УДК 004.054

А.С. Марковский[1]
А.П. Киреев[2]
М.Д. Санин[3]

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Данная статья посвящена проблеме обеспечения аудита информационной безопасности и предлагает комплекс мероприятий, повышающий уровень защищенности систем управления критически важных объектов.

Ключевые слова: *информационная безопасность, аудит, уровень защищенности.*

A.S. Markovsky
A.P. Kireev
M.D. Sanin

THE TECHNIQUE OF CARRYING OUT AUDIT OF INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS OF CRITICAL INFRASTRUCTURE

This article is devoted to the problem of ensuring information security audit and offers a range of activities that enhance the security of the control systems of critical infrastructure.

Keywords: *information security, audit, security level.*

Широкое внедрение систем информационных технологий, являющихся одним из компонентов, поддерживающих цели деятельности критически важных объектов (КВО), обеспечивая их эффективное и бесперебойное функционирование, также привело к необходимости реализации решений по обеспечению информационной безопасности (ИБ). Для того чтобы оценить уровень безопасности автоматизированной системы управления (АСУ) КВО и впоследствии построить эффективную систему защиты информации, проводится целый комплекс мероприятий, называемых аудитом ИБ.

В то же время, для того чтобы сделать компетентные выводы относительно уровня защищенности АСУ КВО, аудитору потребуется наличие всех необходимых исходных данных. Их получение осуществляется в ходе информационного и инструментального обследования.

Вместе с тем, в стране отсутствует единая система взглядов на государственное регулирование процессов аудита ИБ. В настоящее время существует ряд частных организаций, предлагающих услуги по проведению аудита ИБ. В то же время, в отсутствие необходимых национальных регуляторов такая деятельность может нанести непоправимый вред. Ранее были рассмотрены [1] наиболее распространенные методики аудита ИБ, проведен их анализ, представлены сравнительные характеристики (табл. 1).

Исходя из проведенного анализа, а также сложившихся условий отсутствия правового и методического обеспечения аудита ИБ, возникла необходимость разработки собственной методики информационного обследования объекта аудита АСУ КВО, учитывающих цели, задачи обследования и уровни ИБ, с одной стороны, и специфику деятельности КВО, особенности функционирований, топологии самих АСУ КВО – с другой.

[1] Кандидат технических наук, старший научный сотрудник Военно-космической академии им. А.Ф. Можайского.

[2] Старший научный сотрудник Военно-космической академии им. А.Ф. Можайского.

[3] Научный сотрудник Военно-космической академии им. А.Ф. Можайского.

Таблица 1

Сравнительные характеристики различных стандартов оценивания ИБ

	Уровни ИБ	Структурированность	Подход
ГОСТ 15408	технический	11 классов, 61 семейство функциональных требований, 7 классов, 26 семейств требований доверия	системный, функциональный
СТО БР ИББС	организационный	3 группы, 32 групповых показателя, 237 частных показателей	процессный
ISO 17799/ 27001	организационный, процедурный	11 разделов, 133 требования	процессный
BSI	организационный, технический	5 групп, 46 объектов контроля	функциональный
NIST	организационный, процедурный, технический	3 класса, 17 семейств, 163 меры контроля	функциональный
COBIT	организационный, процедурный	4 домена, 34 цели контроля, 318 средств контроля	процессный

Взаимная детализация каждой из рассматриваемых деятельностей позволяет определить основные элементы в основной деятельности КВО, контроль которых на основе методики аудита ИБ обеспечит основу для оценки эффективности внедряемых организационных и технических мероприятий по защите информации.

Методика информационного обследования объекта аудита АСУ КВО состоит из следующих основных этапов (рис. 1).

Рис. 1. Методика информационного обследования объекта аудита АСУ КВО

Этап определения уровней ИБ и критичных ресурсов объекта аудита

Для этого на основе процессного подхода [2] построена обобщенная модель взаимосвязи деятельности по обеспечению ИБ и основной деятельности КВО (рис. 2). Определение уровней ИБ $Y = \{y_1, y_2, y_3\}$ основывается на целях аудита и требованиях руководства, что, в свою очередь, позволит нам сформировать методику сбора и обработки информации об объекте аудита.

Объект аудита может быть представлен в виде множества взаимосвязанных ресурсов $X = \{x_i\}$,

формально представленных в виде $x_i \in X$, где X – множество ресурсов АС, $i \in 1\ldots n$, а n – общее количество ресурсов.

В соответствии со стандартом ISO 17799-2005 [4], ресурсы организации с точки зрения ИБ можно разделить на информационные, физические, программные, сервисные, кадровые и нематериальные. Анализ критичности ресурсов должен выявить ресурсы, наиболее критичные с точки зрения ИБ.

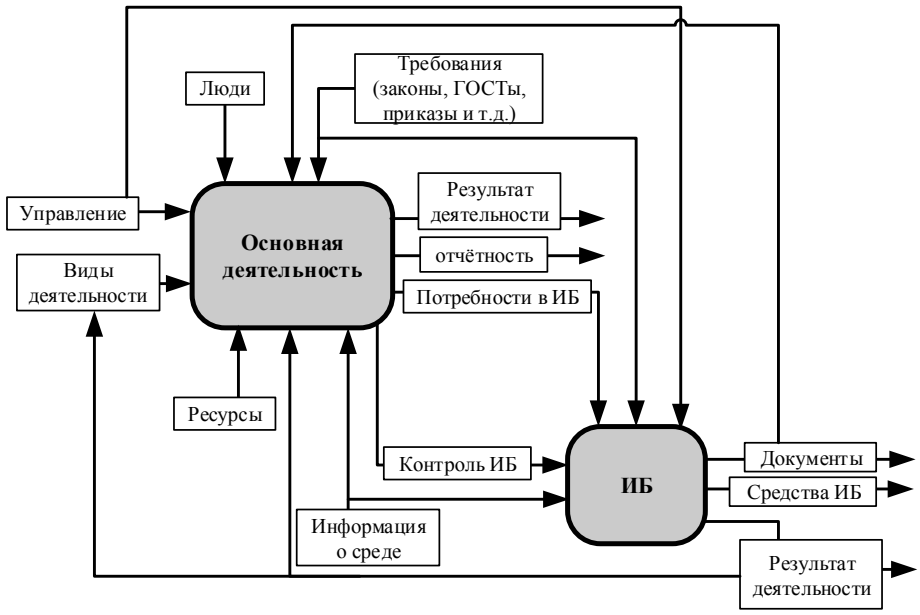

Рис. 2. Модель взаимосвязи деятельности по обеспечению ИБ и основной деятельности КВО

С помощью построенной модели стало возможным провести детализацию каждой деятельности КВО (рис.2), что, в свою очередь, позволило определить критичные ресурсы объекта аудита $X^j = \{x_i^j\}$, $i \in 1\ldots n$, $j \in 1\ldots l$, l – общее количество критичных ресурсов.

Из-за большого количества разнообразных ресурсов в ряде случаев удобнее их сгруппировать по функциональному назначению, принадлежности или местоположению. Серверы и рабочие станции рассматриваются в комплексе с установленным на них программным обеспечением (ПО), реализуемыми сервисами, хранящейся информацией в файлах и базах данных – соответственно как серверные ресурсы и автоматизированные рабочие места (АРМ). Также в качестве комбинированных ресурсов рассматриваются АСУ с используемым аппаратным и программным обеспечением (ПО), прикладными системами, файлами и базами данных. Одна АСУ может включать в свой состав несколько физических (серверы, АРМ), программных (прикладное ПО) или информационных ресурсов (базы данных, файлы).

Все ресурсы объекта аудита ИБ предлагается разбить в соответствии со следующей **иерархией уровней** [3].

1. Нормативно-документационный уровень.
2. Организационно-управленческий уровень.
3. Уровень прикладных систем.
4. Уровень систем управления базами данных (СУБД).
5. Уровень операционных систем и общесистемного ПО.
6. Уровень сетевых сервисов и приложений.
7. Сетевой уровень.
8. Физический уровень.

Этап определения соответствия ресурсов объекта аудита $X = \{x_i\}$ областям контроля $Q = \{q_1 \ldots q_{10}\}$

Для контроля состояния ресурсов объекта аудита можно выделить области контроля информационной безопасности (ИБ). Области контроля охватывают группы взаимосвязанных вопросов в области ИБ. Исходя из имеющейся практики стандартизации, они не обязательно должны соответствовать одному из иерархических уровней ресурсов объекта аудита. Часть ресурсов разных уровней может входить в одну область контроля.

Выделяются следующие ***области контроля*** [4].

1. Нормативно-документационное обеспечение ИБ.

2. Организационно-управленческое обеспечение ИБ.

3. Организация физической защиты элементов инфраструктуры АСУ.

4. Инвентаризация и классификация (категорирование) ресурсов.

5. Защита периметра АСУ и организация доступа пользователей в сети структурных подразделений.

6. Безопасность сетевой инфраструктуры.

7. Администрирование безопасности информации внутри АСУ.

8. Контроль доступа к информации.

9. Обеспечение безопасного функционирования АСУ.

10. Разработка, внедрение и сопровождение АСУ.

В рамках каждой области контроля разрабатывается контрольный список требований и рекомендаций, которые проверяются в ходе проведения аудита. В составе контрольных списков могут быть вопросы двух типов:

– вопросы-требования, имеющие определенный вес, ответы на которые и напрямую влияющие на оценивание показателей уровня ИБ в зависимости от степени соответствия требованию (соответствует, не соответствует, частично соответствует);

– вопросы информационного характера, необходимые для дальнейшей работы аудитора по сбору свидетельств аудита и косвенно влияющие на оценивание показателей уровня ИБ.

Для проверки состояния информационной безопасности ресурсов объекта аудита последние необходимо охватить в проверяемых вопросах контрольных списков по областям контроля.

Можно предложить следующую обобщенную матрицу соответствия иерархического уровня проверяемых ресурсов областям контроля (табл. 2).

Таблица 2

Матрица соответствия иерархического уровня проверяемых ресурсов областям контроля

Уровень ресурса (*X*) / **Область контроля (*Q*)**	**Нормативно-документационный уровень**	**Организационно-управленческий уровень**	**Уровень прикладных систем**	**Уровень систем управления базами данных**	**Уровень операционных систем и общесистемного ПО**	**Уровень сетевых сервисов и приложений**	**Сетевой уровень**	**Физический уровень**
1. Нормативно-документационное обеспечение ИБ	+							
2. Организационно-управленческое обеспечение ИБ	+	+						
3. Организация физической защиты элементов инфраструктуры АСУ		+					+	+
4. Инвентаризация и классификация (категорирование) ресурсов	+	+	+	+	+	+	+	+
5. Защита периметра АСУ и организация доступа пользователей во внешние сети	+					+	+	
6. Безопасность сетевой инфраструктуры						+	+	+
7. Администрирование безопасности информации внутри корпоративной сети			+	+	+	+		
8. Контроль доступа к информации	+	+	+	+	+	+	+	+
9. Обеспечение безопасного функционирования АСУ		+	+		+	+	+	+
10. Разработка, внедрение и сопровождение автоматизированных систем управления	+	+	+					+

На этапе сбора информации о состоянии ИБ объекта аудита АСУ КВО продолжается более подробный сбор и анализ информации. Методика сбора информации основывается на ряде требований (рис. 3).

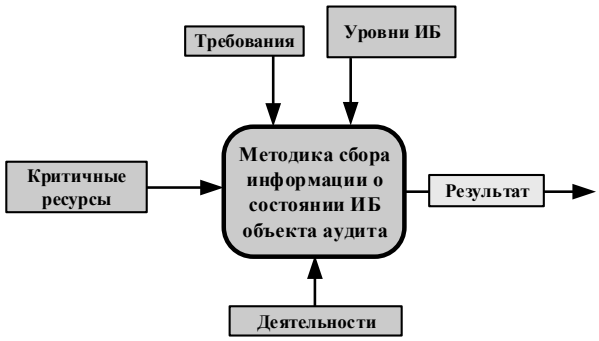

Рис. 3. Формирование методики сбора информации о состоянии ИБ объекта аудита АСУ КВО

В частности, сбор информации включает в себя этапы:

– изучения документации;

– проведения интервьюирования руководителей и специалистов предприятия;

– инструментального обследования;

– наблюдения за работой;

– проверки настроек и конфигураций ИС и др.

Сбор информации, как правило, начинается с изучения существующей документированной информации об объекте аудита, созданной при проектировании, эксплуатации и поддержке функционирования системы.

Интервьюирование персонала проводится с целью получения исходной информации об АСУ, отсутствующей в документированном виде, подтверждения актуальности документированной информации и определения уровня осведомленности сотрудников в части требований по обеспечению ИБ.

Наблюдение за реальными процессами, связанными с обеспечением информационной безопасности, могут касаться следующих вопросов:

– процедура регистрации/исключения пользователей, генерации и смены паролей;

– процедура анализа журналов аудита и реагирования на подозрительную активность;

– порядок изменения конфигурации и обновления системного ПО сетевых устройств и серверов;

– порядок обработки заявок на предоставление дополнительных прав доступа;

– порядок работы с наложенными средствами защиты (межсетевые экраны, системы обнаружения вторжений, антивирусы и т.д.);

– анализ действий, предпринятых при обработке произошедших инцидентов;

– анализ действий, предпринятых при аварийных ситуациях;

– порядок доступа в серверные помещения;

– другие аспекты деятельности по обеспечению ИБ.

При проведении анализа конфигурации типовых рабочих мест, сетевых устройств и ключевых серверов их перечень определяется по согласованию с должностным лицом, ответственным за ИБ на проверяемом предприятии.

Целью такого анализа является оценка соответствия реальной конфигурации тому, что декларируется эксплуатационной документацией, требованиями политики безопасности и персоналом заказчика.

Анализу подлежат параметры аутентификации и контроля доступа, механизмы авторизации, доступа и управления, параметры аудита, меры защиты маршрутной информации, меры защиты от внешних атак АСУ КВО.

Этап оценки, согласования и корректировки результатов реализуется на основании всей полученной информации (в том числе – на основе инструментального обследования).

В процессе анализа и формирования результатов могут возникнуть противоречия между различными источниками информации. Поэтому в случае необходимости проводится повторное уточняющее обследование по конкретному вопросу.

После формирования результатов необходимо воспользоваться методиками оценки соответствия ИБ АСУ КВО требованиям нормативных документов и методикой сравнительной оценки объектов аудита с учетом системы показателей и критериев оценивания.

Литература

1. Марковский А.С. Анализ существующих методик аудита информационной безопасности : научно-технический сборник ОАО «Концерн “Системпром”», 2014.

2. Ерохин С.С., Мещеряков Р.В., Бондарчук С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта. Безопасность информационных технологий // Министерство образования и науки РФ. Московский инженерно-физический институт. – 2007. – № 4. – С. 39–46.

3. Березин А.С., Петренко С.А. Построение корпоративных защищенных виртуальных частных сетей // Конфидент. Защита Информации. – 2001. – № 1.

4. Information technology – Code of practice for Information security management. International Standard ISO/IEC 17799:2005.

5. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

6. Уланов А.В. Повышение оперативности принятия решения в автоматизированных системах / А.В. Уланов, А.А. Нечай, П.Е. Котиков // Наука и современность. – 2014. – № 2 (2). – С. 95–101.

7. Нечай А.А. Контроль сохранности информации / А.А. Нечай, П.Е. Котиков // Научный вестник. – 2014. – № 2 (2). – С. 85–91.

8. Нечай А.А. Применение перепрограммируемых структур в современных информационных решениях / А.А. Нечай, П.Е. Котиков // Научный вестник. – 2014. – № 2 (2). – С. 92–101.

9. Лопатин В.А. Оценка надежности и оперативности распределенной обработки информации / В.А. Лопатин, А.А. Нечай // Экономика и социум. – 2015. – № 1–3 (14). – С. 949–951.

10. Лопатин В.А. Некоторые обобщения в теории множеств, отношений и графов, их применение в информационных технологиях / В.А. Лопатин, А.А. Нечай // Экономика и социум. – 2015. – № 1–3 (14). – С. 958–960.

11. Котиков П.Е. Репликация данных между серверами баз данных в среде геоинформационных систем / П.Е. Котиков, А.А. Нечай // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ и управление. – 2015. – Выпуск 1. – С. 90–93.

12. Нечай А.А. Методика комплексной защиты данных передаваемых и хранимых на различных носителях информации / А.А. Нечай, П.Е. Котиков // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ и управление. – 2015. – Выпуск 1. – С. 94–97.

13. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

14. Нечай А.А. Подходы к выявлению конфиденциальной информации / А.А. Нечай, С.А. Краснов, И.В. Першина // Экономика и социум. – 2015. – № 1–4 (14). – С. 26–31.

15. Першина И.В. Программные методы сокрытия информации / И.В. Першина, А.А. Нечай // Экономика и социум. – 2015. – № 1–4 (14). – С. 195–198.