Моделирование угроз в условиях методической неопределенности

Юлия Дащенко

11.12.2018

Оглавление

Каждый субъект КИИ сталкивается с необходимостью моделирования угроз с самых первых шагов по обеспечению безопасности объекта КИИ. Так, согласно Правилам категорирования, информация об угрозах должна учитываться при категорировании объекта КИИ. Кроме того, анализ угроз безопасности информации в отношении объекта КИИ и разработка модели угроз входят в состав обязательных мер защиты, определенных Требованиями по безопасности КИИ.

Главная трудность при разработке модели угроз связана с выбором методики определения угроз безопасности. Ситуация осложняется тем, что пока в нашей стране не разработаны методические документы, регламентирующие порядок моделирования угроз для объектов КИИ. Поэтому все субъекты КИИ временно вынуждены заниматься анализом угроз в отношении своих объектов КИИ без какой-либо утвержденной методической базы. В связи с этим мы решили поделиться своим опытом разработки модели угроз информационной безопасности для объектов КИИ в условиях такой «временной неопределенности».

Для большей наглядности анализ угроз будет проводиться на примере типового объекта теплоэлектрогенерации. Однако, рассматриваемый подход к моделированию угроз может использоваться и в других отраслях.

Необходимо подчеркнуть, что приведенная ниже методика является лишь одним из возможных вариантов моделирования угроз до выхода соответствующих нормативных документов и не претендует на истину в последней инстанции. После опубликования соответствующих нормативно-методических документов данная методика, безусловно, должна быть пересмотрена с учетом новых требований регуляторов.

В случае, если предложенная в статье методика моделирования угроз будет адаптироваться для конкретного объекта КИИ, мы рекомендуем учитывать текущий уровень зрелости ИБ организации, от которого будет зависеть глубина проводимого анализа угроз. В рассматриваемом примере моделирование угроз проводилось исходя из предположения о минимальном уровне зрелости ИБ. Возможные варианты расширения изложенной методики для субъектов КИИ с более высоким уровнем зрелости рассматриваются в статье отдельно.

Надеемся, что эта статья будет полезна всем, кто уже столкнулся с методическими трудностями при разработке модели угроз для объекта КИИ.

Нормативно-методическая основа

При моделировании угроз мы частично используем методические документы по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры (далее – документы КСИИ), что допускается ФСТЭК России до появления соответствующих новых методических документов, несмотря на упразднение термина «ключевые системы информационной инфраструктуры».

Методика моделирования угроз

Используемая нами методика моделирования угроз включает следующие шаги:

1. Описание объекта защиты.
2. Определение источников угроз.
3. Формирование списка уязвимостей объекта защиты, которые могут быть использованы для реализации угроз.
4. Определение перечня угроз безопасности на основе имеющихся отечественных каталогов угроз.
5. Определение основных атрибутов угроз безопасности.
6. Формирование предположений о возможных киберфизических последствиях угроз.
7. Схема процесса моделирования угроз приведена на рисунке 1.

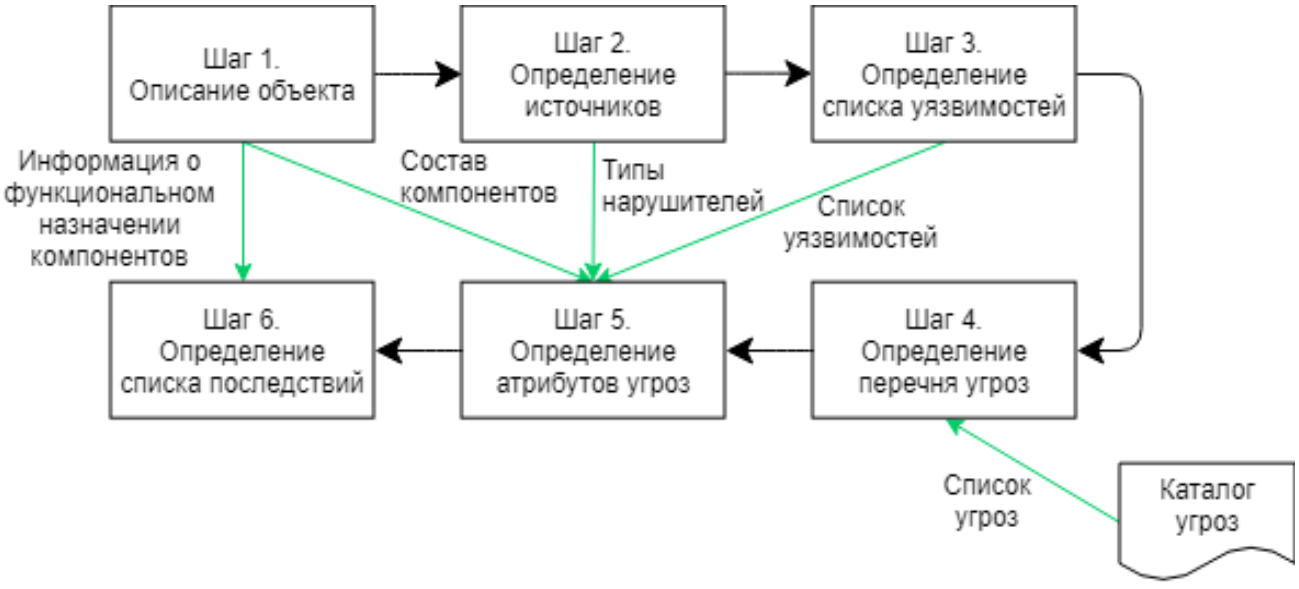

Рисунок 1. Схема процесса моделирования угроз

Шаг 1. Описание объекта защиты

Описание объекта защиты подразумевает определение основных компонентов рассматриваемого объекта КИИ и их функционального назначения.

В качестве примера объекта защиты для проведения моделирования угроз рассмотрим автоматизированную систему управления технологическим процессом (АСУ ТП) типового объекта теплоэлектрогенерации.

Данная система является многоуровневой интегрированной системой, объединяющей в своем составе подсистемы следующих технологических процессов:

- теплотехнического;
- электротехнического;
- информационно-измерительного.

Обобщенный перечень функциональных подсистем АСУ ТП типового объекта теплоэлектрогенерации приведен на рисунке 2.

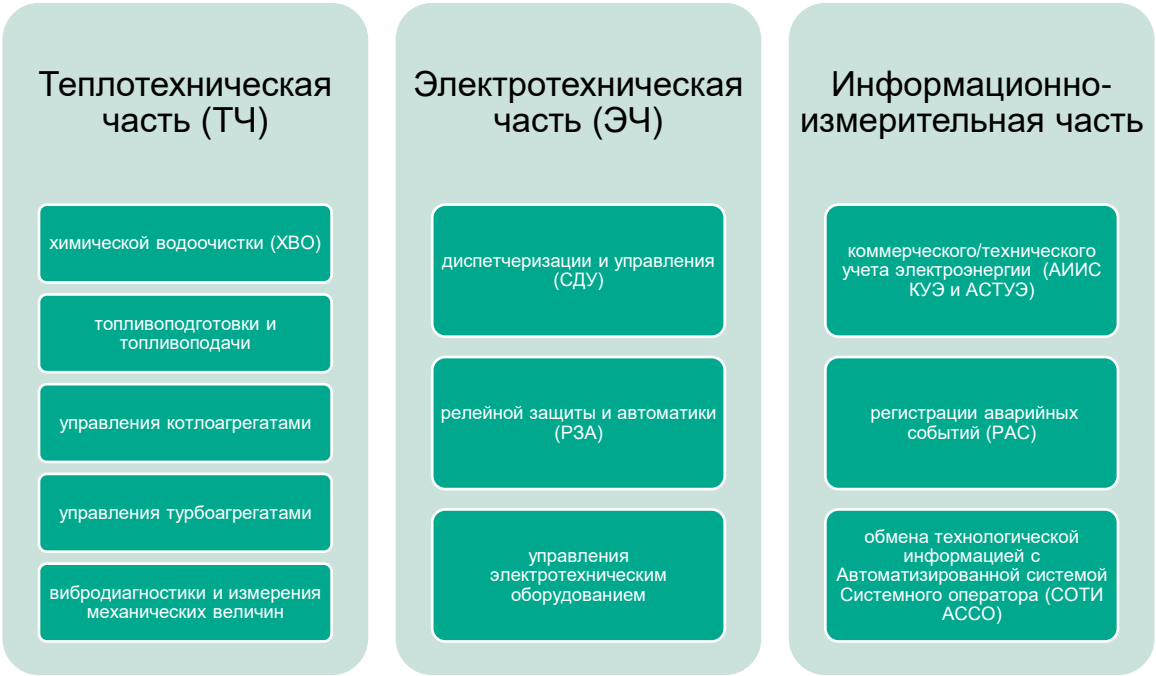

Рисунок 2. Функциональные подсистемы АСУ ТП типового объекта теплоэлектрогенерации

Каждая система в составе АСУ ТП типового объекта теплоэлектрогенерации выполняет определенный набор функций, приведенный в Таблице 1. Функциональное назначение систем потребуется нам на шаге 6 при формировании предположений о возможных киберфизических последствиях угроз.

Таблица 1 Функциональное назначение подсистем АСУ ТП типового объекта теплоэлектрогенерации

Подсистема	Функциональное назначение
ХВО	Обеспечивает водоподготовку для водогрейных котлов с целью предотвращения развития процессов коррозии и образования отложений в контурах водогрейных котлов, теплофикационных систем, защиты от коррозии медных и бронзовых деталей теплообменного оборудования и трубопроводов, отбор и очистку воды из природного источника, доставку воды и восстановление свойств отработанной воды для ее повторного использования.
топливоподготовки и топливоподачи	Обеспечивает подачу топливного газа в форсунки, регулирование его количества в зависимости от нагрузки на котлоагрегат. Кроме того, эта подсистема поддерживает оптимальное соотношение количества топливного газа, поступающего к форсункам, и воздуха на всем диапазоне нагрузок котлоагрегата. В случае использования угля в качестве топлива подсистема обеспечивает сортировку, фракционирование, дробление и подачу при помощи конвейеров.
управления котлоагрегатами	Обеспечивает измерение и контроль технологических параметров, логическое управление, автоматическое регулирование нагрузки, аварийную и предупредительную сигнализацию, передачу данных на уровень управления производством (АСУП). Основная функция подсистемы – поддержание стабильной работы котлоагрегата на всех технологических режимах
управления турбоагрегатами	Обеспечивает измерение и контроль технологических параметров, аварийную, предупредительную и диагностическую сигнализацию, регулирование технологических параметров с помощью программных регуляторов, расчёт технико-экономических показателей работы турбоагрегата, передачу данных на уровень управления производством (АСУП)
вибродиагностики и измерения механических величин	Обеспечивает мониторинг технического состояния оборудования, обнаружение возникших деструктивных нагрузок, дефектов и неисправностей.
СДУ	Обеспечивает удаленное диспетчерское и/или оперативное управление технологическим процессом и контроль состояния оборудования, дистанционное считывание осциллограмм аварийных процессов.
РЗА	Обеспечивает выявление и отделение поврежденного элемента или участка энергосистемы от ее неповрежденных частей, предотвращение аварий, контроль за появлением и развитием аварийных ситуаций.
управления электротехническим оборудованием	Обеспечивает измерение и контроль технологических параметров, логическое управление, аварийную и предупредительную сигнализацию, передачу данных на уровень управления производством (АСУП).
АИИС КУЭ и АСТУЭ	Обеспечивают контроль и коммерческий/технический учет электроэнергии и мощности, автоматизированный сбор и хранение данных об энергопотреблении.

РАС	Обеспечивает запись аварийных процессов и событий, контроль состояния устройств РЗА и положения коммутационных аппаратов в нормальных, аварийных и послеаварийных режимах.
СОТИ АССО	Обеспечивает измерение электрических и технологических параметров и преобразование их к цифровому виду, сбор аналоговых и дискретных данных о технологическом процессе и состоянии оборудования с использованием периодического опроса и/или спонтанно (по изменению), передачу информации СО ЕЭС.

Далее определим состав основных технических средств объекта защиты. Для этого воспользуемся многоуровневой структурой АСУ ТП, предложенной в 31-ом приказе ФСТЭК России, согласно которой выделяется три логических уровня АСУ ТП: уровень операторского (диспетчерского) управления, уровень автоматического управления и полевой уровень**.** Причем каждому уровню соответствуют свои группы технических средств, включающие:

- серверы (серверы системы SCADA, архивные, сервер единого времени, сервер телемеханики и другие);
- АРМ пользователей (операторов, машинистов, инженеров);
- телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, преобразователи интерфейсов, мультиплексоры);
- каналы связи;
- управляющие устройства (ПЛК, устройства связи с объектами, БРКУ, УСПД и др.);
- исполнительные устройства (электротехническое оборудование, датчики, счетчики, КИП и ЗРА, устройства РЗА, измерительные преобразователи).

Таким образом, рассматривая каждую из функциональных подсистем АСУ ТП, мы формируем полный перечень основных компонентов объекта защиты. Пример описания типизированного состава компонентов для АСУ ТП объекта теплоэлектрогенерации приведен в Таблице 2.

Таблица 2. Типизированный состав компонентов АСУ ТП объекта теплоэлектрогенерации

Группа технических средств	Функциональная подсистема АСУ ТЧ	Состав технических средств
Уровень операторского (диспетчерского) управления		
Автоматизированные рабочие места	ХВО	• АРМ оператора ХВО • АРМ инженера • АРМ водоподготовки • АРХ контроля ВХР
	Топливоподготовки и топливоподачи	• АРМ оператора топливоподачи
	Управления котлоагрегатами	• АРМ оператора котла • АРМ машинистов котлов • АРМ старшего машиниста

	Управления турбоагрегатами	• АРМ машинистов турбин
	Вибродиагностики и измерения механических величин	• АРМ вибродиагностики
	-	• АРМ оператора-технолога • Принтер событий • Принтер отчетов • Принтер аварийных сообщений
	Диспетчеризации и управления	• АРМ инженера АСУ ЭЧ • АРМ начальника смены электроцеха • АРМ начальника смены станции
	РЗА	• АРМ оператора
	Управления электрооборудованием	• АРМ оператора-электрика • АРМ инженера • АРМ оператора
	РАС	• АРМ оператора
	СОТИ	• АРМ диспетчера
	АСКУЭ/АСТУЭ	• АРМ АСКУЭ/АСТУЭ
Серверы	Вибродиагностики	• Сервер вибродиагностики
	РЗА	• Сервер РЗА
	АСКУЭ/АСТУЭ	• Сервер АСКУЭ/АСТУЭ
	–	• Сервер SCADA • Сервер аспектов • Сервер единого времени • Сервер коммуникационный • Сервер телемеханики • Сервер архивов и расчетных задач
Телекоммуникационное оборудование	–	• Коммутаторы • Маршрутизаторы • Межсетевые экраны • Преобразователи интерфейсов • Мультиплексоры
Периферийные устройства	–	• Принтер событий • Принтер отчетов • Принтер аварийных сообщений

Уровень автоматического управления		
Управляющие устройства	АСКУЭ/АСТУЭ	УСПД
	РАС	Блоки регистрации контроля и управления (БРКУ)
	СОТИ	УСО
	РЗА	Терминалы РЗА
	–	Программируемые логические контроллеры (ПЛК)
	–	Устройства связи с объектом (УСО)
Уровень ввода (вывода) данных, исполнительных устройств (полевой уровень).		
Исполнительные устройства	–	Контрольно-измерительные приборы (КИП) и запорно-регулирующая аппаратура (ЗРА)
	–	Электротехническое оборудование
	Система вибродиагностики и измерения механических величин	Измерители вибрации и механических величин
	РЗА	Устройства релейной защиты и автоматики (РЗА) Автоматические выключатели
	–	Сигнальные устройства
	РАС	Регистратор аварийных событий
	АСКУЭ/АСТУЭ	Счетчики электрической энергии
	СОТИ	Преобразователи

При анализе угроз необходимо также учитывать, что объектом воздействия угроз выступают не только технические средства АСУ ТП, но и их программное обеспечение (микропрограммы, системное и прикладное ПО), а также информационные активы[1], обрабатываемые в АСУ ТП.

[1] Согласно 31-му приказу, информационными активами является любая информация о параметрах (состоянии) управляемого объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная важная (технологическая) информация), хранящаяся на различных носителях и в различных форматах, обрабатываемая в системе и передаваемая по каналам связи.

Расширение методики на шаге 1

Дополнительно может быть проведена категоризация компонентов объекта защиты по уровню их критичности, что позволит более точно определить степень тяжести возможных последствий от воздействия угрозы на конкретный компонент.

Шаг 2. Определение источников угроз

Согласно документам по защите КСИИ, в качестве источников угроз должны рассматриваться:

- нарушители (физические лица);
- аппаратные закладки;
- вредоносные программы;
- источники электромагнитных воздействий;
- технические средства регистрации, приема, съема, перехвата и фотографирования информации (далее – технические средства перехвата информации).

При определении угроз мы учитываем все типы источников, однако в первую очередь уделяем внимание оценке угроз, напрямую связанных с преднамеренными или случайными действиями нарушителей, так как реализация угроз, определяемых другими источниками, чаще всего подразумевает участие нарушителя.

В зависимости от наличия у нарушителя права доступа в контролируемую зону или периметр сети объекта теплоэлектрогенераци будем рассматривать внешних и внутренних нарушителей.

При детализации угроз существенное значение имеет потенциал нарушителя, определяемый его возможностями и характером воздействия (преднамеренное или случайное воздействие).

Классификация нарушителей в зависимости от имеющихся возможностей с краткой характеристикой методов воздействия на объект защиты представлена в Таблице 3. Для внутренних нарушителей возможности каждого последующего типа нарушителя по умолчанию включает возможности предыдущего.

Таблица 3. Типы и возможности нарушителей

Вид нарушителя	Характеристика имеющихся прав доступа	Способы реализации угроз воздействия	Характер воздействия
Внешний нарушитель			
Произвольный внешний субъект (хакер, преступная группа, спецслужбы иностранных государств, конкуренты и др.)	• Без каких-либо прав доступа к АСУ ТП или связанным с ней сетям и системам	• сбор информации об объекте защиты из внешних источников • поиск путей проникновения через внешние системы • эксплуатация уязвимостей	Преднамеренный

		• применение методов социальной инженерии	
Разработчик	• Доступ к исходным кодам ПО и прошивок отдельных аппаратных и (или) программных компонентов АСУ ТП	• внесение ошибок, уязвимостей, недекларированных возможностей в ПО, программных или аппаратных закладок на стадии разработки • распространение вредоносного ПО через собственные средства вычислительной техники (СВТ)	Преднамеренный Случайный
Внутренний нарушитель без права доступа к АСУ ТП			
Обслуживающий персонал (охрана, уборщики), посетители	• физический доступ в помещения с компонентами АСУ ТП	• физическое воздействие (в т.ч. подключение) на компоненты АСУ ТП	Случайный Преднамеренный
Пользователь внешних сервисов	• доступ к внешним сервисам и системам, связанным с АСУ ТП посредством программных интерфейсов	• эксплуатация уязвимостей • создание вредоносных закладок на ресурсах, доступных из АСУ ТП • злоупотребление полномочиями	Преднамеренный
Администратор внешних сервисов и внешней информационной инфраструктуры	• доступ к сети и сетевому оборудованию	• установка дополнительного оборудования • изменение конфигурации сетевого оборудования	Преднамеренный Случайный
Внутренний нарушитель, авторизованный в АСУ ТП			
Пользователь АСУ ТП (операторы, диспетчеры)	• доступ к отдельным компонентам и функциям АСУ ТП	• некорректное изменение параметров ТП • подлог данных • прослушивание/перехват данных	Преднамеренный Случайный
Администратор АСУ ТП	• полный доступ к компонентам АСУ ТП и функциям конфигурирования, перепрограммирования и администрирования	• изменение конфигурации компонентов АСУ ТП	Преднамеренный Случайный

Внешние субъекты, занимающиеся обслуживанием АСУ ТП (например, интегратор, производитель)	• полный удаленный доступ к компонентам АСУ ТП и функциям конфигурирования, перепрограммирования и администрирования	• изменение конфигурации компонентов АСУ ТП	Преднамеренный Случайный

Расширение методики на шаге 2

При описании возможных типов нарушителей дополнительно могут рассматриваться следующие характеристики, влияющие на потенциал нарушителя:

- мотивация нарушителя (например, хулиганство, обида, достижение политических целей, получение денежной выгоды и т.д.);
- возможный уровень знаний и навыков нарушителя.

Кроме того, при формировании модели нарушителя полезно учитывать возможность нарушителя вступать в сговор с другими типами нарушителей (например, подкуп сотрудников), а также возможность изменения типа злоумышленника по мере реализации угроз, связанных с эскалацией привилегий, в тех случаях, когда в результате им получены соответствующие полномочия.

Указанные дополнения могут быть использованы для качественной оценки вероятности реализации угрозы.

Шаг 3. Формирование списка уязвимостей объекта защиты

В большинстве случаев реализация угроз ИБ становится возможной из-за наличия у объекта защиты уязвимостей, которые могут быть связаны с недостатками как в программно-аппаратном обеспечении, так и в организации его защиты.

Анализ объекта защиты с точки зрения наличия уязвимостей обеспечивает максимальную полноту описания возможных угроз и помогает сформировать комплексный подход к построению системы защиты.

На основании документов КСИИ можно выделить следующие классы уязвимостей АСУ ТП:

- уязвимости системного и прикладного ПО;
- уязвимости аппаратного обеспечения;
- уязвимости протоколов сетевого взаимодействия;
- уязвимости, вызванные недостатками организации обеспечения ИБ систем АСУ ТП при эксплуатации и обслуживании систем АСУ ТП.

Отметим, что мы исключили из рассмотрения уязвимости, связанные с наличием технических каналов утечки информации, ввиду сложности и высокой стоимости технических средств, необходимых нарушителю для их эксплуатации.

Указанные выше классы уязвимостей являются общими для любых типов объектов защиты и могут быть конкретизированы с учетом специфики рассматриваемого объекта

защиты. При этом каждый из основных компонентов объекта защиты должен рассматриваться в качестве потенциально уязвимого.

Пример детализации уязвимостей для АСУ ТП типового объекта теплоэлектрогенерации приведен в Таблице 4.

Таблица 4. Возможные уязвимости АСУ ТП типового объекта теплоэлектрогенерации

Класс уязвимостей	Детализация уязвимостей для объекта теплоэлектрогенерации
Уязвимости системного и прикладного ПО	○ Уязвимости в SCADA и HMI-компонентах ○ Уязвимости OPC-серверов ○ Уязвимости в инженерном программном обеспечении ○ Уязвимости операционных систем и программного обеспечения общего назначения, установленных на АРМ пользователей (диспетчеров, операторов и т.д.) и промышленных серверах
Уязвимости аппаратного обеспечения	○ Уязвимости ПЛК ○ Уязвимости оборудования RTU ○ Уязвимости сетевого оборудования промышленного назначения ○ Уязвимости исполнительных устройств
Уязвимости протоколов сетевого взаимодействия	○ Открытые и незащищённые каналы связи между компонентами систем защиты и управления, а также между объектами силовой инфраструктуры, в том числе: • отсутствие проверки подлинности, что влечет за собой возможности подмены устройств и передаваемых данных; • открытые для изучения стандарты (что облегчает задачу злоумышленникам), и открытая передача данных, позволяющая прослушивать и искажать информацию; • высокая детализация сетевых коммуникаций; • связь с открытыми (корпоративными) сетями, что повышает риск неавторизованного доступа к АСУ ТП.
Уязвимости, вызванные недостатками организации обеспечения ИБ систем АСУ ТП при эксплуатации и обслуживании систем АСУ ТП	○ Отсутствие или недостаточный уровень знаний в области ИБ у обслуживающего персонала, что проявляется в виде: • использования привилегированного удаленного доступа из недоверенной сети; • отсутствия политик парольной защиты и управления пользователями; • использования устаревшего ПО; • обслуживания АСУ ТП с небезопасных рабочих станций; • отсутствия регулярного контроля конфигураций и ПО. ○ Отсутствие следования требованиям ИБ при проектировании решений, что обуславливает: • слабую устойчивость АСУ ТП ко взлому; • некорректные или недостаточные настройки безопасности ЛВС; • отсутствие защиты данных, передаваемых по открытым каналам;

	• отсутствие ролевого разграничения прав доступа; • отсутствие решений по контролю запуска приложений; • отсутствие или недостаточность средств регистрации событий ИБ. ○ Проблемы разграничения и управления доступом подрядных организаций, связанные с необходимостью обеспечения временного доступа к ограниченному количеству оборудования без возможности влияния на остальные части системы, а также отмены такого доступа по окончании работ. ○ Продолжительный срок службы уязвимых компонентов, вызванный сложностью модернизации оборудования и систем

Расширение методики на шаге 3

При формировании списка уязвимостей могут учитываться имеющиеся результаты анализа защищенности и тестирования на проникновение, а также информация из общедоступных каталогов уязвимостей в соответствии с используемым на объекте защиты оборудованием и программным обеспечением.

Кроме того, для каждой уязвимости (или каждого класса уязвимостей) дополнительно может быть проведен анализ на наличие мер защиты, которые позволяют минимизировать или полностью исключить возможность использования уязвимостей для реализации угроз безопасности.

Шаг 4. Определение перечня угроз безопасности

Для формирования перечня угроз безопасности мы используем Банк данных угроз безопасности информации (далее – Банк данных угроз), созданный ФСТЭК России совместно с ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Для конкретной системы содержимое Банка данных угроз позволяет очертить ландшафт угроз в «крупную клетку». После чего, список угроз может дополняться более специфичными угрозами.

Для определения списка угроз в отношении конкретного объекта защиты из состава возможных угроз следует исключить неактуальные для этого объекта угрозы. Например, угрозы, связанные с отдельными типами технологий и систем, которые не используются на объекте защиты.

Так, для АСУ ТП типового объекта теплоэлектрогенерации могут быть исключены следующие категории угроз:

- угрозы для грид-систем;
- угрозы, связанные с использованием облачных технологий;
- угрозы для суперкомпьютеров;
- угрозы, связанные с системами хранения больших данных.

Полученный таким образом перечень угроз еще не является окончательным, и он будет уточняться на следующих шагах методики.

Расширение методики на шаге 4

Другим способом определения перечня угроз для объекта защиты является анализ всевозможных сочетаний трех базовых атрибутов угрозы (источника, объекта

воздействия и уязвимости) с точки зрения того, какие деструктивные действия может совершить конкретный нарушитель по отношению к отдельному компоненту объекта защиты за счет использования определенной уязвимости этого компонента. Каждое такое сочетание, по сути, и будет определять возможную угрозу безопасности. При использовании данного подхода к определению перечня угроз шаг 5 методики должен быть пропущен.

Кроме того, при определении перечня угроз дополнительно может учитываться информация о реализованных на объекте защиты угрозах и инцидентах, если таковые были.

Шаг 5. Описание угроз безопасности

На данном шаге для каждой угрозы из перечня, сформированного на предыдущем шаге, необходимо описать возможный сценарий реализации и установить соответствие между основными компонентами объекта защиты (объектами воздействия угрозы), возможными источниками угроз и уязвимостями.

Для упрощения выполнения данного шага можно использовать описание угроз из Банка данных угроз. Оно содержит сценарий реализации угрозы, предположения об уязвимостях, которые могут быть использованы при реализации угрозы, тип нарушителя (внешний или внутренний) и объект воздействия. Соответствующий пример приведен на рисунке 3.

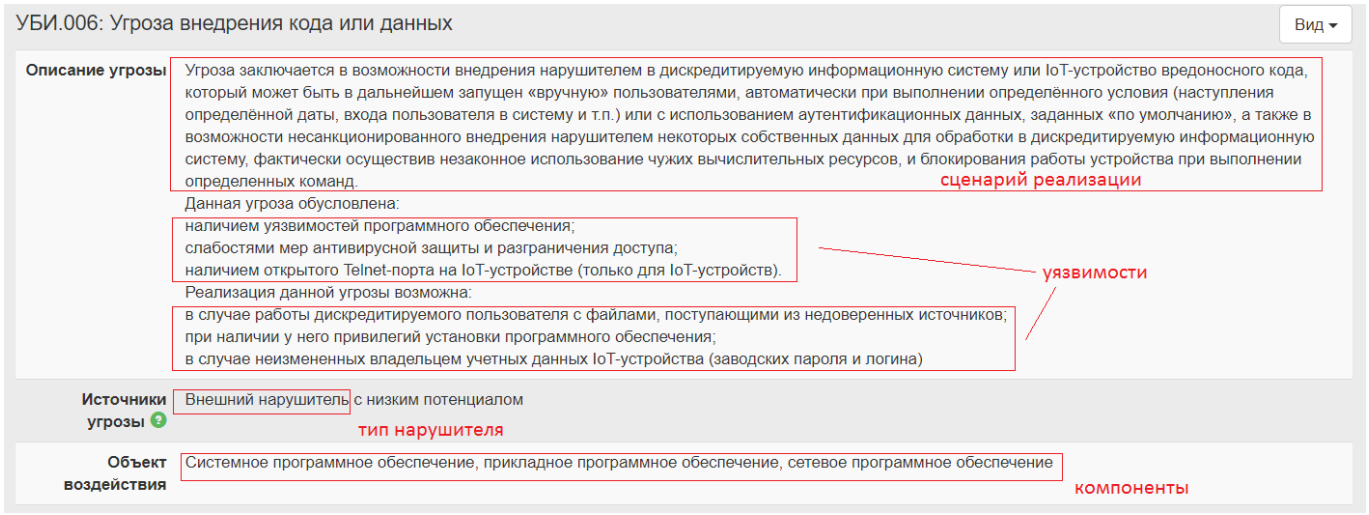

Рисунок 3. Пример описания угрозы из Банка данных угроз

Для того чтобы описание угроз учитывало специфику рассматриваемого объекта защиты, информацию из Банка данных угроз необходимо дополнить и адаптировать, используя сформированный перечень компонентов (шаг 1), классификацию нарушителей (шаг 2) и список уязвимостей (шаг 3).

В Таблице 5 приведен пример описания угрозы для АСУ ТП типового объекта теплоэлектрогенерации, полученный путем адаптации описания угрозы из Банка данных угроз.

Таблица 5. Пример описания угрозы внедрения кода или данных для АСУ ТП типового объекта теплоэлектрогенерации

Угроза внедрения кода или данных	
Сценарий реализации угрозы	Внедрение нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями или автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.), а также возможность несанкционированного внедрения нарушителем в дискредитируемую информационную систему некоторых собственных данных для обработки, фактически осуществив незаконное использование чужих вычислительных ресурсов
Объекты воздействия	• АРМ оператора котла • АРМ оператора топливоподачи • АРМ оператора пускоотопительной котельной • АРМ инженера АСУ ТП • АРМ инженера электроцеха • АРМ машинистов котлов • АРМ машинистов турбин • АРМ оператора-технолога • АРМ старшего машиниста • АРМ оператора-электрика • АРМ генераторов • АРМ РЗА • АРМ инженера АСУ ЭЧ • АРМ начальника смены электроцеха • АРМ начальника смены станции • Сервер связи • Сервер аспектов • Сервер единого времени • Сервер архивов и расчетных задач • Сервер SCADA • Сервер коммуникационный • Сервер телемеханики • Коммутаторы • Маршрутизаторы • Межсетевые экраны • ПЛК
Уязвимости	• Уязвимости в SCADA и HMI-компонентах • Уязвимости в инженерном программном обеспечении • Уязвимости операционных систем и программного обеспечения общего назначения, установленных на АРМ пользователей и промышленных серверах • Уязвимости ПЛК • Уязвимости оборудования RTU • Уязвимости сетевого оборудования промышленного назначения • Некорректное разграничение прав доступа • Отсутствие антивирусной защиты

	• Недостаточный уровень знаний в области ИБ у обслуживающего персонала (использование файлов, поступающих из недоверенных источников) • Некорректные или недостаточные настройки безопасности ЛВС (использование учетных данных, заданных по умолчанию)
Источники угрозы	• Произвольный внешний субъект • Разработчик • Пользователь внешних сервисов • Администратор внешних сервисов и внешней информационной инфраструктуры

Угрозы, для которых не удалось установить соответствие конкретной уязвимости и (или) компоненту объекта защиты, следует исключить из общего перечня угроз.

Расширения методики на шаге 5

Для сформированного перечня угроз дополнительно может быть проведена качественная оценка вероятности их реализации. В этом случае исходными данными для оценки будет являться информация о потенциале нарушителя и существующих мерах защиты, направленных на устранение возможных уязвимостей. Чем больше возможностей имеет нарушитель, чем серьезнее его мотивация и чем выше у него уровень знаний и навыков, тем больше вероятность реализации угрозы. При этом, чем эффективнее существующие меры защиты, тем меньше вероятность реализации угроз.

По результатам оценки вероятности реализации угроз из перечня угроз могут быть исключены те угрозы, реализация которых была признана маловероятной.

В дальнейшем вероятность реализации угроз может учитываться при планировании мероприятий по обеспечению безопасности объекта защиты для приоритезации мер, направленных на нейтрализацию угроз. Так, к первоочередным мероприятиям должны относиться меры защиты в отношении наиболее вероятных угроз.

Шаг 6. Определение возможных киберфизических последствий

На данном шаге для каждой угрозы из перечня требуется определить состав возможных киберфизических последствий.

В Банке данных угроз в качестве последствий от реализации угроз рассматривается нарушение тех или иных свойств безопасности информации (конфиденциальности, целостности, доступности). Применительно к АСУ ТП наиболее критичным является нарушение таких свойств безопасности информации, как целостность и доступность, влекущее за собой негативные киберфизические последствия для функционирования объекта защиты в целом.

Например, киберфизическими последствиями от реализации угроз в отношении АСУ ТП электростанций могут быть:

- снижение качества обслуживания клиентов или отключение конечных и иных потребителей;
- потеря коммерчески критичной информации;
- снижение объемов выработки электроэнергии или временная остановка электрогенерации;
- возникновение аварийных ситуаций на энергогенерирующем объекте.

Для того чтобы определить возможные киберфизические последствия для каждой угрозы, следует опираться на информацию о функциональном назначении объекта воздействия угрозы или подсистемы, в которую он входит (см. шаг 1). Это важно, так как последствия от реализации одной и той же угрозы, реализованной в отношении разных компонентов объекта защиты, могут различаться в зависимости от критичности выполняемых функций каждого компонента.

Пример определения киберфизических последствий угроз в отношении АСУ ТП типового объекта теплоэлектрогенерации в зависимости от функциональной подсистемы, компоненты которой подвергаются воздействию угрозы, приведен в Таблице 6.

Таблица 6. Описание киберфизических последствий угроз в отношении АСУ ТП электростанций

Подсистема	Возможные последствия при нарушении функционирования подсистемы
ХВО	• Уменьшение срока службы водогрейных котлов за счет развития процессов коррозии и образования отложений
топливоподготовки и топливоподачи	• Возникновение аварийной ситуации в связи с излишней подачей топливного газа • Возникновение аварийной ситуации в связи с несоблюдением оптимального соотношения количества топливного газа, поступающего к форсункам, и воздуха на всем диапазоне нагрузок котлоагрегата • Нарушение подачи топливного газа в форсунки
управления котлоагрегатами	• Нарушение стабильной работы котлоагрегата • Снижение объемов выработки электроэнергии или временная остановка электрогенерации
управления турбоагрегатами	• Возникновение аварийной ситуации, вызванной отсутствием предупредительной сигнализации из-за некорректных данных измерения и контроля технологических параметров • Возникновение аварийной ситуации, вызванной некорректной регулировкой технологических параметров • Снижение объемов выработки электроэнергии или временная остановка электрогенерации
вибродиагностики и измерения механических величин	• Возникновение аварийной ситуации, вызванной отсутствием своевременного обнаружения возникших деструктивных нагрузок, дефектов и неисправностей

СДУ	• Возникновение аварийной ситуации из-за некорректных или несвоевременных действий диспетчера или оператора • Снижение качества обслуживания клиентов или отключение конечных и иных потребителей • Снижение объемов выработки электроэнергии или временная остановка электрогенерации
РЗА	• Возникновение различных аварийных ситуаций на энергогенерирующем объекте из-за отсутствия своевременного выявления и отделения поврежденного элемента или участка энергосистемы от ее неповрежденных частей
управления электротехническим оборудованием	• Возникновение аварийной ситуации, вызванной некорректным измерением технологических параметров • Снижение объемов выработки электроэнергии или временная остановка электрогенерации
АИИС КУЭ и АСТУЭ	• Потеря или искажение коммерчески критичной информации
РАС	• Потеря или искажение коммерчески критичной информации
СОТИ АССО	• Потеря или искажение коммерчески критичной информации

При анализе возможных последствий нужно учитывать, что некоторые угрозы не приводят к каким-либо киберфизическим последствиям, однако могут повлечь за собой реализацию других угроз, которые уже напрямую влияют на технологические и бизнес-процессы организации.

Заключение

Использование предложенного в этой статье подхода к моделированию угроз позволит получить детализированный перечень угроз безопасности с указанием возможных киберфизических последствий от их реализации для конкретного объекта защиты. В дальнейшем на основании этого перечня могут быть определены соответствующие меры защиты и расставлены приоритеты по реализации подсистем защиты, исходя из критичности определенных последствий.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky lab ICS CERT

Ics-cert@kaspersky.com