УДК 004. 413. 4

А.А. ЗАМУЛА, канд. техн. наук, К.И. ИВАНОВ, В.И. ЧЕРНЫШ, Б.В. ВОЛОБУЕВ

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности.

В качестве объекта аудита может выступать как информационно-телекоммуникационная система (ИТС) организации в целом, так и ее отдельные сегменты, обеспечивающие обработку информации, которая подлежит защите.

Для того чтобы оценить реальное состояние защищенности ресурсов ИТС и ее способность противостоять внешним и внутренним угрозам безопасности, необходимо регулярно проводить аудит информационной безопасности. Но при такой регулярности возникает проблема проведения качественного аудита в наиболее сжатые сроки. Очевидно, что аудит информационной безопасности (ИБ) проводится не спонтанно, а в соответствии с жестко выделенной последовательностью этапов. [1, 2]

Работы по аудиту безопасности включают в себя последовательность действий, которые можно структурировать в виде ряда этапов. Далее приведены этапы проведения аудита ИБ (рис. 1).

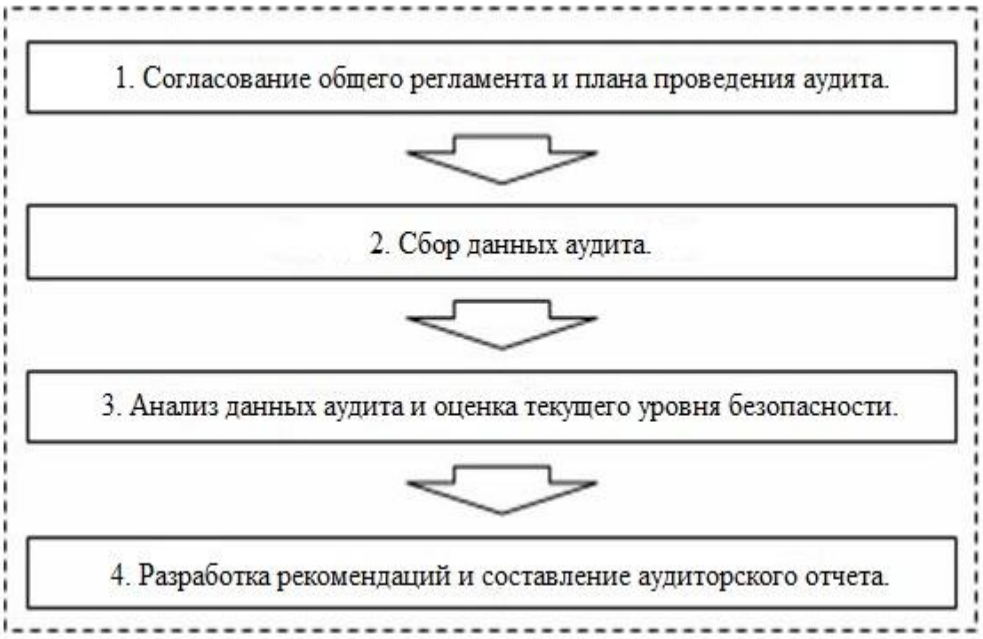

Рис. 1

Согласование общего регламента и плана проведения аудита

Аудит ИБ проводится по инициативе руководства компании, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства компании является необходимым условием для проведения аудита.

Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора оказываются задействованными представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть скоординированы [1].

Регламент как раз и является тем документом, который определяет обязанности сторон во время проведения аудита [3].

Как правило, регламент содержит следующую основную информацию:

- состав рабочих групп от исполнителя и заказчика, участвующих в процессе проведения аудита;
- обязательства сотрудников компании оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию;
- перечень информации, которая будет предоставлена исполнителю для проведения аудита;
- порядок решения спорных вопросов;
- сроки проведения работ.

На первом этапе также должны быть определены границы (некоторые из подсистем могут оказаться некритичными, другие же могут оказаться недоступными для аудита из-за соображений конфиденциальности) и план проведения обследования.

В данных документах определяется следующее:

- список и местоположение помещений заказчика, подлежащих аудиту;
- список обследуемых физических, программных и информационных ресурсов;
- перечень ресурсов, которые рассматриваются в качестве объектов защиты (информационные активы, программные ресурсы, физические ресурсы и т.д.);
- модель угроз информационной безопасности, на основе которой проводится аудит.

Как правило, утверждение регламента и плана проведения аудита обсуждаются на рабочем собрании, в котором должны участвовать аудиторы, руководство компании и руководители структурных подразделений.

Сбор данных аудита

Этап сбора данных аудита является достаточно сложным и крайне важным. Компетентные выводы относительно текущего положения информационной безопасности на предприятии могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа. Получение информации об организации, функционировании и текущем состоянии информационной системы (ИС) осуществляется с помощью:

- предоставления опросных листов, заполняемых сотрудниками заказчика;
- интервьюирования сотрудников заказчика, обладающих необходимой информацией;
- анализа существующей организационно-технической документации, используемой на предприятии, в том числе документации на ИС [3].

Подготовка значительной части документации на ИС обычно осуществляется уже в процессе проведения аудита. Когда все необходимые данные по ИС собраны и подготовлены, можно переходить к их анализу.

Анализ данных аудита и оценка текущего уровня безопасности

После сбора необходимой информации проводится её анализ для оценки текущего уровня защищённости системы.

Анализ данных основывается на методах анализа рисков. Это требует высокой квалификации аудитора и тесно связано с субъективным фактором. При оценивании рисков возможно использование приведенного ниже метода, состоящего из двух этапов [4].

1) Этап определения вероятности.

Этап определения вероятности необходим для подсчета уровня вероятности успешной атаки – это зависит от потенциала угрозы, которая создается активным источником угрозы.

Данные в табл. 1 демонстрируют пороговый эффект, который связан с преодолением защиты. Пороговый эффект получен на основе операции алгебраической разности.

2) Этап определения рисков.

Целью этапа является определение максимального уровня риска ИБ при успешной реализации атаки от *i*-го источника по отношению к *j*-й уязвимости.

Относительно простой способ получения оценки риска для каждой из пар угроза/уязвимость заключается в перемножении вероятности реализации угрозы и ущерба от успешной реализации угрозы с последующим ранжированием полученных значений.

Таблица 1

Эффективность защиты *Z(i,j)*	Потенциал угрозы *U(i,j)*				
	1	2	3	4	5
0 (защита отсутствует)	1	2	3	4	5
1	0	1	2	3	4
2	0	0	1	2	3
3	0	0	0	1	2
4	0	0	0	0	1
5	0	0	0	0	0

Результаты перемножения величин *P*(*i*,*j*) и последующего ранжирования полученных значений уровня вероятности реализации угрозы и ущерба от успешной реализации угрозы приведены в табл. 2 (числа – результат перемножения *P*(*i*,*j*) та *S*(*i*,*j*), а буквенные индексы отображают результат ранжирования).

Таблица 2

Ущерб от реализации угрозы *S(i,j)*	Уровень вероятности реализации угрозы *P(i,j)*				
	1 (Н)	2 (Н)	3 (С)	4 (С)	5 (В)
1	1 (Н)	2 (Н)	3 (Н)	4 (С)	5 (С)
2	2 (Н)	4 (Н)	6 (С)	8 (В)	10 (В)
3	3 (Н)	6 (С)	9 (В)	12 (В)	15 (К)
4	4 (С)	8 (В)	12 (В)	16 (К)	20 (К)
5	5 (С)	10 (В)	15 (К)	20 (К)	25 (Д)

В шкале для оценивания рисков ИБ использованы следующие уровни (табл. 2):

- Н – низкий (отвечает значениям от 1 до 3);
- С – средний (от 4 до 6);
- В – высокий (от 8 до 12);
- К – критический (от 15 до 20);
- Д – очень высокий (от 21 до 25).

Также при анализе данных аудиторы опираются на использование стандартов информационной безопасности. Международные стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. В качестве базового стандарта целесообразно рассматривать стандарт ISO/IEC 17799:2005 [4]. В соответствии с данным стандартом, полученная информация анализируется на соответствие следующим требованиям информационной безопасности:

- к составу и назначению политики информационной безопасности;
- организационной структуре управления информационными технологиями;
- применяемым средствам антивирусной защиты;
- порядку взаимодействия с ресурсами сети Интернет;
- порядку применения средств криптографической защиты информации;
- системе управления информационной безопасностью;
- анализу рисков информационной безопасности заказчика;
- политике информационной безопасности;
- организационным мерам информационной безопасности и другие. [5]

Данные о соответствии различных областей функционирования ИС требованиям стандарта, обычно, представляются в форме таблицы, из которой видно, какие требования безо-

пасности в системе не реализованы. Исходя из этого делаются выводы о соответствии обследуемой ИС требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.

Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины.

Разработка рекомендаций и составление аудиторского отчета

На последнем этапе проведения аудита разрабатываются рекомендации по совершенствованию и доработке организационно-технического обеспечения информационной безопасности на предприятии заказчика аудита. Эти рекомендации должны быть конкретными и применимыми к данной ИС, а также экономически обоснованными и аргументированными.

Рекомендации входят в состав отчета о проведении аудита. Аудиторский отчет является основным результатом проведения аудита. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита. Помимо рекомендаций в отчете должны быть такие разделы:

- описание целей проведения аудита;
- характеристика ИС;
- указание границ проведения аудита и используемых методов;
- результаты анализа данных аудита.

Выводы

Аудит безопасности является одной из наиболее эффективных мер, позволяющих повысить уровень информационной безопасности компании. В данной работе представлена структурированная методика проведения аудита информационной безопасности с описанием каждого из этапов проведения и аргументированием их необходимости в процессе проведения аудита информационной безопасности. В соответствии с международными стандартами, внешний аудит ИБ, методике проведения которого посвящена данная работа, должен проводиться не реже одного раза в год.

Список литературы: 1. *Симонов, С.В*. Аудит безопасности информационных систем. – М. : Jet Info, 1999. №9. 2. *Беккер, Й., Вилков, Л.* Менеджмент процессов. – М. : Эксмо, 2007. – 358 с. 3. *Сердюк,В.А*. Аудит информационной безопасности как мера для повышения уровня защиты компании. / А.В.Сердюк // TComm спецвыпуск по ИБ, 2009. – С.24-26 4. *Замула, А.А.* Необхідність моделі структурування при оцінюванні ризиків інформаційної безпеки / А.А.Замула, В.И.Черныш, К.И.Иванов // Зб. наук. праць Харк. ун-ту Повітряних Сил. – Харків : ХУПС, 2011. – № 3(29). – С.110 – 113. 5. *ISO/IEC 17799:2005* "Information technology – Security techniques – Code of practice for information security management".

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.03.2012