– 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-

ствует для достижения каких-либо целей, которые изложены в её учредительных документах или приказах о создании. Для достижения своей основной цели организация может иметь набор промежуточных целей, достижение которых позволяет достичь основной цели. Для достижения основной и промежуточных целей организация ведёт какую-либо деятельность. Для этого обычно проводится планирование, крупные задачи разбиваются на подзадачи, которые распределяются между исполнителями. Для эффективного управления как работой всей компании в целом, так и деятельностью отдельных исполнителей, выполняющих частные подзадачи, необходимо вести контроль достигнутых результатов на всех уровнях управления. Анализ результатов позволяет оценить, достигнуты ли поставленные перед исполнителями цели, или требуется дополнительные управляющие воздействия, чтобы достигнуть этих целей. Все описанные выше положения формируют контур управления организацией (рисунок 1).

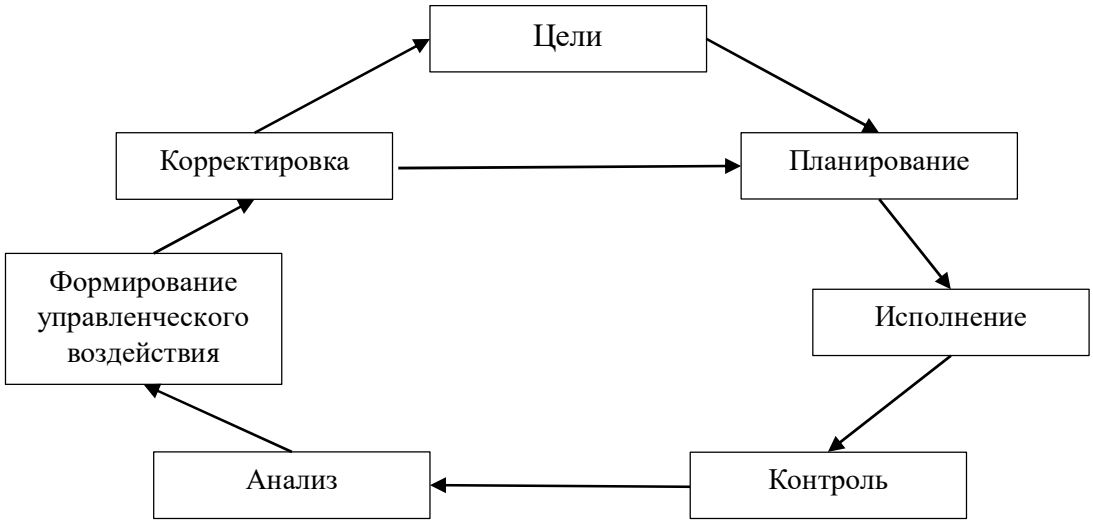

Рисунок 1 – Схема контура управления

Таким образом, из рисунка 1 видно, что контроль исполнения поставленных задач и анализ достигнутых результатов являются важными составляющими эффективного управления любых процессом в организации.

Эффективное управление системой защиты информации организации основывается на тех же подходах, что и управление другими системами и подсистемами, т.е. осуществляется по схеме контура управления. Для мониторинга эффективности управляющих воздействий необходимо проводить контроль и анализ полученных результатов. Эти два процесса составляют вместе аудит системы информационной безопасности организации.

В широком смысле аудит информационной безопасности организации – это набор мероприятий, включающих тестирование автоматизированных информационных систем на проникновение, внутренний аудит информационной безопасности, анализ защищённости используемого программного обеспечения и разработку рекомендаций по устранению обнаруженных уязвимостей. По

своей сути аудит системы информационной безопасности представляет собой независимую экспертную оценку работы системы, которая подразделяется на внешнюю и внутреннюю. Внешняя экспертиза является нечастым организованным мероприятием, инициатором которого выступает руководитель или совет акционеров. Внутренний аудит проводится гораздо чаще, а иногда и непрерывно, чтобы своевременно выявлять уязвимости в системе информационной безопасности.

Аудит системы информационной безопасности преследует следующие цели:

– оценку актуальности системы защиты информации текущей модели угроз информационной безопасности в целом;

– оценку защищённости каналов, по котором может произойти утечка информации ограниченного доступа;

– анализ используемых средств защиты информации, приведение их перечня и состояния в соответствие с актуальными требованиями;

– корректировку документации, относящейся к области информационной безопасности, приведение ее к актуальными требованиями;

– моделирование ситуаций, при которых может произойти несанкционированный доступ к защищаемой информации или случиться утечка информации;

– выработку рекомендаций по устранению выявленных уязвимостей информационных систем.

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.

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 ор-

ганизации 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.

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.

Методы аудита информационной безопасности можно классифицировать как экспертно-аналитические, экспертно-инструментальные и моделирование действий злоумышленника. Экспертно-аналитические методы заключаются в анализе и оценке состояния безопасности информационной среды на основе экспертной оценки. Экспертно-инструментальные методы - проведение анализа при помощи специального инструментария. Моделирование действий злоумышленника или так называемый «этичный взлом» системы защиты информации - реализуется уже после проведённых ранее исследований как заключительный контрольный этап аудита информационной безопасности.

Результатами аудита информационной безопасности могут быть следующие:

– уменьшение риска компрометации информационной системы за счет внедрения организационных мер или технических средств защиты, направлен-

ных 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.

Таким образом, внутренний аудит информационной безопасности организации является наиболее эффективным инструментом, позволяющим получить объективные сведения о текущем уровне защищенности информационной системы. План аудита информационной безопасности должен учитывать все возможные риски компрометации системы, только в этом случае экспертиза принесет реальную пользу.

Литература

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

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

3. Ситнов А.А. Организация аудита информационной безопасности [Электронный ресурс]. – Режим доступа: https://accounting.fa.ru/jour/article/viewFile/129/130.pdf.

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

Д.И. Парфёнов, В.А. Торчин, Л.С. Забродина

РАЗРАБОТКА ПОДХОДА К ПОИСКУ УЯЗВИМОСТЕЙ В СЕТЯХ ПРОВАЙДЕРОВ ТЕЛЕКОММУНИКАЦИОННЫХ УСЛУГ

(Оренбургский государственный университет)

Развитие информационных технологий предполагает появление новых угроз и возникновение необходимости разработки новых подходов к обеспечению безопасности. Это особенно актуально для операторов связи и провайдеров телекоммуникационных услуг, являющихся ключевым звеном инфраструктуры передачи данных для любой компании. Для обеспечения защиты собственной инфраструктуры и сервисов провайдерам приходится применять не тривиальные решения [1]. Инфраструктура провайдеров телекоммуникационных услуг на сегодняшний день, как правило, строится на базе автономных систем, организованных на базе мультиоблачных платформ. Такой подход позво-