системы мониторинга событий. В этом отношении служба ИБ не вмешивается в технологические процессы и их администрирование, а обеспечивает безопасность доступа и управления.

Среда мониторинга — это совокупность специальных средств, которые аккумулируют любую информацию, касающуюся угроз безопасности, в том числе и по отношению к инфраструктурам АСУ. Сюда включаются уже упомянутые средства антивирусной защиты, межсетевые экраны, системы мониторинга состояния компонентов всех вышеперечисленных уровней. Важно отметить, что сами инциденты различного характера необходимо максимально подробно журналировать и впоследствии анализировать, формируя собственную практику проактивной работы с угрозами.

Рынок готовых продуктов и специализированных решений

Тем временем рынок готовых решений для обеспечения безопасности АСУТП бурно развивается в своей продуктовой составляющей. Мы наблюдаем, как процессы устранения уязвимостей в прошивках ПЛК и полевые устройства выходят на новые уровни своего развития, адаптируя все больше новых технологий, в том числе призванных увеличить защищенность таких устройств «из коробки», видим, как расширяется законодательная база в части требований государства к ИБ и какое влияние она оказывает на специфику и конфигурацию продуктов, как вендоры ИБ выпускают свои собственные решения для обеспечения безопасности сегментов АСУ (ОС, брандмауэры, песочницы и т. д.), наконец, как совершенствуется сфера услуг аудита ИБ в применении к АСУТП и SCADA.

Потребность в ИБ промышленных систем существовала всегда, однако до недавних пор мероприятия по увеличению защищенности этих систем по объективным причинам заключались в соблюдении режима ограничения физического доступа на объекты автоматизации и противодействии иностранным техническим разведкам, использовавшим визуальное наблюдение и вербовку сотрудников. Сейчас же в арсенале потенциальных злоумышленников имеется значительно более широкий спектр удаленных дестабилизирующих воздействий на промышленные системы, в связи с чем несколько снизился порог квалификации злоумышленников, необходимый для проникновения в защищаемый периметр и увеличилось число потенциальных атакующих. Нельзя не упомянуть в очередной раз о Stuxnet, ставшем показательным примером вывода из строя ключевых систем иранской ядерной программы, и вызвавшем первый серьезный толчок к переосмыслению подходов безопасности АСУТП, который продолжается и сегодня. Да, «Стакснет» во многом похож на «пугало», помогающее вендорам продавать свои продукты. Да, в рамках атаки помимо создания собственно вредоносного кода использовалось огромное число менее технологичных воздействий, включающих внедрение и вербовку. Однако развитие угроз объектам автоматизации критически важных производств показывает, что атаки также автоматизируются опережающими темпами, например, более свежие и менее известные вредоносы семейства Turla уже умели преодолевать пресловутый воздушный зазор без ведома «переносчика». Тенденция к автоматизации атак на АСУТП определенно продолжится, и это определяет необходимость постоянного пересмотра методологии защиты с поправкой на прогресс как в части функциональности АСУ, так и в части возможностей атакующего.

Вероятно, специалист по ИБ АСУ уже задается вопросами, близкими к риторическим. Следует ли скупать все, что предлагает рынок продуктов и услуг в сфере ИБ АСУТП? Оправдан ли маркетинг, который навязывает все новые и новые решения? Во что обойдется их интеграция и будет ли она целесообразна?

Попробуем прояснить ситуацию, начиная с вопроса целесообразности: если в корпоративном периметре сети находится хост с необновленной, устаревшей и уязвимой ОС, то это не повод для закупки средств анализа трафика АСУ. Это элементарное нарушение стандартов, правил сегментации сетей и преступление против здравого смысла. Формулировать задачу кибербезопаности современных промышленных систем как защиту заведомо уязвимых, неправильно развернутых или некорректно настроенных систем закупками универсальных решений, которые сами по себе могут требовать конфигурирования и внедрения как минимум нерационально. Правильнее сначала обеспечить безопасность инфраструктуры АСУ на каждом из ее уровней, выделенных ранее, соблюдая требования стандартов, обозначив и сократив тем самым потенциальные «точки входа» в сегмент АСУТП и проанализировав возможные угрозы и риски. И только после этого стоит задумываться над приобретением накладных средств обеспечения ИБ.

Как оценить текущий уровень защищенности?

Для фактической оценки состояния защищенности своей инфраструктуры можно прибегать к различным методам: формировать отдельный тестовый стенд, передающий всю функциональность, создавать устройство текущей архитектуры, на котором специалисты по ИБ будут пробовать различные векторы атак; проводить внутренний аудит своими силами в рамках отдельного проекта, что зачастую не всегда возможно; заказывать услугу аудита защищенности со стороны. Наша практика показывает, что независимый аудит ИБ выигрывает у многих альтернатив по следующим причинам:

- не все организации способны содержать у себя постояннодействующий отдел ИБ хотя бы в силу существенного бюджета на его содержание, превышающего, как правило, стоимость регулярных проверок сторонними организациями;
- работы по аудиту проводятся специалистами с подтвержденными компетенциями и опытом подобных проектов, что предсказуемо положительно сказывается на качестве;
- заказывая услуги по ИБ, компания исключает фактор «закрытых глаз»: специалисты, проводящие аудит, независимы и не состоят ни в каких личностных или любых иных взаимоотношениях с персоналом организации. Это позволяет добиваться максимальной объективности результатов, где недоработки в том или ином направлении не будут скрыты договоренностями, условностями или обещаниями;
- аудит включает разработку экспертных рекомендаций по устранению выявленных уязвимостей с учетом всей специфики и особенностей инфраструктуры: заказчик услуги не остается наедине со всеми проблемами безопасности, а имеет на руках готовое руководство к действию;
- наконец, аудит ИБ можно проводить параллельно с работами по стандартизации, что позволяет непротиворечиво усилить и актуализировать меры, сформулированные руководящими документами.

Стоит, однако, предостеречь и от другой крайности. Заказ услуг по анализу защищенности исключительно у сторонних организаций, излишнее доверие к результатам их работ и дистанцирование от вопросов киберзащиты также приводит к появлению слабых звеньев в системах киберзащиты. Мы абсолютно уверены и регулярно убеждаемся в том, что только дискуссия владельцев процесса автоматизации управления технологическими процессами и специалистов по ИБ способна привести к формированию по-настоящему комплексного и всестороннего подхода к защите от киберугроз АСУ.

Подводя итог

Кибербезопаность — это не статичная характеристика ИТ-инфраструктуры, а динамический комплекс регулярных мероприятий по обеспечению безопасности как каждой из отдельно взятых структур, так и всех возможных их совокупностей, который помимо выявления и устранения уязвимостей включает также постоянный мониторинг внутрисетевых активностей с целью предупреждения возможных атак и реагирования на возникшие угрозы как извне, так и изнутри.

При обеспечении безопасности АСУТП необходим комплексный подход, который включает регулярный аудит защищенности всей инфраструктуры. Это поможет выявить уязвимости, смоделировать, детализировать и проанализировать возможные риски и сформировать перечень угроз исследуемым объектам.

Угроза кибертерроризма становится все более реальной, и, когда цели киберпреступных групп изменятся со скрытного присутствия на объектах автоматизации критически важных технологических процессов на создание инцидентов, приводящих к техногенно-экологическим катастрофам и чрезвычайным ситуациям, реагировать будет уже поздно. Поэтому крайне важно уже сейчас выносить задачи обеспечения ИБ систем на первый план, наращивая компетенции в данном вопросе для создания наиболее эффективных решений для защиты АСУТП. Важно видеть в исполнении требований и рекомендаций руководящих документов не только путь к формальному подтверждению соответствия ожиданиям регуляторов, но и способ поднятия фактической защищенности. Чрезвычайно важно усиливать мероприятия, описанные в упомянутых документах, стендовыми испытаниями систем на устойчивость к актуальным воздействиям, еще не успевшим попасть в отраслевые модели угроз, и критически подходить к выводам внешних аудиторов, включаясь в работу по формированию как перечней угроз и злоумышленников, так и рекомендаций по усилению обороны от угроз, пришедших «по проводу».

Список литературы

1. *Белов В. С., Брызгин А. А.* Безопасность (и/или) АСУТП// Автоматизация в промышленности. 2015. № 2.
2. *Арефьев А.С.* Таргетированные атаки на промышленный сектор: новое оружие в кибервойне // Автоматизация в промышленности. 2015. №2.

***Корнев Александр Викторович** – специалист подразделения "Аудит и Консалтинг ИБ" компании Group-IB.*
Контактный телефон (495) 984-33-64.
E-mail: kornev@group-ib.com