Информационная безопасность современных АСУТП

Р.Ф. Зулькарнаев (Компания «Инфосистемы Джет»)

Рассмотрены проблемы информационной безопасности АСУТП, а также систем, использующих технологию Industrial Internet of Things. Сформирована концепция и предложен подход для обеспечения ИБ АСУТП на базе IIoT.

Ключевые слова: АСУТП, Industrial Internet of Things, информационная безопасность, функциональная безопасность.

Введение

Логически АСУТП можно представить в виде многоуровневой структуры (рис. 1): уровень операторского (диспетчерского) управления; уровень программируемых логических контроллеров (автоматического управления); уровень ввода/вывода данных, исполнительных устройств (полевой уровень).

Для развития и роста экономики Правительство РФ утвердило программу «Цифровая экономика РФ» Распоряжением № 1632-р от 28 июня 2017 г.

Цифровая экономика — это система экономических, социальных и культурных отношений, основанных на использовании цифровых информационно-коммуникационных технологий [1].

Одним из ключевых направлений в цифровой экономике является модернизация производственной отрасли в рамках Industry 4.0. Последняя подразумевает цифровизацию всех уровней автоматизации производства с использованием концепции IIoT (Industrial Internet of Things), которая предполагает активное использование виртуальных и облачных сред [2, 3]. Структурная схема АСУТП на базе IIoT [2] приведена на рис. 2.

Облачные технологии — это подход к размещению, предоставлению и потреблению приложений и компьютерных ресурсов, при котором приложения и ресурсы становятся доступны через Internet в виде сервисов, потребляемых на платформах устройствах [5]. Эта концепция вызывает множество вопросов, связанных с информационной безопасностью (ИБ).

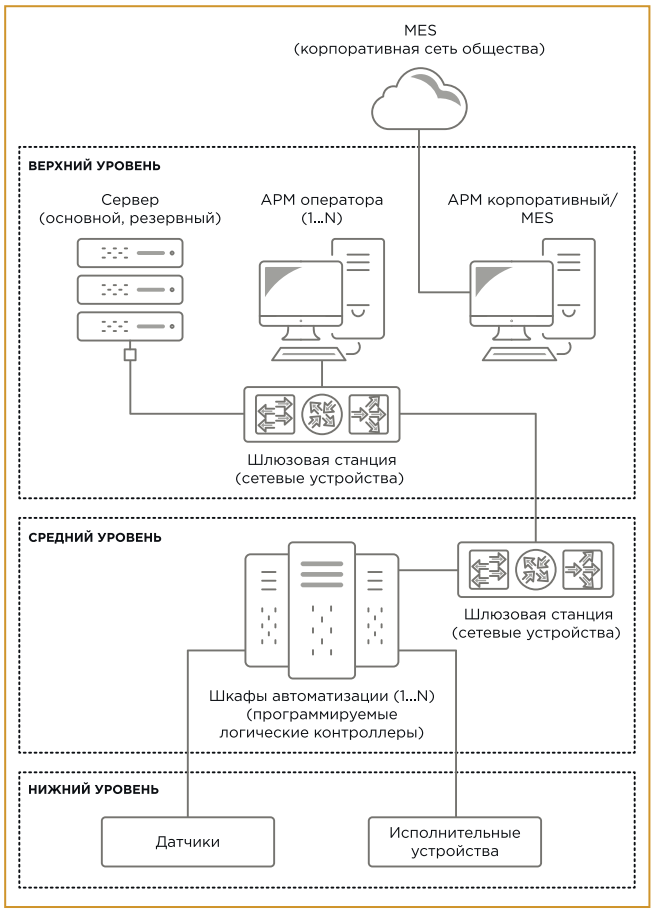

Рис. 1. Структурная схема АСУТП

Проблемы информационной безопасности в АСУТП

Многие владельцы АСУТП считают, что если их система является изолированной, то заниматься вопросами ИБ нет необходимости. Это мнение является ошибочным, так как любая система имеет уязвимые элементы и подвержена информационным атакам. Опыт автора, наработанный при проведении аудитов ИБ АСУТП отечественных предприятий, говорит о том, что многие технические средства не имеют встроенных функций защиты, а если они и есть, то, как правило, не настроены или настроены некорректно. В 95% случаев любая АСУТП имеет ряд проблем, связанных с ИБ: отсутствие настроенных политик на операционной системе (ОС), отсутствие настроек Access Control List (ACL, при технической возможности) и т. п. Также свои ограничения накладывают используемые технические средства. Например, некото-

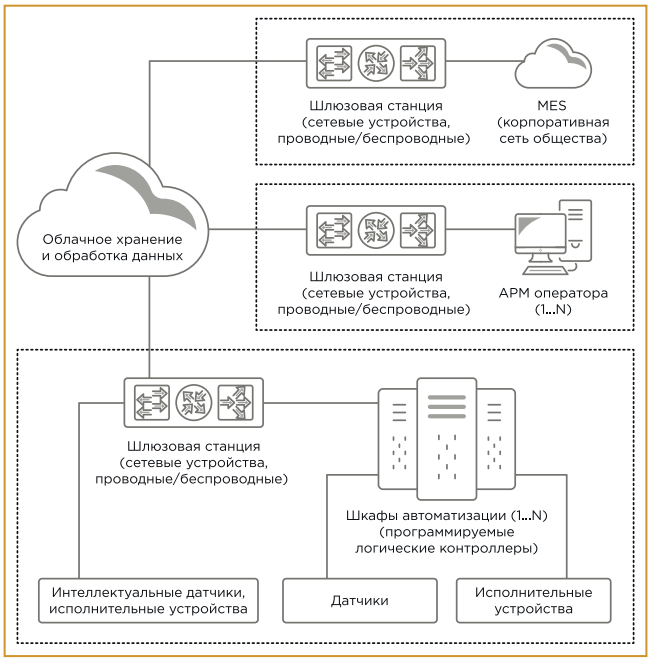

Рис. 2. Структурная схема АСУТП на базе IIoT

рые SCADA-системы не совместимы с антивирусными средствами. Использование групповых учетных записей на SCADA-системах обуславливается невозможностью создать индивидуальную учетную запись на каждого сотрудника в действующей системе и т. п.

Дополнительно существует большой пласт вопросов, связанных с обновлением компонентов АСУТП: проблемы совместимости, не выстроенные процессы внутри организации, возможные сложности при необходимости остановки технологического процесса, долгий цикл тестирования обновлений вендором, а также необходимость приобретать дорогостоящую подписку на данные обновления. В противном случае вендоры не всегда гарантируют корректную работу устройства или ПО при обновлении каких-либо элементов.

Каждое обновление — это долгий процесс, проходящий в несколько этапов: установка в зоне тестирования, тестирование и установка в действующую систему. Зачастую в функционирующих АСУТП обновления отсутствуют или устанавливаются сразу в работающую систему. Разработка зоны тестирования для АСУТП является сложной и дорогостоящей задачей, поскольку необходимо продублировать часть ее инфраструктуры. Во многих организациях не определены лица, ответственные за обновления компонентов АСУТП, то есть отсутствует понимание, кто должен заниматься этим процессом: подразделение ИБ или АСУТП.

Многие элементы действующих АСУТП устарели, а их ПО или ОС не поддерживается разработчиками или вендорами. Этот вопрос решается компенсирующими мерами защиты либо заключением дополнительных соглашений с разработчиками о дальнейшей поддержке устаревших решений. Также отметим, что многие владельцы АСУТП уделяют недостаточное внимание ИБ процессорной части, имеют недостаточный штат и уровень специалистов ИБ.

Для перехода на технологию IIoT вопросы подобного плана должны быть решены или сведены к минимуму. При этом сам по себе подход IIoT накладывает дополнительные риски, приводящие к новым векторам атак на систему. В работе [4] описаны возможные проблемы при переходе на новые технологии, а также угрозы ИБ, которые могут привести к значительным потерям.

При построении АСУТП с использованием IIoT возникают следующие дополнительные факторы:

– отсутствие периметра объекта;

– использование проприетарных протоколов;

– высокая гетерогенность средств и протоколов связи;

– отсутствие элементарных механизмов безопасности;

– автономность устройств;

– физическая незащищенность элементов.

В связи с новыми факторами для АСУТП на базе IIoT увеличивается число векторов атак и, как следствие, рисков и угроз ИБ.

Концепция защиты АСУТП на базе IIoT

Любое обеспечение ИБ начинает формироваться с разработки требований. В настоящее время требования для АСУТП описаны в ряде Приказов ФСТЭК России.

– № 31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

– № 239 от 25 декабря 2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

– № 235 от 25 декабря 2017 г. «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования».

Концептуальный подход к обеспечению защиты кардинальным образом не отличается от подхода для систем общего пользования. При этом существует ряд дополнительных факторов и ограничений, которые влияют на ее реализацию:

– должна обеспечиваться надежность основных и вспомогательных систем в рамках АСУТП;

– для АСУТП обеспечение ИБ направлено на повышение уровня функциональной безопасности (ФБ).

Второй фактор является следствием особенностей существующих активов АСУТП. По большому счету, требование к обеспечению защиты выполняемых функций системы идентично требованию защиты самого бизнес-процесса и могло бы гарантировать безопасность АСУТП. Как показывает практика, при расчете параметров функциональной безопасности сотрудниками компании зачастую не учитываются реализации угроз безопасности информации (УБИ). То есть учитываются только техногенные факторы и не учитываются злоумышленные антропогенные угрозы. При этом в случае реализации такой угрозы первоначальные расчеты надежности будут неверны. Очевидно, что распределение отказов и прочие исходные данные для оценки ФБ неизбежно изменяются при злонамеренных информационных воздействиях. Основной проблемой в этой части на данный момент является, как правило, неучастие специалистов ИБ при расчете ФБ.

Общий алгоритм построения системы защиты информации в соответствии с системным подходом может быть следующим:

1) определение защищаемых активов (элементов, процессов);

2) определение УБИ, прямо или косвенно воздействующих на защищаемые активы, с учетом мировых БД, например, National Vulnerability Database (NVD), Open Sourced Vulnerability Database (OSVB), Secunia Advisory and Vulnerability Database и российской БД ФСТЭК;

3) определение класса защищенности (Приказ ФСТЭК России № 31) или категории значимости (ФЗ № 187, ПП № 127);

4) определение мер защиты информации в соответствии законодательством РФ (Приказы ФСТЭК России № 31, 239, 235);

5) выборка мер и средств защиты от определенных УБИ в соответствии с классом защищенности или категорий значимости.

Специалистам в области ИБ, сетевым администраторам и производителям ПО (как системного и прикладного ПО, так и программных продуктов защиты информации), работающим в интересах российских организаций и компаний РФ с государственным участием, рекомендуется использовать базу данных ФСТЭК, как содержащую наиболее релевантную информацию по актуальным уязвимостям для компьютерных систем и программного обеспечения, применяемого именно в российских организациях [6].

Один из действующих подходов к обеспечению защиты информации заключается в формировании наиболее полного перечня актуальных УБИ, после чего в соответствие каждой угрозе и требованию законодательства РФ ставится мера защиты. Системность подхода при этом заключается не только в самом факте составления перечня, но и в разбиении угроз на классы и защите от групп угроз методами (в формировании связей «многие ко многим»). К СЗИ предъявляются требования полноты защиты (защиты от всех актуальных УБИ, выполнения требований законодательства РФ) и бизнес-требования, такие как низкая цена внедрения и поддержания, простота использования и т. д., напрямую связанные с отсутствием функциональной избыточности СЗИ. По этим причинам необходимо реализовывать комплексный подход к защите информации. В зарубежных стандартах данный подход называется «обеспечение комплексной “сквозной” безопасности».

Помимо использования приказов и постановлений РФ при разработке системы информационной безопасности (СИБ) рекомендуется использовать стандарты, разработанные различными международными организациями и институтами, такие как:

– Industrial Internet of Things: Security Framework (IISF);

– International Standards Organization (ISO);

– Institute of Electrical and Electronic Engineers (IEEE);

– International Electrotechnical Commission (IEC);

– Internet Engineering Task Force (IETF);

– National Institute for Standards and Technology (NIST).

Важно отметить, что для разработки СИБ законодательством не запрещается использовать зарубежные стандарты и лучшие практики, но разработанная СИБ должна соответствовать требованиям нормативных документов РФ (при их наличии), в частности для АСУТП, требованиям приказов № 31 (носит рекомендательный характер), № 239, № 235 (обязательный для критических информационных инфраструктур, имеющих категорию значимости) ФСТЭК России.

Подход к обеспечению ИБ IIoT

Стандарт IIFS (Industrial Internet Consortium: Industrial Internet of Things Volume G4: Security Framework) предлагает разрабатывать СИБ на основе многоуровневой структуры, при этом каждый уровень имеет функциональные блоки. На данный момент этот стандарт является наиболее зрелым в части концепции обеспечения безопасности IIoT.

Верхний уровень включает: защиту конечных вычислительных устройств; защиту связей и подключений; мониторинг и анализ безопасности; управление конфигурацией безопасности; защиту данных; политику и модель ИБ.

Стандарт IISF для разработки СИБ вводит понятие «конечное вычислительное устройство», подразумевающее любые устройства, имеющие вычислительные или коммуникационные функции. Это могут быть серверы, автоматизированные рабочие места, коммутаторы, программируемые логические контроллеры, интеллектуальные датчики, облачные серверы, пограничные устройства и т. п. Конечное вычислительное устройство может быть частью сети управления, концентратором или маршрутизатором сетевого трафика между другими конечными устройствами. Они могут находиться на выделенном или виртуализированном оборудовании. В России для данного спектра устройств введен свой термин — «комплекс технических средств».

Функции безопасности блоков могут быть реализованы с помощью встроенных функций безопасности устройства или наложенными средствами защиты информации, такими как межсетевые экраны, криптошлюзы, специализированные средства обнаружения вторжений и т. п.

Реализация ИБ зависит от вычислительных возможностей устройств. Разрабатываемая СИБ должна быть модульной и масштабируемой.

Также необходимо разрабатывать и поддерживать в актуальном состоянии модель зрелости ИБ, которая позволяет провести оценку на основе механизмов и процессов при проектировании, разработке, обслуживании и эксплуатации. Системный интегратор и владелец системы могут оценивать уровень зрелости ИБ, что позволит в будущем предоставлять информацию об ИБ вендорам и возможность определять динамику реализации и развития СИБ.

Конечное вычислительное устройство (комплекс технических средств)

Конечные вычислительные устройства охватывают весь спектр периферийных устройств IIoT.

Защита конечных вычислительных устройств включает следующие основные функции безопасности:

– обеспечение физической защиты;

– формирование корня доверия;
– идентификация устройств;
– защита целостности ОС, ПО и конфигураций;
– аутентификация на устройствах;
– контроль управления политиками безопасности и конфигурациями;
– мониторинг и анализ событий ИБ;
– защита данных при хранении и обработке на устройствах.

Конечные вычислительные устройства имеют потенциальные уязвимости, такие как:
– уязвимости в аппаратном обеспечении;
– перехват или переопределение процессов загрузки ОС, BIOS;
– некорректная настройка гостевой ОС, гипервизора;
– атака «отказ в обслуживании» на API и вычислительные устройства;
– уязвимости и ошибки в процессе конфигурации устройства;
– внедрение потенциального вредоносного кода;
– несанкционированный доступ к критически важным данным, нарушение целостности данных;
– нарушение целостности системы мониторинга, компрометация оборудования и ПО;
– нарушение контроля доступа в системе управления конфигурациями;
– неконтролируемые изменения в политике и модели безопасности;
– уязвимости в среде разработки.

Модель безопасности IIoT должна начинаться с обеспечения безопасности конечных устройств вендорами. После поставки оборудования вопросами ИБ должен заниматься интегратор технического решения совместно с производителями.

Для реализации функций безопасности на конечных устройствах необходимо использовать аппаратные модули защиты, модули доверенной загрузки, аппаратные чипы и контейнеры. Наиболее распространенным является использование шлюза безопасности, который обеспечивает безопасность устройств, находящихся за ним. Такие шлюзы осуществляют защиту на уровне сети и являются первым шагом к обеспечению ИБ системы. Позже могут быть добавлены элементы безопасности на уровне устройства, такие как контроль целостности во время выполнения и другие средства защиты.

Все конечные устройства должны быть физически защищены путем ограничения доступа к ним, например, с помощью замков, биометрических и RFID-карт, а также с использованием систем видеорегистрации. Некоторые датчики могут находиться за периметрами физической защиты, в таком случае необходимо использовать физические ограждения, которые позволят зафиксировать факт взлома. Корпус устройства должен обеспечивать стабильные условия работы и температуру, защиту от пыли и других веществ окружающей среды, способных оказать негативное воздействие. Физический доступ к внешним интерфейсам (USB, CD-ROM, DVD-ROM) должен контролироваться. Устройства могут иметь встроенные функции безопасности, все конечные устройства должны иметь уникальный идентификационный номер.

Корень доверия должен быть реализован на аппаратном уровне устройства. Конечное устройство может иметь один или несколько идентификаторов (учетных данных), используемых для разных приложений. Может быть несколько уровней доверия, применяемых к устройству. Каждый уровень доверия определяет минимальные возможные полномочия учетных данных. Цифровые сертификаты, RFID, пароли, биометрические и QR-коды являются примерами учетных данных, но сильно различаются по уровню доверия. IP-адрес, MAC-адрес и QR-код — это уникальные, но при этом ненадежные учетные данные, поскольку их целостность может быть нарушена, например, при атаках ARP-spoofing, когда устройство злоумышленника выдает себя за другое конечное устройство. Криптографический сертификат является уникальным (с соответствующей случайностью) и надежным (в зависимости от типа и длины ключа). Но если закрытый ключ, связанный с сертификатом, не хранится и не обрабатывается в защищенном хранилище, сертификат все равно может быть скомпрометирован. Существует несколько стандартов, которые обеспечивают руководство по выбору правильного уровня защиты для идентификатора конечных устройств: ISO/IEC 29115, IEC 62443 и ISO/IEC 24760-1.1. Требования безопасности позволяют владельцам системы оценить уровень доверия, необходимый для защиты учетных данных.

На всех конечных устройствах должна быть реализована функция аутентификации. При аутентификации необходимо проверять уровень доверия пользователя и актуальность учетных записей, поскольку они могут быть приостановлены. Учетные записи должны храниться на защищенном сервере. Для передачи информации при аутентификации рекомендуется использовать безопасные протоколы аутентификации, например, Kerberos. Для критических элементов системы возможно рассматривать многофакторную аутентификацию.

Необходимо устанавливать доверие к среде, то есть осуществлять защиту целостности при загрузке ОС и впоследствии при запуске ПО на устройстве. Также должен быть сформирован Black List или White List ПО. Исполняемым файлам рекомендуется иметь хеши, и если хеш не соответствует сохраненному, то выполнение такого файла блокируется с созданием инцидента ИБ. Поэтому все изменения необходимо строго контролировать и регистрировать.

В качестве защиты конечных устройств и ограничения между пользователями можно использовать изоляцию, то есть ограничения взаимодействия компонентов. Изоляция может быть различной: процессорная, с использованием контейнеров, виртуальная, физическая.

Защита связи и подключений

Защита связи и подключений подразумевает идентификацию устройств между собой, защиту передаваемой информации и включает следующие основные функции безопасности:

– физическая безопасность проводных каналов связей;
– логическая защита конечных точек связи;
– защита данных при передаче;
– защита информационных потоков, то есть гарантия доставки информации;
– доверенное управление компонентами сети;
– мониторинг и анализ событий ИБ;
– контроль конфигурации и целостности сети.

Для защиты и обеспечения целостности данных при их передаче используются криптографические методы защиты. Требуемый уровень защиты зависит от информации, передаваемой по каналам связи. Ее источниками могут быть датчики, телеметрия, команды управления, сигналы тревоги, события безопасности, журналы безопасности, изменения состояния или обновления конфигурации. Необходимый уровень защиты должен описываться в политике безопасности и устанавливается владельцем системы.

Первоначально между элементами сети необходимо установить безопасное соединение и только затем передавать необходимую информацию. Протоколы связи, которые не обеспечивают целостность и конфиденциальность обмениваемых сообщений, должны быть направлены через зашифрованные и аутентифицированные туннели.

В качестве обеспечения безопасности на периметре сети должны использоваться средства защиты, такие как межсетевой экран, система обнаружения вторжений и т. п. На сетевых устройствах должен быть настроен ACL.

Стандарты промышленной безопасности, такие как ISA/IEC 62443-1-1, ISA/IEC 62443-3-3, ANSSI, NIST 800-82 и другие, рекомендуют разделять сети на сегменты. Они также рекомендуют назначать каждому сегменту сети уровень доверия и защищать связь и подключения через периметры сетей, особенно если взаимодействие между сегментами происходит на разных уровнях доверия. В качестве фильтрации для контроля информации между сегментами сети могут использоваться шлюзы, а для контроля подключения к Web-ресурсам — прокси-серверы.

Виртуальные сети для фильтрации и обеспечения защиты могут использовать функциональность гипервизоров.

В системе должен быть настроен логический доступ, то есть при физическом подключении сотрудника к какому-либо устройству система должна определить — предоставлять доступ или нет. В данном случае отказ является инцидентом ИБ.

Мониторинг и анализ информационной безопасности

Мониторинг и анализ ИБ подразумевает сохранение функций безопасности на всем жизненном цикле системы и отвечает за сбор данных об общем состоянии системы с конечных устройств, а затем анализ полученных данных для выявления возможных нарушений безопасности, то есть следующие этапы: мониторинг, анализ, действие.

Каждый этап имеет основные функции безопасности.

• мониторинг: сбор информации с конечных устройств, логирование событий ИБ, определение взаимосвязей событий ИБ;
• анализ: поведенческий анализ (эвристический метод), анализ на основе правил (сигнатурный метод);
• действие: профилактика инцидентов ИБ, ликвидация последствий инцидентов ИБ, расследование инцидентов ИБ.

При мониторинге безопасности осуществляется сбор разных типов данных системы, что позволяет определять события безопасности и прогнозировать будущие риски. Данные могут собираться как с конечных устройств, так и из сети, например, информация о подключении нового устройства, срабатывании антивирусного средства или блокировании учетной записи по причине неоднократного ввода некорректного пароля и т. п. Перечень данных для мониторинга определяется при проектировании СИБ специалистами ИБ и владельцами систем, их объем должен быть достаточным для предотвращения, определения и локализации инцидента. Мониторинг настраивается с использованием стандартных средств ОС, ПО и специализированных систем для консолидации всей информации, например, Security information and event management (SIEM).

Мониторинг может использоваться для поиска потенциальных уязвимостей путем пассивного или активного анализа системы. Сама система мониторинга должна быть защищена, а все собранные данные храниться на защищенном сервере.

Анализ безопасности должен давать конкретные выводы по состоянию системы и может быть включен в план автоматического реагирования на инциденты. Также злоумышленник может оставлять следы, которые система должна фиксировать, это поможет в дальнейшем расследовании инцидента ИБ.

Проблемы, связанные с ИБ, должны быть обнаружены и локализованы до их использования злоумышленником, то есть в политике ИБ необходимо описать полный перечень действий для предотвращения инцидентов ИБ.

Во время инцидента ИБ необходимо точно знать, какие изменения происходят в системе. Сотрудники ИБ должны незамедлительно выполнить необходимые действия при регистрации инцидента: блокировку или отключение сервиса, отключение сегмента сети либо отмену изменений. Корректное ведение журналов может ускорить процесс расследования инцидентов и анализа причины возникновения. Должны соблюдаться все процедуры, указанные в плане реагирования на инциденты.

После инцидента должна быть восстановлена работа системы. Каждый инцидент необходимо проанализировать и предпринять меры для предотвращения повторного случая и при необходимости внести изменения в план реагирования.

Для обеспечения необходимого уровня безопасности и реагирования на инциденты ИБ рекомендуется запустить Security Operation Center (SOC).

Безопасная конфигурация и управление

Безопасная конфигурация и управление отвечают за контроль изменений функциональных возможностей системы и мер безопасности, обеспечивающих их защиту. Безопасная конфигурация и управление включают следующие основные функции:

– безопасное и контролируемое изменения системы, то есть функций системы;

– безопасное и контролируемое изменения политик и мер безопасности;

– управление идентификаторами устройств, то есть генерация, обновление и отзыв криптографических материалов (ключи, сертификаты и т. п.);

– безопасное управление конфигурациями системы;

– безопасное и контролируемое изменения конфигураций сети;

– защита данных;

– контроль над изменениями модели и политики ИБ.

Все версии ОС, ПО и конфигураций должны контролироваться. Конфигурацию сети также следует анализировать для обнаружения отклонений. Существует два вида управлений:

– оперативное управление системой — это конфигурация функциональных возможностей конечных устройств, обновление этих устройств, настройка физической и логической сети, настройка ОС, ПО;

– управление безопасностью — это управление средствами безопасности на конечных устройствах, настройка средств защиты информации и настройка политик. Это процесс, который настраивает и обновляет систему для поддержания уровня ИБ.

Оба этих вида должны функционировать независимо друг от друга, но, как правило, данная грань сильно размыта. Например, оперативное управление может взаимодействовать с мониторингом системы для выявления уязвимых мест.

Управление и конфигурация не должны нарушать эксплуатационные процессы или снижать безопасность и надежность системы. При оценке рисков необходимо рассматривать каждое конечное устройство или группу устройств. Контроль безопасности элементов системы должен осуществляться на всем жизненном цикле.

Защита данных

Стратегии защиты данных в зависимости от их типа делятся на три категории:

– Data-at-Rest (DAR) — данные находятся в хранилище, облачном хранилище, локальном USB-носителе и т. п.;

– Data-in-Use (DIU) — данные находятся в непостоянном хранилище: RAM, кеши;

– Data-in-Motion (DIM) — данные находятся в движении от одних конечных устройств до других.

Защита данных осуществляется в части компрометации, защиты от угроз модификации, перехвата, дублирования и доступности. Различные типы данных для защиты включают защиту:

– данных на конечных устройствах;

– данных, передаваемых по линиям связи;

– конфигураций оборудования;

– данных мониторинга инцидентов ИБ.

Уровень защиты должен быть соизмерим с последствиями от потери или фальсификации и нарушения доступности данных, а также для всех данных должен быть определен срок хранения.

Для обеспечения защиты данных необходимо использовать криптографических подход, помимо этого для защиты от утечек рекомендуется применять DLP-системы.

Политика и модель ИБ

Политика ИБ — это совокупность правил, процессов, процедур, методов для обеспечения ИБ в деятельности компании (системы). Она описывает цели безопасности системы, а модель — это формальное представление (в виде диаграмм, схем) политики.

Политика ИБ определяет отношения (разрешающие или запрещающие) между субъектами и объектами, то есть должно определяться взаимодействие между системой и сотрудниками, между системами и внутри системы. Она необходима для обеспечения ИБ и порядка взаимодействия в течение всего жизненного цикла, то есть для выстраивания процессов взаимодействия с точки зрения ИБ внутри объекта. Она должна описывать работу всех функциональных элементов СИБ для обеспечения комплексной безопасности и охватывать нормативный и организационный уровень безопасности объекта. Политика также должна определять, что следует анализировать, восстанавливать, а также кто и как может вносить изменения в элементы системы и т. п.

Политика и модель ИБ должны включать следующие разделы:

– анализ угроз системы, то есть непрерывный процесс определения возможной угрозы и оценки уязвимости системы для информационного воздействия;

– определение целей безопасности системы с точки зрения требований к конфиденциальности, целостности и доступности системы;

– политика безопасности, определяющая процессы, правила, меры безопасности и средства контроля, которые должны применяться в системе;

– модель безопасности, обеспечивающая формальное представление политики безопасности;

– политика безопасности защиты данных, конечных устройств, связей и подключений, мониторинга и анализа, конфигураций и управления изменениями системы.

Во всех разделах (безопасность защиты данных, конечных устройств и т. п.) должны быть отражены требования, описанные в разделах выше, например, для политики безопасности конечных устройств должны быть описаны требования в части взаимодействия, безопасной настройки и т. п. В политике безопасности связей и подключений должны быть определены требования при передаче информации, установка безопасной связи между устройствами, определены элементы, которым разрешено в сети взаимодействовать между собой и т. п. В политике безопасности мониторинга и анализа должна быть определена периодичность проведения работ по анализу уязвимостей, определен перечень информации, необходимый для анализа инцидентов и т. п. В политике безопасности конфигураций и управления изменениями системы должны быть описаны правила изменения конфигураций, определена конфигурация всех элементов системы и т. п. В политике безопасности защиты данных должна быть проведена классификация существующей информации, определены правила работы с различными типами информации, например, правила работы с конфиденциальной информацией и т. п.

Политика и модель должны соответствовать требованиям, описанным в нормативных документах РФ, например, приказах № 31 или № 239 ФСТЭК России. В соответствии с требованиями политика должна содержать следующие регламентации правил и процедур:

– идентификация и аутентификация;
– управление доступом;
– ограничение программной среды;
– защита машинных носителей информации;
– аудит безопасности;
– антивирусная защита;
– предотвращение вторжений (компьютерных атак);
– обеспечение целостности, доступности;
– защита технических средств и систем;
– защита информационной (автоматизированной) системы и ее компонентов;
– реагирование на компьютерные инциденты;
– управление конфигурацией информационной (автоматизированной) системы;
– управление обновлениями программного обеспечения;
– планирование мероприятий по обеспечению защиты информации;
– обеспечение действий в нештатных ситуациях;
– информирование и обучения персонала.

Принято считать, что политика — это верхнеуровневый документ, поэтому для простоты чтения документ рекомендуется разделять на части, а документы с глубокой проработкой выделять в виде регламентов.

Политика должна обновляться каждый год, но при внесении изменений в нормативные стандарты, введении новых приказов, постановлений правительства политика ИБ должна быть пересмотрена.

Не позволяй облакам застилать горизонт.
Ремейк по фразе Элизабет Гаскелл

Защита облачных технологий и виртуализации

Для облачных технологий и виртуализации используются классические подходы к обеспечению ИБ, применяемые в информационных системах (ИС). В связи с критичностью IIoT рекомендуется использовать частные облака, а не общего пользования. В облачных технологиях активно используются виртуальные сети и машины.

Все пользователи должны быть изолированы друг от друга. В последнее время для изоляции процессов и пользователей активно развивается технология контейнеризации. Виртуальные сети должны быть построены с использованием таких технологий, как VPN, VPLS и VLAN. Должна быть настроена аутентификация пользователей и устройств. Сетевой периметр к самой виртуальной машине должен быть защищен, например, с использованием межсетевых экранов и систем обнаружения вторжений. Гипервизоры должны быть корректно настроены, а также должны быть настроены встроенные функции безопасности виртуальных машин.

Данные при передаче должны быть зашифрованы и доступны только после аутентификации.

Проблема функциональной безопасности

Введенных в эксплуатацию АСУТП с использованием IIoT достаточно мало. Основная причина — это неготовность владельцев системы принимать существенные риски, связанные в первую очередь с ФБ объекта, а также проблемами интеграции технических средств АСУТП с данной средой. Существующие АСУТП имеют устаревшие технические средства, многие из которых не способны к интеграции, для которых необходимо использовать шлюзы, концентраторы, что усложняет систему и, как следствие, уменьшает ее надежность. Для внедрения концепции IIoT во введенные в эксплуатацию системы необходимо провести дорогостоящую модернизацию, со всеми этапами жизненного цикла, что повлечет высокие экономические издержки. Второй критичный фактор, связанный с ФБ, — это надежность облачных технологий и время отклика. Для большинства промышленных систем критична потеря связи при управлении. Как правило, на критически важных объектах, потенциально важных объектах при управлении технологическим процессом время реакции должно составлять доли микросекунд — задержки и потери недопустимы. Концепция IIoT не может предоставить необходимый уровень ФБ.

В существующих реалиях концепция IIoT применима для АСУ, при которой осуществляется только мониторинг технологического процесса, например, автоматизированная информационно-измерительная система коммерческого учета электроэнергии, поскольку

ку данная система осуществляет только мониторинг потребительской электроэнергии и отсутствует технологическое управление. Также следует рассматривать данную концепцию на этапе разработки новых автоматизированных систем.

Заключение

В данной статье были рассмотрены проблемы АСУТП при переходе на базу IIoT и один из подходов обеспечения ИБ. Также имеются другие стандарты и подходы в части обеспечения ИБ, например, набор стандартов IEC 62443.

Концепция IIoT имеет огромный пласт проблем, связанных с обеспечением ИБ.

Помимо этого, данная концепция не применима для всего промышленного сегмента. Это связано, в частности, с критичностью АСУТП. Для многих систем технологический процесс является критичным, и его остановка или задержка не допустимы. На данный момент большинство АСУ в РФ не готовы к переходу на IIoT, а сама технология не может предоставить необходимый уровень безопасности (как с точки зрения ИБ, так и ФБ) и скорости работ. Но концепция работоспособна для некритических АСУ, направленных в большей степени на мониторинг процессов или сбор определенной информации. Подход IIoT для данных систем позволит осуществлять дополнительный мониторинг, при этом события ИБ не повлекут существенных потерь.

Список литературы

1. *Капранова Л.Д.* Цифровая экономика в России: состояние и перспективы развития // Экономика и управление. 2018. №2. С. 58-69.
2. *Kireev V.S., Guseva A.I., Bochkaryov P.V., Kuznetsov I.A., Filippov S. A.* Association Rules Mining for Predictive Analytics in IoT Cloud System // Advances in Intelligent Systems and Computing, 2018, Vol. 848, pp.107-112.
3. *Astakhov M.I.* Creation of the National Ecosystem Based on Digital Technology and Smart Things // Bulletin of the Federal Agency for Technical Regulation and Metrology. 2017. №.4. p.30.
4. Цифровые платформы управления жизненным циклом комплексных систем. Под общ. редакцией проф. В. А. Тупчиенко. М.: Издательство «Научный консультант». 2018. 440 с.
5. *Котяшичев И.А., Бырылова Е.А.* Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. 2015. №6.4. С. 30-34.
6. *Сапожников А.* Общий обзор реестров и классификаций уязвимостей (CVE, OSVDB, NDV) // Безопасность пользователей в сети Internet. 2019 URL: https://safe-surf.ru/specialists/article/5228/607311/ (дата обращения 29.06.2019).

Зулькарнаев Равиль Фикратович *– аспирант МИФИ, старший консультант Центра информационной безопасности компании «Инфосистемы Джет». Контактный телефон (495) 411-76-01.*

К 2021 г. более 40% организаций будут использовать для борьбы с мошенничеством ИИ и машинное обучение

По данным компании SAS и Ассоциации сертифицированных специалистов по расследованию хищений и мошенничества (Association of Certified Fraud Examiners, ACFE), всего через два года искусственный интеллект (ИИ) и машинное обучение будут использоваться для противодействия мошенничеству в три раза чаще, чем сейчас. В настоящее время такие антифрод-инструменты уже используют в 13% организаций, принявших участие в опросе, и в еще 25% заявили, что планируют их внедрить в течение ближайшего года-двух.

Совместное исследование SAS и ACFE было запущено в феврале 2019 г., а его итоги подведены в конце июня 2019 г. Для этого были изучены ответы 1055 членов ACFE, работающих в разных странах мира. По итогам был создан интерактивный отчет. Вопросы, заданные экспертам, касались технологий и инструментов, которые используются в их организациях для борьбы с мошенничеством.

Как выяснилось, в настоящее время большинство организаций чаще всего пользуются преднастроенными отчетами по ключевым событиям мошенничества с использованием классических инструментов, например, от Microsoft Office. Это стандартный инструмент для 64% компаний, охваченных исследованием. На втором по популярности месте автоматический мониторинг с использованием экспертных бизнес-правил — его используют в 54% организаций. Замыкает тройку визуальное исследование данных с использованием BI инструментов — на ее долю приходится 35%.

В перспективе помимо роста интереса к ИИ ожидается развитие следующих трендов:

- более широкое распространение биометрии. Сейчас ее использует примерно каждая четвертая организация, а еще 16% участников опроса планируют внедрить до 2021 г.;
- увеличение внимания различным инструментам и приемам анализа данных. Ожидается, что к 2021 г. 72% организаций будут использовать для борьбы с мошенничеством автоматический мониторинг данных, автоматическое обнаружение аномалий и др.;
- предиктивная аналитика планируется использоваться в 52% организаций, что на 22% выше показателей предыдущего исследования;
- применение инструментов визуализации данных, — их планируют использовать или продолжить использовать 47% организаций (сейчас примеряют 35%).

Один из вопросов, заданных участникам, касался наиболее часто используемых аналитических инструментов. Выяснилось, что решения SAS чаще всего выбирают для решения задач предиктивной аналитики и моделирования, для анализа социальных взаимосвязей и применения графовой аналитики, для глубокого анализа текстовой информации.

Https://www.itweek.ru