УДК 004.056.5:378.3

И. А. Ветров, В. В. Подтопельный

ОСОБЕННОСТИ ПОДГОТОВКИ АКТИВНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП

Рассмотрены проблемы, возникающие на предприятии при постановке задач активного аудита информационной безопасности автоматизированных систем управления технологическими процессами при использовании трансляции данных в режиме реального времени. Указаны особенности методики определения безопасного активного аудита автоматизированных систем управления при их совместной работе с другими системами. Рассмотрены особенности определения параметров безопасного аудита многоуровневых автоматизированных систем управления.

The problems that arise when setting the tasks of active audit of information security of automated control systems for technological processes when using data transmission in real time at the enterprise are considered. The features of the methodology for determining the safe active audit of automated process control systems when they work together with other systems are indicated. The features of determining the parameters of a secure audit of multi-level APCS are considered.

Ключевые слова: аудит, риск, информационная система, автоматизированная информационная система технологических процессов, уязвимость

Keywords: audit, risk, information systems, automated information system of technological processes, vulnerability

Введение

При аудите информационной безопасности (ИБ) инфраструктуры современных производственных предприятий следует учитывать распределение подсистем автоматизированных систем управления технологическими процессами (АСУТП) по функциональным уровням. Аудит активного типа производится при функционировании системы, что может негативно повлиять на скорость передачи данных и работоспособность системных компонентов. Соответственно, из-за специфики среды исследования набор задач и порядок процедур аудита АСУТП будет отличаться от набора задач и порядка, принятого при исследовании безопасности корпоративных информационных систем (КИС), в среде которых ошибки при трансляции допустимы. Кроме того, содержательная часть подобных задач должна включать отдельное рассмотрение угроз, возникающих по отношению к системным сервисам и трафику в режиме производственной эксплуатации АСУ (real-time) при инструментальном поиске уязвимостей.

Определение специфики подготовки безопасного активного аудита информационной безопасности АСУТП

Изначально в соответствии с порядком решения задач аудита перед инструментальным поиском уязвимостей требуется провести комплексное исследование инфраструктуры АСУТП: определить специфику передачи информации, протоколы промышленного типа, способ распределения данных, службы, функционирующие в границах уровней АСУ. Также необходимо распределить системные компоненты и актуальные протокольные среды по выделенным уровням. Обычно выделяют следующие уровни:

— уровень КИС;

— диспетчерский уровень, на котором совмещаются компоненты и протоколы промышленного типа и уровня КИС (сервисы и протоколы семиуровневой модели OSI);

— уровень, на котором используется только компоненты и протоколы обработки промышленных данных (полевой уровень).

Далее необходимо решить следующие задачи [1; 2]:

1. Сбор информации с уровневым разделением (инвентаризация).

2. Поиск уязвимостей (при решении этой задачи предполагается не только анализ транслируемой информации, но и активное воздействие на нее и ее источник). При этом поиск уязвимостей может быть реализован даже в организационной составляющей комплекса ИБ. Процедура активного сбора и аудита технической составляющей предполагает определение:

— будут ли задержки при передаче данных;

— будет ли искажения информации при передаче данных;

— будут ли изменяться настройки систем передачи данных и т. д.

3. Анализ угроз, обнаруженных уязвимостей и вычисление рисков с последующим определением уровня защищенности.

Так как условия проведения аудита ИБ всех уровней инфраструктуры предприятия разные, как и число процедур на различных уровнях АСУТП предприятия, следует выделить две модели аудита:

1) модель аудита, которая относится непосредственно к верхним уровням — модель КИС;

2) модель аудита нижних уровней (три уровня, на которых активно используются промышленные протоколы). Она будет содержать дополнительные задачи, связанные с вычислением успешной реализации процедур аудита и времени его безопасной реализации. На основе анализа полученных в результате вычислений данных необходимо принимать решение о целесообразности применения инструментального поиска уязвимостей и определения меры их эксплуатируемости на рассматриваемых уровнях.

Поскольку основная проблема активного аудита в сетевых системах реального времени связана именно с задержкой передачи данных, то

очевидно, что угрозы, которые существуют в системе, не относятся к типичным видам угроз ИБ (перехват данных, подмена таковых, раскрытие конфиденциальной информации). Основными угрозами при активном аудите являются именно возникновение не предполагаемой алгоритмом протокола задержки пакета данных или появление недопустимых периодов прерывания трансляции, которые препятствуют передаче данных в режиме real-time, вызывая их запаздывание, недопустимое по технологическим спецификациям уровня АСУТП. Поскольку воздействие активного аудита приводит к тем же результатам, что и целенаправленная атака, то их можно отождествить с той лишь разницей, что тип угрозы при аудите заранее известен и по способу реализации неизменен. Соответственно, перед проведением аудита требуется рассмотреть проблемы возникновения рисков прерывания трансляции технических данных, которые могут привести к повреждению системы и, соответственно, прекращению самих процедур аудита.

Таким образом, этапы анализа будут включать не только выявление угроз и уязвимостей, определение рисков, но и предварительный анализ безопасности процедуры аудита на основе априорных оценок рисков возникающего при исследовании систем АСУТП негативного воздействия инструментария исследования. Это является отличительной особенностью реализации активного аудита в системах реального времени (разного типа) на предприятиях с распределенными функциональными уровнями АСУТП. Соответственно, в список задач требуется внести дополнительную задачу определения безопасности процедур поиска уязвимостей и инвентаризации системных сервисов исследуемой инфраструктуры.

Поскольку угроза при процедуре аудита была определена как временной период, за который система утрачивает функциональность, необходимо подобрать такую модель расчета успешности аудита, которая будет учитывать специфику используемых параметров, то есть позволит вычислить вероятность появления задержки при передаче данных, период ее существования и период штатного функционирования системы при активном аудите. Такая модель может быть основана на методике определения надежности функционирования систем.

Предполагается, что период, учитываемый в расчетах, охватывает время сканирования инфраструктурных компонентов. Любая задержка трансляции информационных пакетов промышленных протоколов типа CAN, ModBus, HART приводит к нарушению режима работы real-time и, соответственно, будет считаться отказом (поскольку переданная информация не пришла к адресату вовремя в соответствии со спецификацией протокола) [3]. Тогда интенсивность отказов будет трактоваться как интенсивность (среднее число) фиксаций задержек при передаче данных в процессе активного аудита ИБ в режиме real-time. Несмотря на то что угрозы задержек трансляции на каждом уровне типологически тожественны, длительность задержки, которая будет являться критичной, для каждого уровня будет своя. Соответственно, интен-

сивность отказа системы передачи данных по промышленным протоколам равна сумме интенсивностей задержек фиксируемых при аудите на каждом уровне АСУТП и рассчитывается по следующей формуле [6]:

$$A = \sum_{i=1}^{n} a_i , \quad (1)$$

где A — интенсивность отказа системы передачи данных по промышленным протоколам; a_i — интенсивность задержек при аудите.

Таким образом, вероятность $p(t)$ исправной работы в течение интервала времени проведения аудита t с учетом интенсивности отказов, то есть задержек при передаче данных, определяется так:

$$p(t) = e^{-a_i} . \quad (2)$$

Учитывая уровневую сегментацию АСУТП, можно рассчитать для каждого уровня вероятность исправной работы и вычислить вероятность исправной работы в целом для системы, суммируя показатели всех существующих на производстве систем, связанных с передачей данных в режиме real-time, и таким же образом вычислить среднее время работы взаимосвязанных систем АСУТП.

Однако с учетом связанности уровней инфраструктуры необходимо рассматривать влияние функционала одной подсистемы на работоспособность других. Поскольку это влияние определяется спецификой промышленных протоколов и служб, показатель вероятности исправной работы должен отражать специфичность данных взаимосвязей и взаимозависимостей. С другой стороны, учитывая технологическую специфику рассматриваемых уровней (три нижних уровня АСУТП технологически схожи), их можно объединить в единый сегмент. Решение рассматривать подсистемы реального времени как единый сегмент или как несколько взаимосвязанных зависит от специфики распространения протокольных сред и системных сервисов на следующих уровнях АСУТП [5]:

— уровень диспетчерского управления;

— уровень автоматического управления и полевого управления.

Использование промышленных протоколов между уровнем диспетчерского управления и уровнем автоматического управления, уровнем автоматического управления и полевого управления подразумевает наличие взаимосвязей между их службами.

Далее необходимо рассмотреть промежуток времени между двумя задержками при передаче пакетов по промышленным протоколам. Данный параметр является показателем времени успешной работы системы при активном аудите до первого отказа (задержки), обозначается как «наработка на отказ трансляции данных при активном аудите и инвентаризации сетевых сервисов» (H) и рассчитывается по следующей формуле [6]:

$$H = \frac{1}{A} . \quad (3)$$

Для каждого уровня АСУ этот показатель рассчитывается отдельно. Однако если рассматривать два нижних уровня как единый сегмент автоматизированной системы, то и время наработки на отказ будет единым для данной сборки уровней. Таким образом, можно выяснить время успешной работы систем аудита и инструментария инвентаризации сетевых сервисов без прерывания трансляции данных, возможные периоды возникновения проблем с передачей данных и вероятность возникновения этих проблем в период активной эксплуатации промышленных протоколов в режиме real-time.

Поскольку в состоянии системы «как есть» (as-is) параметр времени восстановления H_r будет оцениваться как время, которое потребуется для возобновления режима real-time, то, соответственно, данный параметр не следует рассматривать как показатель нивелирования канала несанкционированного доступа (НСД). В данном случае возникновения угроз НСД, в отличие от параметров вычислительной модели риска, рассматривается всего одна угроза (задержка трансляции данных), которая хорошо известна и перекрывается простым отключением инструментов исследования подсистем АСУТП. При этом система в режиме real-time (в соответствии с моделью) возобновит свою работу так же, как если бы возобновляла свою работу система защиты, при условии того что она была бы повреждена. Это позволяет определить коэффициент готовности возобновления трансляции данных с требуемой скоростью и выявить, насколько этот коэффициент соответствует тому показателю, который означал бы возможность возобновления работы системы без каких-либо критических ее повреждений. Таким образом, коэффициент готовности системы возобновить трансляцию и работу в целом без критических повреждений является ключевым показателям в модели расчетов:

$$K_w = \frac{H}{\left(H - Hr\right)}. \tag{4}$$

Соответственно, можно вычислить также коэффициент неготовности K_{nw} системы к возобновлению трансляции данных в режиме реального времени:

$$K_{nw} = 1 - K_w. \tag{5}$$

Совмещение работы систем в режиме real-time и работы в виртуальном режиме возможно на одном уровне АСУ предприятия. Поэтому всегда следует дифференцированно подходить к вопросу определения допустимого времени прерывания трансляции данных и количества задержек (нужно знать точно компонентный состав анализируемого оборудования, его характеристики, спецификации протокольных сред).

При выявлении специфики активного аудита и порядка его проведения предварительно не требуется анализировать модель нарушителя

и применять таковую при обработке собранных данных. Это существенно облегчает работу по подготовке процедур безопасного активного исследования подсистем АСУТП при их непосредственной эксплуатации.

Выводы

Таким образом, перед проведением активного аудита АСУТП, работающих на диспетчерском, полевом и других уровнях, компоненты которых используют промышленные протоколы, требуется решить ряд дополнительных задач. Первоначально следует разделить АСУ предприятия на уровни, использующие и не использующие реальный режим. Затем необходимо проанализировать исследуемые системы и определить специфику (допустимость) проведения активного аудита. В процессе анализа нужно определить вероятность успешной работы системы при использовании инструментария аудита (ключевой параметр), допустимое время задержки с учетом спецификаций промышленных протоколов, время успешной работы аудита до возможного первого отказа. Последний параметр необходим для создания специальной методики активного аудита, которая будет ориентироваться на допустимые периоды тестирования в соответствии с технологическими спецификациями промышленных протоколов АСУТП. В системах с мягким режимом real-time минимальные задержки допустимы. Поэтому следует применять методику тестирования с учетом времени восстановления скорости трансляции данных и работы сервисов, которое не должно превышать периода отсутствия информационных пакетов в канале передачи данных. Для более точного определения этих параметров требуется определить еще один ключевой параметр — коэффициент готовности системы возобновить трансляцию.

Список литературы

1. *Аверичников В.И., Рытов М.Ю., Кувылкин А.В., Рудановский М.В.* Аудит информационной безопасности органов исполнительной власти : учеб. пособие. М., 2011.

2. *Астахов А.* Введение в аудит информационной безопасности : доклад // GlobalTrust Solutions. 2018. URL: http://globaltrust.ru (дата обращения: 29.01.2018).

3. *Большев А., Чербов Г., Черкасова С.* Компоненты DTM: тайные ключи к королевству АСУ ТП / Исследовательский центр DigitalSecurity. М., 2014.

4. *Горбачев И.Е., Глухов А.П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры // Тр. СПИИРАН. 2015. Вып. 1 (38). С. 112—135.

5. *Макаренко С.И.* Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (дата обращения: 15.01.2021).

6. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. СПб., 2004.

Об авторах

Игорь Анатольевич Ветров — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: vetrov.gosha2009@yandex.ru

Владислав Владимирович Подтопельный — ст. преп., Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «КГТУ», Россия.
E-mail: ionpvv@mail.ru

The authors

Dr Igor A. Vetrov, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: vetrov.gosha2009@yandex.ru

Vladislav V. Podtopelny, Assistant Professor, Baltic State Academy of Fishing Fleet, Russia.
E-mail: ionpvv@mail.ru