УДК 004.056.5:378.3

Д. А. Хватов, А. И. Ковтун, В. В. Подтопельный

ПРОБЛЕМЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП

Рассмотрены проблемы, возникающие при постановке задач в процессе проведения аудита информационной безопасности автоматизированных систем управления технологическими процессами на предприятии. Указаны особенности аудита автоматизированных систем управления технологическими процессами при их совместной работе с другими системами, актуальные для АСУ ТП критерии безопасности. Приведены и охарактеризованы разновидности аудита многоуровневых информационных систем со встроенным АСУ ТП, проанализирована их пригодность для различных классов проверок.

The problems that arose during the formulation of tasks and during the audit of information security of automated process control systems at the enterprise were studied. Features of the audit of automated process control systems during their joint work with other systems are indicated. Safety criteria relevant to the process control system are considered. The types of audit of multi-level information systems with integrated process control systems are presented and characterized, their suitability for various classes of checks is analyzed.

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

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

Современные комплексы информационной безопасности автоматизированных систем управления технологическими процессами, применяемые в технологических сетях различных предприятий с критической инфраструктурой, должны создаваться с учетом требований существующих стандартов и руководящих документов, изданных государством (руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденный ФСТЭК России 18 мая 2007 г., приказ ФСТЭК России №31 от 14 фев. 2014 г. и др.). Перед внедрением подобных комплексов требуется произвести аудит инфраструктуры предприятия. При этом процедуры аудита должны строиться с учетом указанных в документах требований. Однако специфика организации АСУ ТП не всегда делает доступными методы исследования, которые применяются при аудите корпоративных информационных систем, основанных на современной архитектуре клиентско-серверного типа.

Для достижения целей аудита (выявление уровня защищенности информационных блоков и подсистем АСУ ТП предприятия) превентивного (определение угроз и уязвимостей) и детектирующего характера требуется решить ряд задач:

— произвести поиск уязвимостей различными методами;

Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2019. № 4. С. 67 – 75.

— анализировать риски;

— оценить уровень защищенности системы в состоянии «as is»;

— определить наличие соответствия существующим стандартам ИБ и выработать ряд рекомендаций по повышению уровня защищенности [1; 2].

Для решения поставленных задач необходимо провести исследование технических систем (для определения их надежности) и организационной составляющей, в дальнейшем рассмотреть их комплексно с возможным использованием тестирования на проникновение.

При этом требуется учитывать особенности архитектуры АСУ ТП: системы и подсистемы, созданные на основе различных технологий, объединяются в одну. Это значит, что подсистемы диспетчерского контроля и полевого применения должны быть связаны с информационными подсистемами административного управления. Поэтому методы решения поставленных задач аудита будут отличаться в зависимости от свойств исследуемых подсистем на разных уровнях, а именно:

— организации и бизнес-процессов;

— систем управления (менеджмента) и корпоративных информационных систем;

— технических систем.

При этом часть системы подобного рода, за счет эксплуатации полевого уровня, может работать в реальном режиме времени. Он может совмещаться с виртуализированной обработкой данных на уровнях общего управления. Поэтому процедуры аудита, связанные с реализацией активного исследования, будут различаться в зависимости от технологических основ подсистем. Кроме того, нужно учитывать особенности технического обеспечения — контуры управления, которые представлены как автоматизированными системами, так и автоматическими. Очевидно, в таких системах не всегда возможно реализовать тестирование. При этом вывяленные результаты требуется рассматривать, используя методологии вычисления и анализа рисков с учетом особенностей исследуемых подсистем и уровней анализируемого объекта. Таким образом, первое затруднение, с которым сталкивается аудитор на предприятии с внедренным АСУ ТП, — это создание модели аудита, учитывающей при реализации процедур проверки все технологические различия подсистем, объединенных в едином комплексе. Соответственно, чтобы разработать модель аудита, требуется предварительно отдельно создавать формальные описания объектов разного уровня (уровни КИС, АСУ ТП), описания актуальных угроз, и отдельно определять процессы аудита для каждого сегмента инфраструктуры предприятия. Подобным образом формируется модель аудита.

В модели следует учитывать следующие уровни и сегменты:

— уровень планирования;

— уровень управления;

— уровень диспетчерского управления;

— уровень автоматического управления;

— полевой уровень.

Необходимо отметить, что фактически формируется две модели аудита (при описании в том числе актуальных угроз). Очевидно, будут резкие отличия моделей аудита уровней, относящихся к планированию и управлению производством, от моделей уровней и сегментов АСУ ТП (эти отличия могут быть также связаны с определенными правилами передачи и обработки данных уровней системы). Это означает, что будут прослеживаться разные подходы к проведению аудита в разных сегментах системы предприятия.

Разность подходов к аудиту обусловлена и тем, что важную для систем корпоративного уровня контролируемую информацию можно обработать стандартными методами, в то время как данные ПЛК, серверов АСУ ТП, измерительные, сигнализационные данные — то есть информацию, поставляемую в режиме реального времени — следует анализировать, используя специальное оборудование и программное обеспечение, способное разбирать и интерпретировать пакеты данных протоколов промышленного типа. Соответственно, критерии оценки критичности информации различных уровней АСУ ТП будут также различаться, как и методы анализа и оценки информации, что сказывается на выборе общего теоретического подхода к проведению аудита.

Особенности работы с АСУ ТП проявляются уже при подготовке к проведению аудита, когда требуется предварительно собрать информацию об уязвимостях в системе из открытых источников. В соответствии с делением на типы сегментов делятся и классы уязвимостей:

— уязвимости уровня MES и схожие с ними (связаны операционными средами и средствами, программным обеспечением, передачи данных на основе стека протоколов TCP/IP);

— уязвимости уровня АСУ ТП, в том числе SCADA-систем, если они присутствуют, и уязвимости полевого уровня (для выяснения этого можно использовать специализированные банки данных: ICS-CERT, NVD/CVE, SCADA Strangelove, SiemensProduct CERT).

При проведении инвентаризации требуется учитывать наличие клиентско-серверной модели, актуальной для всех уровней инфраструктуры предприятия со встроенным АСУ ТП. Это предполагает в большинстве случаев применение стека протоколов TCP/IP (при активном аудите, как правило, проблем с поиском уязвимостей в силу распространенности не возникает). Иная ситуация складывается с протоколами нижних уровней (уровень автоматического управления, полевой уровень). Здесь сосредоточены как средства, принадлежащие к верхним уровням, так и компоненты контроля элементов полевого уровня со своим спектром решений в области трансляции данных. Требуется избирательный подход. На границе нижних и верных уровней могут находиться технологические решения со своей структурной спецификой, сопрягающие эти технологии (различные решения SCADA, OPC-серверы).

Если компоненты подсистем среднего и полевого уровня строго локализованы, то компоненты верхних уровней могут быть распределены. Поэтому при инвентаризации ресурсов и активов предприятия с АСУ ТП отдельно следует учитывать различные средства межуровнево-

го сопряжения по трафику и средства изолирования компонентов одного уровня от другого. Это необходимо будет реализовать, чтобы четко понимать границы аудита технологической сети с ее специфическими правилами функционирования и корпоративной сети со стандартизированной структурой организации компонентов систем.

Фактически диспетчерский уровень не только выступает в роли управляющего компонента, но и выполняет функции межуровневого и межсистемного шлюза. Поэтому при анализе угроз его целесообразно рассматривать отдельно, учитывая возможности схождения в нем разноуровневых уязвимостей при реализации атак на других уровнях.

Угрозы у перечисляемых уровней и сегментов разные, поэтому при аудите вызывает затруднение описание ассоциативных связей угроз и инвентаризируемых компонентов. Это, в свою очередь, влияет на порядок проведения аудита. В этом случае процесс обследования, который разделяется на два этапа (заочное, то есть по полученным от организации сведениям о программной и технологической базе, и очное обследование всех уровней систем обработки информации) будет ограничен. Во-первых, заочный аудит неприменим к технологической сети из-за специфики ее функционирования. Во-вторых, методы интенсивного исследования, то есть методы pen-теста, могут нанести непоправимый ущерб подсистемам АСУ ТП, что в итоге обессмыслит весь процесс аудита.

И с этих позиций активный аудит (если он, конечно, возможен) будет весьма избирателен. Это может поставить под сомнение объективность исследования. Кроме того, полученные результаты нельзя экстраполировать на компоненты технологической сети в силу их ограниченной достоверности: они буду свидетельствовать о состоянии конкретного ресурса отдельного сегмента.

Соответственно, в модель аудита требуется отдельно внести сегменты и компоненты, которые на этапе активного аудита можно использовать в качестве целевых ресурсов, и особо отметить те, которые не стоит подвергать воздействию. Для них должна быть выбрана другая методика, без агрессивного воздействия или предполагающая использование стендовых решений. Поскольку правила и критерии определения работоспособности подобных систем отличаются от распространенных систем на основе стека IP/TCP, следующей проблемой становится определение критериев нарушения в технологической сети. Основным показателем реализации угрозы являются задержки при трансляции пакетов с техническими данными или в работе комплекса программно-аппаратной платформы. Они могут свидетельствовать как о появлении паразитной нагрузки на трафике, так и о воздействии на сегменты, участвующие в трансляции, внешних источников или о несогласованности работы скомплектованного оборудования, что уже не является областью ИБ. В этом случае процесс аудита будет осложнен дополнительными процедурами из-за потребности отличать признаки собственно технических неисправностей и признаки проявления инцидента ИБ, которые в технологической сети, на диспетчерском и полевом уровне схожи.

Эти особенности влияют на формирование модели нарушителя при ее формализации, в том числе на формирование критериев нарушения, что необходимо при реализации аудита и сценариев действий нарушителей различных категорий.

При решении вопросов активного аудита можно использовать уровневую модель дифференциации систем управления АСУ предприятия (при выявлении уязвимостей). При моделировании атак могут помочь наборы известных эксплойтов (SAINTexploit, MetasploitFramework, ImmunityCanvas).

Отдельно стоит обратить внимание на возможное наличие уязвимости систем и интерфейсов управления операторских АРМ (автоматизированных рабочих мест). Системы диспетчерского уровня функционируют на основе клиентско-серверной архитектуры. При этом клиентами серверной части могут являться как компоненты того же уровня, так и верхних уровней, включая службы удаленного управления и контроля технологических процессов. Это означает, что технология тонких клиентов и удаленных рабочих столов широко распространена на современных предприятиях. На этом уровне возможна установка стандартных средств защиты информации, в том числе системы фильтрации трафика и шифрования передаваемых данных. Однако ее применение приводит к задержкам при передаче данных технологического характера как внутри управляемого сегмента, так и при передаче технической информации за его пределы. Более того, могут использоваться веб-интерфейсы для доступа к управляющим компонентам на месте осуществления технических операций. Поэтому при аудите трафик и элементы, информация от которых должна поставляться на АРМ (в том числе удаленные) фактически в режиме реального времени, как и доступ к технологической сети самих АРМ, целесообразно отделять от остального массива компонентов системы предприятия.

Соответственно, требования к процедуре и критерии безопасности необходимо корректировать всякий раз при столкновении с новой технологической базой. Это, в свою очередь, осложняет расчет рисков при формировании итогового отчета. Вдобавок, сопоставление разноуровневых уязвимостей и угроз будет носить гипотетический характер. Поэтому требуется, чтобы методика практического анализа результатов аудита отражала специфику исследуемого объекта. В целом можно использовать комбинирование анализа рисков и анализа стандартов ИБ — при условии, что эти стандарты безопасности с учетом специфики технологий (в том числе зарубежных) применимы, существуют или являются актуальными. Это сужает возможности аудита на соответствие стандартам и, наоборот, расширяет поле анализа на основе аудита рисков. При этом нужно четко понимать и ограничивать возможности тестовой компрометации узлов сети, в соответствии с требованиями обеспечения надежности ее работы в реальном времени. Это также сужает поле применения методик анализа рисков.

Такой проблемы не возникает, когда выполняются задачи аудита по отношению к административному уровню. На нем требования к информации по скорости передачи существенно ниже (к ней можно отнести информацию административного уровня). Кроме того, нужно учитывать наличие на ЭВМ статических наборов данных, представленных в виде архивов и конфигурационных файлов. Контроль целостности можно осуществлять периодически.

Принимая во внимание специфичность предъявляемых к технологической сети требований, целесообразно первоначально проводить тестирование на устойчивость к отказам при помощи наблюдения за ее работой в конечном наборе специально выбранных ситуаций. При этом тесты должны быть четко дифференцированы по возможностям воздействия на состояние системы. Вызывающие подозрения должны проводиться на специально сформированном стенде. Таким образом, еще одним осложнением, возникающем при аудите, является создание специализированных лабораторных стендов, учитывающих специфику технологической сети конкретного предприятия. Можно выделить следующие задания, связанные проверкой на стенде устойчивости системных компонентов:

— проверка надежности обеспечения управления питанием энергосети;

— проверка надежности обеспечения работоспособности интерфейсов и терминалов защиты;

— проверка надежности обеспечения управления техническими устройствами нижнего уровня системы управления с возможным последующим повреждением (обход, модификация блокировок; передача недокументированных, запрещенных команд) [7].

Тестовые испытания направлены на проверку требований к исследуемой системе. Используемые задачи в тестах должны обеспечивать проверку всех возможных вариантов поведения технологической сети и ее компонентов, иначе выводы о качестве системы, сделанные на основе проведенного тестирования, будут недостоверны [6].

Тестирующие задания легче всего построить и классифицировать на основе функций компонентов системы. Функции могут быть такими:

— контроль состояния компонентов технологической сети, отображение данных в процессе контроля (в том числе применение графических и иных средств отображения процесса контроля);

— регистрация и архивация данных по рабочим процессам технических компонентов;

— оповещение о различных событий с учетом передачи данных через модемы;

— контроль распределения прав доступа пользователей на различных уровнях технологической сети;

— формирование отчетов с учетом эксплуатации серверов АСУ ТП, SCADA-систем, OPC-серверов;

— трансляция данных по протоколам HTTP, HTTPS;

— использование файлов XML-формата для трансляции данных и их хранения [7].

Если рассматривать аудит по структуре АСУ ТП, то на технологическом уровне при активном аудите целесообразно применять модульное (компонентное) тестирование. Оно позволяет проверить безопасность функционирования отдельно взятого элемента исследуемого объекта (программного или аппаратного модуля, подпрограммы, отработки должностных обязанностей по защите информации отдельным должностным лицом и т.д.). Методика определения рисков в этом случае будет наиболее выгодна, поскольку позволит проанализировать покомпонентно состав сегмента системы и, более того, учесть последовательность поэтапного воздействия на анализируемый компонент при его тестовой компрометации. Особенно хорошо данная методика проявляет себя при работе с испытательными стендами. Учесть системные связи межуровневого характера при использовании тестового стенда можно только в редуцированном виде.

Таким образом, межуровневый характер отношений сегментов и компонентов технологической сети можно проследить в аудите, используя интеграционное тестирование (взаимодействие между элементами объекта проверяется путем реализации методов тестирования «сверху вниз», «снизу вверх», распределения потоков управления и данных и т.д.) [6]. Однако состав сети и требования по непрерывной трансляции технических данных ограничивают данный метод в практике применения только теми компонентами сети, тестирование которых не вызовет коллизий (число и тип подобных компонентов определяется при подготовке к «активному» аудиту).

Для получения целостного представления о состоянии компонентов проверяемой инфраструктуры требуется использовать системное тестирование, которое охватывает весь объект и его внешние интерфейсы, а также среду функционирования. Однако в силу разности технических платформ и особенностей требований к надежности компонентов технологической сети осуществить системное тестирование чрезвычайно трудно.

Чтобы подробнее проанализировать программные компоненты системы на предмет определения особенностей и подходящих режимов тестирования, предварительно необходимо их классифицировать по следующему критерию: в каком направлении движется исходящий сигнал от компонента среднего уровня. Данные, направленные на нижние уровни, принадлежат медленному трафику, а направление потока данных указывает на потенциальные системные узлы и сервисы, которые окажутся в поле интересов злоумышленника, действующего извне.

Таким образом, при аудите АСУ ТП возникает много затруднений. Во-первых, это сложность создания модели аудита, в которой необходимо учесть все технологические особенности различных подсистем. Во-вторых, использование разных подходов к проведению аудита в технологически отличных сегментах системы предприятия. Более того, требования к процедуре и критерии безопасности корректируются при столкновении с новой технологической базой. В-третьих, критерии

оценки критичности информации различных уровней АСУ ТП будут также различаться. В модели аудита нужно учитывать отдельно те сегменты и компоненты, которые на этапе активного аудита не стоит подвергать воздействию, что налагает ограничения на процедуру тестирования.

В целом процедура аудита АСУ ТП сегментов предприятия характеризуется чрезвычайной требовательностью к описанию и определению практик аудита фактически каждого сегмента системы и, в частности, компонент технологической сети.

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 // 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 // Zero Nights. 2014.

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

5. *Котенко И.В.* Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. 2004. №1. С. 56—72.

6. *Макаренко С.И.* Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1. С. 1—29.

7. *Подтопельный В.В.* Особенности аудита информационной безопасности АСУ ТП V // Прикладная радиофизика, радиотехника и информационная безопасность (21—27 мая) : матер. Междунар. науч. конф. Калининград, 2017. С. 513—518.

8. *Резников Ю.Г.* Построение эффективных систем информационной безопасности АСУ ТП на базе комплексного подхода // Технологии безопасности. 2012. №2. С. 46—49.

9. *Farsi M., Barbasa M.* CANopen Implementation Applications to Industrial Networks. Research Studies Press, 2000.

Об авторах

Дмитрий Александрович Хватов — начальник управления криптографической защиты информации, ГАУ КО «Калининградский государственный научно-исследовательский центр информационной и технической безопасности», Россия.

E-mail: hvatov-dmitrii@mail.ru

Алексей Игоревич Ковтун — директор ООО «Центр защиты информации», Россия.

E-mail: czi@baltzi.ru

Владислав Владимирович Подтопельный — ст. преп., Балтийская государственная академия рыбопромыслового флота, Россия.

E-mail: ionpvv@mail.ru

The authors

Dmitry A. Khvatov, Head of the Department of Cryptographic Information Security, Kaliningrad State Research Center of Information and Technical Security, Russia.
E-mail: hvatov-dmitrii@mail.ru

Alexey I. Kovtun, Director of the LLC «Center for Information Security», Russia.
E-mail: czi@baltzi.ru

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