и воздействуют на выходные приборы. На этом принципе работают приемные антенны радиоприёмников. Следовательно, симметричные вибраторы, как и электрический диполь, могут использоваться для регистрации величины электрического поля электромагнитной волны. При этом индукционный ток, возбужденный в цепи вибратора будет пропорционален напряженности электрического поля. Переменное электрическое поле, изменяющееся по гармоническому закону, а именно такие поля применяются для передачи информации, возбудит в цепи электрического диполя электрический ток, который будет определятся функциональным выражением. Таким образом, электрический диполь представляет собой линейный преобразователь изменений напряженности электрического поля в изменения электрического тока в его цепи.

В настоящее время важно понимать значимость физических процессов, в особенности процессов измерительных преобразований. В современном мире всё больше и больше проблем и задач человечества переходит «на плечи» электронных приборов. И всё чаще при использовании того или иного прибора, а в том числе измерительных приборов мы не то что не знаем, даже не представляем, как сложно они могут быть устроены. Большинство людей не задумывается о том какие физические процессы протекают в их электронных средствах. Но не стоит забывать об этом, ведь существуют различные нюансы, которые определенно стоит учитывать при эксплуатации наших устройств.

Особенно стоит обратить внимание на тематику данной проблемы с точки зрения информационной безопасности, которая не может быть обеспечена без должного уровня знаний и подготовки в сфере физических процессов различных измерительных преобразований, т. к. любая оплошность в этом вопросе может понести за собой значительные потери и убытки во многих сферах общества.

Литература

1. Сагдеев К.М., Петренко В.И., Чипига А.Ф. Физические основы защиты информации: Учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 394 с.

И.С. Палканов

АНАЛИЗ МЕТОДОВ И АЛГОРИТМА ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

(Северо-Кавказский федеральный университет)

Развитие подходов и методов осуществления атак на информационные системы происходит постоянно, появление новых угроз снижает эффективность существующей системы защиты информации. Кроме того, изменениям подвергается и сама информационная система организации: увольняются и принимаются на работу сотрудники, появляются новые отделы, изменяется перечень должностных обязанностей – всё это требует изменения правил разгра-

ничения доступа к информационным ресурсам в корпоративной информационной системе. Указанные процессы становятся причиной того, что разработанная некогда политика информационной безопасности и функционирующая на её основе система информационной безопасности утрачивают свою актуальность текущему положению дел, что может привести к ситуации, когда система защиты информации не обеспечивает требуемого уровня защищённости для информационных ресурсов организации. В таких случаях требуется изменение системы информационной безопасности организации таким образом, чтобы она соответствовала актуальному состоянию угроз информационной безопасности и структуре информационных потоков в организации. Эффективность управления системой защиты информации организации базируется на тех же подходах, что и управление другими системами, т.е. осуществляется по схеме контура управления. Для поддержания актуальности системы защиты информации предъявляемым к ней требованиям по обеспечению необходимого уровня защищённости информации следует проводить периодический аудит состояния системы информационной безопасности.

Внутренний аудит информационной безопасности – регламентированная внутренняя деятельность организации, организованная с целью анализа и оценки функционирования системы защиты информации организации. Процедуры внутреннего аудита позволяют определить эффективность деятельности системы защиты информации. Кроме того, такой тип аудита помогает управленцам достичь поставленных целей и усовершенствовать деятельность как системы защиты информации, так и всей организации.

Независимо от формы, аудит информационной безопасности состоит из четырёх основных этапов:

1. Формирование регламента проведения аудита. Данный документ разрабатывается группой по проведению аудита совместно с заказчиком (руководством организации) и включает в свой состав и порядок проведения работ. Приоритетная цель регламента аудита информационной безопасности - определение границ, в рамках которых будет проводиться обследование информационных систем и систем обеспечения информационной безопасности. В нём прописываются все обязанности и права сторон - заказчика и исполнителя работ.

2. Сбор данных для обследования. На данном этапе осуществляется сбор сведений об актуальном состоянии системы информационной безопасности организации через интервьюирование сотрудников, анализ организационно-распорядительной документации, информации об используемом аппаратном и программном обеспечении и т.д.

3. Анализ собранных данных. На данном этапе проводится оценка текущего уровня защищенности автоматизированной информационной системы организации с помощью разнообразных методов. Как правило используется две группы методов оценки текущего уровня информационной безопасности. Первая группа методов позволяет оценить уровень рисков в информационной системе организации посредством анализа соответствия определенному набору

требований по обеспечению защиты. Вторая группа методов проведения аудита информационной безопасности предусматривает определение вероятности реализации атак и наступления ущерба от них.

4. Разработка рекомендаций по устранению выявленных уязвимостей или повышению уровня информационной безопасности системы в целом. Специалисты подробно расписывают действия, которые необходимо осуществить для минимизации выявленных угроз. Они могут включать снижение рисков за счет внедрения дополнительных средств защиты, изменение архитектуры и структуры информационных потоков и т.д.

Поскольку система информационной безопасности организации представляет собой одну из подсистем управления организацией в целом, в качестве документа, регламентирующего процедуру проведения внутреннего аудита системы информационной безопасности целесообразно использовать стандарт ГОСТ Р ИСО 19011-2012 «Руководящие указания по аудиту систем менеджмента». Данный стандарт содержит детальное описание управления проведением аудита: регламент разработки целей аудита, руководство по разработке программы проведения аудита, рекомендации по внедрению программы аудита и мониторингу её реализации. В стандарте также содержатся методические рекомендации по проведению аудита: организация проведения аудита, подготовка к проведению аудита на месте, проведение аудита на месте, подготовка и рассылка отчёта по аудиту, завершение аудита, действия по результатам аудита. Отдельно следует выделить важную часть рассматриваемого документа – рекомендации по оценке компетентности аудиторов. В стандарте приведены следующие методические указания: определение компетентности аудиторов для удовлетворения потребностей программы внутреннего аудита, определение критериев оценки компетентности аудиторов, выбор подходящего метода оценки аудитора, поддержание уровня и повышение компетентности оценки аудитора. В приложении к стандарту приведены руководящие указания и пояснительные примеры в отношении специальных знаний и навыков аудиторов в области специальных дисциплин.

Регламент аудита информационной безопасности определяет состав и порядок выполнения работ во время проведения аудита. Являясь основным документом, определяющим границы проводимого обследования, регламент четко определяет обязанности сторон.

Как правило, в регламенте содержится следующий набор сведений:

– список объектов, подлежащих аудиту, и их местоположение;
– порядок и время проведения программного и инструментального обследования системы защиты информации;
– состав рабочих групп как со стороны заказчика, так и со стороны исполнителя;
– перечень ресурсов, подлежащих обследованию;
– перечень информации, которую предоставят исполнителю;
– модель угроз информационной безопасности организации;

– категории пользователей, считающихся потенциальными нарушителями.

На основе составленного регламента аудита информационной безопасности осуществляется все взаимодействие исполнителя и заказчика.

План аудита согласуется с заказчиком и, как правило, содержит следующие данные:

– цель проведения аудита информационной безопасности;
– критерии проведения аудита информационной безопасности;
– область аудита информационной безопасности;
– даты и срока проведения аудита информационной безопасности;
– роли членов аудиторской группы;
– результаты анализа по итогам проведённого аудита.

Саму схему проведения внутреннего аудита информационной безопасности можно представить в виде следующего алгоритма (рисунок 2).

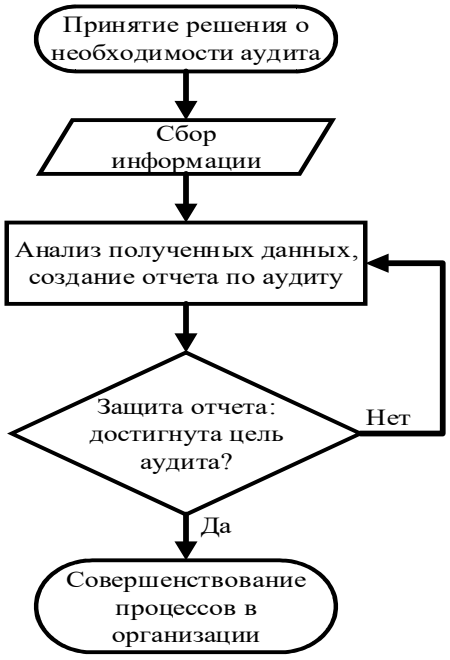

Рисунок 2 – Алгоритм проведения аудита информационной безопасности

Из представленного алгоритма следует, что результатом аудита является создание документа, который содержит детальную информацию о [3]:

– всех выявленных уязвимостях объекта аудита;
– критичности найденных уязвимостях;
– качественная и количественная оценка рисков информационной безопасности;
– стратегия обеспечения информационной безопасности;
– последствие в случае реализации угроз;
– рекомендации по устранению уязвимостей.

Таким образом, из всего написанного, можно сделать вывод, что результатами аудита информационной безопасности могут быть следующие:

– уменьшение риска компрометации информационной системы за счет внедрения организационных мер или технических средств защиты, направленных на снижение вероятности реализации угроз хакерских атак или ущерба от них;

– исключение возможности проведения атаки за счёт изменения схемы информационного потока и архитектуры информационной системы;

– минимизация негативного действия риска за счет применения мер по страхованию;

– уменьшение риска до таких значений, при которых он перестает представлять опасность для информационной системы.

Также можно сделать вывод, что процедуры внутреннего аудита позволяют определить эффективность деятельности системы защиты информации и тех структурных подразделений, которым поручено эту систему поддерживать и развивать. Такой тип аудита помогает управленцам достичь поставленных целей организации и усовершенствовать деятельность как системы защиты информации, так и всей организации.

Литература

1. Сердюк В.Д. Аудит информационной безопасности (ИБ) [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=6781

2. Аудит состояния информационной безопасности на предприятии [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/professional_retraining/964/courses/419/lecture/9583?page=1

3. EFSOL – эффективные решения. Аудит ИБ [Электронный ресурс]. – Режим доступа: http://efsol.ru/promo/info-security-audit.html

4. АйТи. Система ИБ. Аудит ИБ [Электронный ресурс]. – Режим доступа: http://www.it.ru/services/sub/sud_detail.php?ID=383&SUB_ID=6916

5. ProtectMi – лаборатория безопасности. Аудит и управление ИБ [Электронный ресурс]. – Режим доступа: http://www.infosecurity.ru/iprotect/audit/

И.С. Палканов

ЗНАЧЕНИЕ ВНУТРЕННЕГО АУДИТА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

(Северо-Кавказский федеральный университет)

Любая организация существует для выполнения какой-либо цели. Для коммерческих компаний главной целью, как правило, является получение прибыли. Для государственных и муниципальных организаций целями могут являться оказание каких-либо услуг населению или другим организациям, осуществление контрольных функций, возложенные на эти организации их учредителями при создании. Словом, любое предприятие или организация суще-