УДК 004.056.5:378.3

О. В. Гальченко, В. В. Подтопельный

ОСОБЕННОСТИ МОДЕЛИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ SCADA

Поступила в редакцию 15.09.2021 г.
Рецензия от 06.10.2021 г.

Рассмотрены проблемы, возникающие при аудите автоматизированных систем управления технологическими процессами и корпоративной сети предприятия, а также особенности формирования модели аудита автоматизированных систем управления при наличии встроенных SCADA-систем. Выявлены возможности применения модели аудита при эксплуатации систем управления в реальном и защищенном режиме времени.

The problems arising during the audit of automated control systems for technological processes and the corporate network of an enterprise are considered. The features of the formation of the audit model of automated control systems in the presence of built-in SCADA-systems are considered. The possibilities of using the audit model in the operation of control systems in real and protected time modes are considered.

Ключевые слова: риск, информационная система, сетевая атака, сетевое вторжение, аудит

Keywords: risk, information system, network attack, network intrusion, audit

Введение

Современная автоматизированная система управления технологическим процессом (АСУТП) представляет собой человеко-машинную систему, которая обеспечивает автоматизированный сбор и обработку информации, необходимой для оптимизации и урегулирования управления технологическими процессами в соответствии с принятыми критериями управления объектом. Человек в этой связке анализирует работу средств вычислительных техник, предлагает варианты более безопасной эксплуатации, удобного управления, регулирует процесс обработки информации [1]. При этом АСУТП не избавлена от уязвимостей и, соответственно, от проблем, связанных с информационной безопасностью. В связи с этим специалисту, проводящему аудит, необходимо разработать такой подход, чтобы он мог полностью исследовать систему на наличие уязвимостей и при этом учитывать допустимые и

недопустимые временные задержки, характерные для систем данного типа. Также необходимо подобрать инструментарий таким образом, чтобы при исследовании уровня защищенности информационной системы не возникало лишней нагрузки на трафик [2].

Определение специфики подготовки безопасного активного аудита информационной безопасности АСУТП

При анализе проблемной области и исследовании системы АСУТП (в лабораторной среде) были выявлены следующие угрозы:

— проникновение злоумышленника извне в сеть с намерением вывести из строя автоматизированную систему или провоцирование сбоя в управляемых объектах для саморазрушения системы безопасности всей системы;

— взятие под контроль и управление технологическими объектами, несанкционированное проникновение в сеть с определенными целями (компрометация, выведение из строя, нарушение работы, распространение вируса для дальнейшего разрушения системы);

— проникновение с целью блокирования управления автоматизированными системами или управляемыми объектами;

— несанкционированное внесение с реестр обновлений программного обеспечения технологических объектов для изменения режимов работы.

Автоматизированная система подразумевает разделение на уровни [3]. Количество этих уровней может отличаться в каждой организации в зависимости от назначения АСУТП и выполняемых функций. Любую АСУТП в конечном итоге можно разделить на три основных уровня. Связь между уровнями обеспечивается коммуникационными серверами или контроллерами.

Исходя из сложности организации исследуемых систем аудит АСУТП подразделяют на несколько типов, которые отличаются друг от друга целями, перечнем анализируемых компонентов, исполнителями, применяемыми инструментами и результатами [4]:

— активный аудит (данный тип позволяет провести исследование уровня защищенности сегментов АСУТП и уделить особое внимание инженерно-техническому и полевому уровню, выявить уязвимости в линиях связи, ПО, ОС и компонентах АСУТП);

— пассивный аудит (этот тип также обращает внимание на два нижних уровня АСУТП, однако его воздействие на компоненты минимально, исследование проводится в виде прослушивания с целью выявления уязвимостей);

— экспертный аудит (аудит проводится в основном приглашенными специалистами, информация о системе собирается посредством опроса сотрудников, руководства и дополнительного инструментария);

— аудит на соответствие стандартам ИБ (проводят сотрудники специально уполномоченных организаций, которые проверяют систему безопасности компании на соответствие стандартам ИБ).

При проведении аудита ИБ АСУТП необходимо обращать особое внимание на защиту от воздействий следующих ключевых элементов:

— системы реального времени (СВР);

— системы управления и контроля над технологическими процессами и объектами;

— диспетчерский уровень (SCADA-система);

— линии связи и применяемые протоколы для передачи данных;

— технологические объекты на предмет возможного вмешательства в ПО.

Система технологических процессов может включать в себя несколько систем и подсистем, которые разработаны с использованием разных технологий. При проведении аудита диспетчерского уровня автоматизированной системы предприятия стоит учитывать, что при работе с системой реального времени нельзя допускать задержек, которые могут привести к катастрофическим последствиям. Таким образом, аудит некоторых АСУТП будет отличаться с учетом данного условия [5].

В процессе аудита решаются следующие задачи:

1. Сбор информации о системах безопасности, проведение инвентаризации инфраструктуры предприятия с учетом уровневого разделения АСУТП.

2. Проводится поиск уязвимостей (аналитический и активный, в ходе которого производится воздействие на уязвимость и ее источник). Активный аудит подразумевает определение следующих факторов:

— будут ли задержки в линиях связи при передаче информации;

— возникает ли искажение получаемой и передаваемой информации, что может стать целевой информацией для злоумышленника;

— будут ли возникать изменения в настройках систем и линиях передачи данных.

3. Анализ угроз, выявленных уязвимостей, вычисление рисков.

С учетом всех факторов процедуры аудита АСУТП могут отличаться. Выделяют несколько моделей и методов проведения аудита.

Существует модель аудита, которая охватывает по большей части организацию ИБ на верхних уровнях. Однако в таком случае аудит может быть неполным: часть уязвимостей, находящихся на нижних уровнях, закрыть не получится. Для того чтобы учесть все возможные негативные факторы, влияющие на состояние безопасности системы, требуется провести анализ нижних уровней АСУТП. Анализ проводится в следующих областях [6]:

— исполнительные модули и другие компоненты SCADA-системы;

— установленная операционная система на диспетчерском рабочем месте;

— программное обеспечение компонентов АСУТП;

— выявление возможных брешей, с помощью который есть возможность получить несанкционированный доступ.

Аудит АСУТП с учетом всех факторов и различий технологических подсистем предполагает рассмотрение следующих моделей аудита:

— первая модель разрабатывается для систем корпоративного уровня, которые можно проанализировать и обработать стандартными методами;

— вторая модель разрабатывается для подсистем, передающих и принимающих данные в режиме реального времени, которые стоит анализировать, используя специальное оборудование и ПО, способное разбирать пакеты данных, передающихся по промышленным протоколам.

С учетом множества компонентов автоматизированной системы строится формальная модель вычислений. Расчеты основываются на формуле определения общего показателя уязвимости системы. Результаты используются в качестве математического обеспечения для моделирования всевозможных ситуаций несанкционированного доступа (НСД), поступающих извне. Также данную можель можно применить для создания ПО и разработки лабораторной установки, имитирующей производственные процессы на предприятии.

Исходя из специфики разных уровней АСУТП, важной особенностью проводимого аудита является недопущение нарушения скорости передачи данных и работоспособности [6]. Порядок действий во время аудита будет отличаться в зависимости от уровня. Основные причины возникновения задержек при аудите:

1. Проблемы, связанные с нарушением связи по сети, а также с подключением к серверу клиентов. Это проверяется при запуске серверов пользователя и локальном подключении: возникают задержки в обновлении данных из-за проблем с сетью или скоростью трафика.

2. Задержки могут возникать из-за времязатратного скрипта. В одном из проектов могут применяться сложные скрипты, обработка и выполнение которых требуют определенного количества времени. По этой причине сервер ожидает, когда действие скрипта окончится. Только после выполнения скрипта данные отправятся на рабочие места.

3. Цикл между скриптами. Этот сценарий маловероятен, но может возникнуть в связи с тем, что один скрипт вызывает работу другого, и наоборот. Таким образом, возникает цикл скриптов и система занята ожидаем данных.

4. Задержки, возникающие из-за медленной работы серверов и пониженной скорости передачи данных.

5. Задержки, возникающие из-за передачи данных между OPC-серверами и SCADA-системой. При расположении OPC-сервера и SCADA-системы на разных рабочих станциях в случае нарушения работы сети возникают задержки в передаче данных.

Возможное влияние времени задержки сигналов в модулях, отвечающих за ввод и вывод данных на работу блоков управления, рассматривается с двух сторон:

— компенсация задержек благодаря вводу экстраполятора в модули ввода и вывода данных;

— учет влияния всех задержек на работу поставленного алгоритма управления.

С учетом фактора возникновения задержки при передаче пакетов данных следует подобрать такую модель аудита, которая позволит учесть специфику АСУТП и поможет вычислить вероятность появления задержки (период ее существования, период штатного функционирования системы во время проведения активного аудита).

При аудите для определения вероятности реализации той или иной угрозы моделируются несколько ситуаций.

Первая ситуация рассматривает возможности доступа нарушителя к уровням АСУТП. Особое внимание уделяется типу нарушителя. Таким образом, получается, что возможный доступ к граничным компонентам и подсистемам автоматизированной системы имеет внешний нарушитель. А скомпрометировать систему безопасности может как внешний, так и внутренний нарушитель. Однако при построении зональной модели в приоритете рассматривается внешний тип нарушителя.

Следующая ситуация рассматривает взаимодействие нарушителя с системой. Чтобы злоумышленник проник в систему и начал свою работу, ему необходимо в первую очередь проникнуть в канал связи для передачи данных в АСУТП. Он должен учесть специфику развернутой корпоративной сети, применяемых портов и способы передачи информации между рабочими станциями и компонентами нижнего уровня.

Третья ситуация обращает внимание на квалификацию нарушителя, так как подключение к каналам связи является довольно сложным занятием. Квалификация нарушителя напрямую зависит от его типа: для внутреннего нарушителя, имеющего свой прямой доступ к конфиденциальной информации, высокие знания в плане проникновения в систему безопасности компании не нужны, тогда как внешнему злоумышленнику необходима высокая квалификация, опыт и большой объем знаний, чтобы удаленно выявить уязвимости системы и реализовывать атаки.

Заключающим фактором является наличие поврежденных данных в канале связи, с помощью которых во время НСД злоумышленник сможет скомпрометировать систему безопасности.

Модель аудита должна учитывать специфику средств реализации инвентаризации и поиска уязвимостей в АСУТП. Обычно используют программные средства и инструменты съема данных с учетом специфики исследуемого объекта. Инструментальный аудит предполагает применение программно-аппаратных средств для выявления уровня защищенности АСУТП. Главными целями проведения инструментального аудита ИБ являются:

— получение информации о настоящем состоянии системы безопасности на разных уровнях автоматизированной системы, выявление внутренних и внешних угроз со стороны возможного злоумышленника;

— разработка мер и требований по повышению уровня защищенности системы предприятия.

Во время проведения инструментального аудита выявляются границы проведения аудита. Они могут варьироваться от проведения аудита ИБ всего предприятия в пределах контролируемой зоны до аудита только определенного уровня АСУТП [3]. После выявления границ для уточнения модели аудита выясняются перечень и местоположение объектов аудита. Определяется их физическая и логическая об-

ласть. Под физической областью понимается физическое местоположение объекта в автоматизированной системе. Логическая область охватывает каналы связи и способы подключения объектов к системе, использование промышленных протоколов, портов и IP-адресов для взаимодействия.

Во время проведения сетевого анализа инструментальный аудит подразумевает два этапа. Предварительно собирается вся информация о применяемых хостах, указывается перечень открытых портов, пользователей, имеющих доступ к данным и хостам, информация о применяющихся сетевых службах. На основе собранной информации проводится анализ системы и выявление уязвимостей в сетевых службах. Особенностью такого анализа является то, что не применяются атаки для вывода служб из рабочего состояния. В таком методе определяется факт наличия уязвимости без ее активации [6].

Также во время инструментального аудита проверяются конфигурационные настройки ПО АСУТП. С помощью данного анализа можно выявить эксплуатационные уязвимости, возникающие при неправильной настройке объектов автоматизированной системы.

Таким образом, можно рассмотреть применение разных инструментов для выявления уровня защищенности АСУТП и SCADA-системы для разных видов аудита ИБ (табл.) [7].

Применение инструментов для выявления уровня защищенности АСУТП для разных видов аудита ИБ

Инструмент	Активный аудит	Пассивный аудит	Экспертный аудит	Аудит на соответствие стандартам ИБ
DATARK в режиме активного и пассивного мониторинга	+	-	+	+
DATARK в режиме сканирования	–	+	+	+
Применение XSpider вместе с Nmap	+	–	+	+
XSpider: режим pentest	+	–	–	–
Nessus: безопасный режим	+	+	+	+
Nessus: опасный режим	+	–	–	–
SCADA-аудитор	+	+	–	–
Infowatch ARMA	+	+	+	+
OSSEC	+	+	–	+
Redcheck	+	+	+	–

Далее необходимо определить последовательность применения инструментов аудита, выбрать режимы и сценарии применения для безопасной работы, также рассматриваются методы и режимы работы инструментов.

Предварительно ознакомившись и выбрав необходимые настройки, можно составлять последовательность действий для проведения комплексного аудита. Собранную информацию необходимо структурировать перед проведением аудита. Разрабатывается перечень правил, необходимых для получения более полной информации о защищенности системы. Помимо описанной аналитической модели и представленных инструментов для аудита, в инструкции также необходимо обозначить организационные и нормативно-правовые мероприятия. Таким образом, в инструкции аудита присутствует информация о следующих действиях специалиста [6]:

1. Сбор информации о специфике развернутой АСУТП, применяемой SCADA-системе, основных конфигурациях, используемых компонентах и исполнительных модулях, применяемых средствами защиты информации.

2. Ознакомление с организованной корпоративной сетью и ее параметрами.

3. Определение систем реального времени, применяемых в АСУТП.

4. Производятся расчеты временных задержек.

5. На основе расчетов подбираются необходимые инструменты для проведения аудита системы безопасности.

Сама модель аудита в системах жесткого реального времени предполагает применение следующих инструментов сбора данных и поиска уязвимостей:

1. При помощи сканера уязвимости SCADA-аудитор проводится анализ имеющихся хостов, определяется программное обеспечение компонентов АСУТП и посредством пассивного анализа производится исследование системы на наличие уязвимостей.

2. OSSEC в выбранном режиме предупреждений в режиме реального времени уведомляет специалиста об уязвимостях и категоризирует их уровень критичности. Благодаря этому есть возможность понять, на какую уязвимость надо немедленно обратить внимание.

Проведение аудита в системах мягкого реального времени предполагает следующие действия [4]:

1. При помощи сканера уязвимости SCADA-аудитор проводится анализ имеющихся хостов, определяется ПО компонентов АСУТП и с использованием пассивного анализа производится исследование системы на наличие уязвимостей.

2. OSSEC в выбранном режиме предупреждений в режиме реального времени уведомляет специалиста об уязвимостях и категоризирует их уровень критичности. Тем самым есть возможность понять, на какую уязвимость надо немедленно обратить внимание.

3. Комплексная работа сканера XSpider проводится в три этапа:

— специалист применяет фильтр для выявления всех портов, как действующих, так и случайных и неактивных. Определяется, какие компоненты и сервисы применяются в автоматизированной системе;

— после получения всей информации об инфраструктуре проводится ее исследование на наличие уязвимостей;

— после выявления уязвимостей сканер предлагает решения по устранению;

— также можно применять программу в штатном режиме, назначив расписание сканирования, чтобы постоянно иметь информацию о системе безопасности.

4. Комплекс DATARK работает в нескольких режимах:

— при пассивном мониторинге отсутствует прямое влияние на компоненты, собирает данные в одностороннем порядке;

— при активном мониторинге происходит взаимодействие в формате «запрос — ответ», требующее минимальных вычислительных ресурсов, от компонента АСУТП;

— в случае применения скриптов система рассматривается более детально, ведется анализ непосредственно выбранных специалистом компонентов.

5. Сканер RedCheck проводит следующие аудиты системы:

— аудит уязвимостей проверяет их наличие на выбранных хостах;

— аудит обновлений проверяет актуальность установленного ПО на компонентах и рабочих станциях;

— аудит конфигураций системы автоматизирует контроль установленных параметров безопасности и оценку системы и ее компонентов.

6. Nmap применяется после определения необходимого диапазона хостов. Их необходимо проверить на уязвимости и компоненты, связанные с сетью. Сканирование проводится в несколько этапов. Большинство применяемых методов можно комбинировать друг с другом, разрабатывая универсальный метод сканирования системы. Проводится пингование для определения адресов, выявляются открытые порты. Также есть возможность просканировать протоколы, применяемые в хостах.

7. Nessus производит сканирование с помощью сценариев. Сканировать систему мягкого времени рекомендуется предварительно изученными безопасными сценариями.

Заключение

Для решения поставленной задачи требовалось рассмотреть такой комплекс процедур аудита, который должен был не только выявлять уязвимости автоматизированной системы, но и учитывать риск возникновения временных задержек. Временные задержки могут возникать как по причине нарушенной целостности состояния запроса, так и при проведении аудита различными сканерами уязвимости. Исследуя уязвимости, они нагружают трафик каналов связи, и работоспособность систем реального времени ставится под угрозу.

Представленные особенности модели аудита АСУТП и его сегмента SCADA-систем дает возможность исследовать уровень защищенности с учетом возникновения риска временных задержек. Специалист сможет предварительно ознакомиться с временными параметрами и, опираясь на них, произвести выборку инструментария. Представленный инструментарий позволит выявлять уязвимости с учетом систем реального времени. Опираясь на него, можно произвести аудит, применяя необходимый инструмент и выбранный режим. Также нужно отметить, что аудит ИБ всегда проводится комплексно, с применением нескольких

инструментов. Таким образом, выяснив временные задержки, можно работать со сканерами уязвимости, применяя их определенные режимы, подходящие к системам жесткого или мягкого реального времени.

Список литературы

1. *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 : приказ ФСТЭК России от 14.03.2014 г. №31 (ред. от 23.03.2017 г.). URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 10.08.2021).

2. *Вострецова Е.В.* Основы информационной безопасности : учеб. пособие для студ. вузов. Екатеринбург, 2019. URL: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 01.04.2021).

3. *Втюрин В.А.* Автоматизированные системы управления технологическими процессами. Основы АСУ ТП : учеб. пособие для студ. вузов / Санкт-Петербургская государственная лесотехническая академия им. С.М. Кирова. СПб., 2006.

4. *Хватов Д.А., Ковтун А.И., Подтопельный В.В.* Проблемы аудита информационной безопасности АСУ ТП // Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2019. №4. С. 67—75.

5. *Вериго А.А., Цапко Г.П., Каташев А.С.* Оценка уязвимостей автоматизированных систем управления технологическими процессами // Международный научно-исследовательский журнал. 2016. №11. С. 47—49.

6. *Ветров И.А., Подтопельный В.В.* Особенности подготовки активного аудита информационной безопасности АСУ ТП // Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2021. №1. С. 5—11.

7. *Зюзев А.М., Нестеров К.Е., Головин И.С.* SCADA-системы : учеб. электрон. текстовое изд. Екатеринбург, 2009. URL: https://study.urfu.ru/Aid/Publication/9022/1/Zyuzev_Nesterov_Golovin.pdf (дата обращения: 10.04.2021).

Об авторах

Ольга Васильевна Гальченко — студ., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: ogalcenko3@gmail.com

Владислав Владимирович Подтопельный — ст. преп., Балтийский федеральный университет им. И. Канта; Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «КГТУ», Россия.
E-mail: ionpvv@mail.ru

The authors

Olga V. Galchenko, Student, Immanuel Kant Baltic Federal University, Russia.
E-mail: ogalcenko3@gmail.com

Vladislav V. Podtopelny, Senior Lecturer, Immanuel Kant Baltic Federal University; Baltic State Academy of Fishing Fleet, Russia.
E-mail: ionpvv@mail.ru