IV. Кибербезопасность. Особенности обеспечения безопасности в социальных сетях

Промыслов В.Г., Семенков К.В.

Управление риском кибербезопасности на этапе проектирования для промышленных систем

Аннотация: В работе рассматривается процедура оценки риска кибербезопасности для этапа разработки в промышленных системах. Предлагается двухэтапная процедура. Первый этап включает общую для системы оценку риска, не использующую детальных данных о системе, что позволяет преодолеть неопределенность входных данных на начальном этапе жизненного цикла. Второй (опциональный) этап включает детальную оценку риска, что позволяет учитывать особенности архитектуры системы и специфичную для системы модель угроз.

Ключевые слова: кибербезопасность, оценка риска, разработка, неопределенность данных

Нет простого рецепта, как обезопасить промышленную систему управления (АСУ ТП) от киберугроз. Однако, есть общее понимание, что работа по обеспечению кибербезопасности, должна начинаться на самых ранних этапах жизненного цикла системы, начиная с первых шагов по ее разработке [1]. Этап разработки характеризуется неопределенностью в понимании деталей реализации системы и частично – в требованиях, предъявляемых к системе. Этап разработки может быть не самым значительным по времени, но является одним из важных этапов, когда закладываются основные технически решения по обеспечению информационной безопасности.

В ситуации, когда нет четко сформулированных моделей явлений или есть неопределенность во входных данных, часто применяют риск-ориентированные подходы. Поэтому обеспечение

кибербезопасности промышленных систем во многом связано с управлением риском. С каждой АСУ ТП у организации связаны разные риски, которые зависят как от внешнего контекста (месторасположение, специфические для отрасли угрозы и вероятности реализации угроз в смысле как она понимается в оценке риска [2]), так и внутреннего контекста (присущие конкретной системе: уязвимости, влияние последствия кибератаки на объект управления и пр.).

В данной работе рассматривается двухэтапный подход к оценке риска кибербезопасности для промышленных критически важных объектов (КВО).

Процедура оценки риска на этапе разработки делится на два этапа. Целью первоначальной оценки рисков кибербезопасности для системы, свойства которой известны только в самом общем виде, является получение базовой оценки риска.

Риск в этом случае обычно оценивается с точки зрения воздействия инцидента кибербезопасности на здоровье, безопасность, окружающую среду, или нарушение производственной деятельности.

Эта оценка помогает установить приоритеты детальной оценки рисков и облегчает разработку архитектуры безопасности КВО, например, в части деления на зоны безопасности или классификации активов. Существенным с точки обеспечения и анализа кибербезопасности системы является то, что система управления обычно строится по иерархическому принципу. Иерархия заложена и в архитектуру системы (наличие подсистем), и в архитектуру кибербезопасности (уровни и зоны кибербезопасности). Для обеспечения эффективной защиты и минимизации набора применяемых мер активы группируют по уровням кибербезопасности. Этот процесс неотделим от задачи категоризации/классификации активов. Объединение активов на уровне архитектуры системы приводит к появлению комплексных активов, которые принадлежат к другому уровню иерархии системы управления.

Процесс управления кибербезопасностью АСУ ТП КВО на первом этапе можно представить в виде последовательности следующих шагов:

– разработчик совместно с собственником КВО, в рамках общей программы информационной безопасности, определяет внешний и внутренний контекст оценки риска [3]. Внешний контекст включает всю доступную информацию об окружении КВО на данный момент, требования регуляторов или применяемых стандартов. Внутренний контекст составляют требования высших политик безопасности, которые действуют в организации-разработчике, известная на данный момент спецификация системы. Принимается неизменный набор мер безопасности, определяемый требованиями регулятора, используемых стандартов или политик безопасности верхнего уровня. Обязательным элементом внутреннего контекста должно стать информация о допустимом уровне риска для организации;

– для анализа риска используются стандартные для данного типа объекта наборы угроз и уязвимостей, без учета деталей реализации системы [3];

– оценку первоначального риска можно выполнять с использованием матрицы рисков, которая устанавливает взаимосвязь между вероятностью, воздействием и риском [4];

– полученный риск сравнивается с допустимым для организации риском.

Если риск для организации приемлем, то оценка риска может быть завершена. По крайне мере, до момента, когда она будет требовать переоценки. Переоценка может быть частью периодической процедуры перерасчета риска по истечении времени, или в связи с завершением этапа разработки или получения новых данных, не учтенных на предыдущем шаге.

Если же риск неприемлем, то необходим детальный анализ риска с целью выявления «точек напряжения» в системе и применения мер защиты для снижения риска до допустимого уровня.

Второй этап оценки риска по структуре повторяет процессный подход первого этапа, однако имеет более детальный характер. К моменту завершения первого этапа оценки риска обычно уже известна архитектура системы, в частности, ее разбиение на подсистемы. Подсистемы определены, по крайней мере, с точностью до ее спецификации, часто известны детали реализации.

Оценка риска на втором этапе проводится для каждой из подсистем.

– Проводится описание внешнего и внутреннего контекстов. Внешний контекст включает список специфичных для подсистемы угроз. Внутренний контекст включает всю доступную информацию о подсистеме на данный момент. Должен быть определен набор уязвимостей для реализации подсистемы.

– Собственник идентифицирует цифровые активы в подсистеме, а также функциональность активов в части обработки, хранения, передачи информации в цифровой форме.

– С использованием информации о специфичных угрозах и уязвимостях формируются сценарии атак на активы подсистемы.

Применяя одну из методик оценки риска [4], получают оценку риска.

Полученные риски сравниваются с допустимым для организации риском.

Для рисков, превышающих допустимый уровень, выбирается одна из стратегий управления риском [3].

Применение двухэтапной процедуры оценки риска имеет несколько преимуществ. Первый этап можно провести еще на самых начальных стадиях разработки, на неполных данных о системе, сразу после появления спецификации системы. Такой подход позволяет избежать критических ошибок в формировании требований на систему, связанных с недооценкой или переоценкой требований по кибербезопасности. Разбиение на этапы в случае необходимости предусматривает детальную оценку риска, но, с другой стороны, позволяет уменьшить выполняемый объем работ, устранив детальную оценку риска для подсистем, если общий риск для системы не превышает допустимый уровень.

Литература:

1. *M. de la Cámara, F.J. Sáenz, J.A. Calvo-Manzano and M. Arcilla*. Security by design factors for developing and evaluating secure software / 10th Iberian Conference on Information Systems and Technologies (CISTI) (17-20 June 2015 Aveiro). – URL: https://ieeexplore.ieee.org/document/7170500 (дата обращения 10.10.2021).

2. IEC 62443-3-2. Security for industrial automation and control systems. Part 3-2: Security risk assessment for system design. – IEC, 2020. – 63 p.

3. ГОСТ Р ИСО/МЭК 27005. Менеджмент рисков информационной безопасности–2010. – Москва: Стандартинформ, 2011. – 48 с.

4. ГОСТ Р ИСО/МЭК 31010. Методы оценки риска–2011. – М.: Стандартинформ, 2012. – 70 с.

Асратян Р.Э.

Использование технологии SSL/TLS для создания защищенных сетевых каналов в распределенных системах

Аннотация: Рассмотрены принципы организации защищенного сетевого взаимодействия на основе использования технологии SSL/TLS для создания защищенных сетевых каналов через общедоступную сеть. В отличие от технологии VPN, описываемый подход предполагает подключение средств информационной защиты на верхнем («транспортном») уровне стека протоколов модели OSI, что позволяет более точно «сфокусироваться» на потребностях конкретного протокола приложения: HTTP/SOAP, т.е. на защите взаимодействий web-клиентов и web-сервисов.

Ключевые слова: распределенные системы, Интернет-технологии, информационная безопасность, SSL/TLS, web-сервисы, разграничение прав доступа

Многие современные распределенные информационные системы включают десятки и даже сотни рабочих станций и серверов, взаимодействующих через общедоступную глобальную сеть. Задача организации безопасных взаимодействий в таких системах уже давно вышла «на первый план» [1-2]. Обычный способ решения этой задачи заключается в использовании технологии VPN (Virtual Private Network), позволяющей реализовать защищенный «туннель» через общедоступную сеть [3]. Так как средства криптозащиты подключаются в VPN на нижнем уровне иерархии протоколов OSI (как правило, не выше