**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**ЛАБОРАТОРНАЯ РАБОТА**

**по дисциплине**

**«Введение в аналитику информационной безопасности»**

**Выполнила: ст. гр. 201-331 Заднепрянская А. А.**

**Проверили: Кривоногов А. А.,**

**Плоткин А. С.**

**Москва – 2021**

**Задание № 1**

Большое количество организаций финансового рынка проводят некоторое количество аудитов информационной̆ безопасности в год, тем самым подтверждая своё соответствие нормативным требованиям и выявляя новые бреши и уязвимости.

**Вопросы**.

1. Какие виды аудита необходимо осуществлять в течение года финансовым организациям?
2. Чем внутренний аудит отличается от внешнего? Какие можно выделить преимущества и недостатка того или иного подхода к аудиту информационной̆ безопасности?
3. Можно ли осуществлять только внутренний аудит организации, при этом не прибегая к контрагентам для проведения внешнего аудита?

**Задание**.

Следует составить **план внутреннего аудита информационной безопасности в финансовой организации** (план представляет собой перечень задач по пунктам, которые необходимо выполнить специалистам ИБ (аудиторам)). При составлении плана необходимо комплексно подойти к оценке ИБ организации, которая будет включать все аспекты ИБ.

**Ход выполнения задания № 1.**

Что такое аудит информационной безопасности?

Аудит ИБ — это процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности предприятия, которые позволяют выработать практические рекомендации по управлению и обеспечению ИБ предприятия.

Аудит безопасности может проводится либо силами самого предприятия (в этом случае создается комиссия, состоящая из представителей служб ИБ, кадрового аппарата, руководителя предприятия, представителей структурного подразделения), либо для проведения аудита приглашаются представители сторонних организаций, компетентность который в данном вопросе подтверждается соответствующими лицензиями.

Процедуру проведения аудита можно условно разделить на несколько этапов: подготовительные мероприятия, непосредственное проведение аудита, завершающий этап.

На подготовительном этапе выбирается объект аудита, составляется команда аудиторов-экспертов, определяется объемы, масштабы аудита, устанавливаются конкретные сроки работы.

В процессе непосредственного проведения аудита проводится общий анализ состояния безопасности объекта аудита, проводится регистрация, сбор и проверка статистических данных, результатов инструментальных измерений, опасности и угроз, оцениваются результаты проверки и составляется отчет о результатах проверки по отдельным составляющим.

По завершению аудита составляется итоговый отчет, разрабатывается план мероприятий по устранению узких мест и недостатков в обеспечении безопасности организации.

Вопрос № 1.

1. Экспертный аудит безопасности, в процессе которого выявляются недостатки и уязвимости в системе мер ЗИ на основе имеющегося опыта экспертов, участвующих в процедуре аудита.

2. Оценка соответствия рекомендациям Международного стандарта ISO 17799 и требованиям руководящих документов ФСТЭК.

3. Инструментальный анализ защищенности автоматизированной системы, который направлен на выявление и устранение уязвимостей программно-аппаратного обеспечения системы.

4. Комплексный аудит, включающий в себя вышеперечисленные формы проведения обследования.

5\*. Финансовый аудит (назначение) для выявления финансовый рисков, например, налоговых, правовых, административных и др. и рекомендаций по их снижению.

Каждый из вышеперечисленных видов аудита может проводиться по отдельности или в комплексе.

Вопрос № 2.

Отличия внутреннего аудита от внешнего:

1. По цели аудита. Внутренний аудит направлен на потребности руководства компании, а внешний – на потребности сторонних пользователей (инвесторы, банки, налоговые органы и т.п.).
2. По объекту. При внешнем аудите обычно проверяется только достоверность бухгалтерской отчетности. Внутренний аудит направлен на проверку эффективности работы предприятия в целом или отдельных бизнес-процессов.
3. По нормативной базе. Внутренний аудит регламентируется внутренними документами компании, а внешний – законодательными актами и международными стандартами.
4. По исполнителям. Внутренний аудит осуществляется сотрудниками самой организации, а внешний – работниками сторонней аудиторской фирмы.
5. По оплате. Внешний аудит проводится на основании договора, заключенного с аудиторской фирмой или отдельным аудитором (частным предпринимателем). При внутреннем аудите работу выполняют сотрудники компании, получающие свои обычные должностные оклады.
6. По периодичности. Внешний аудит проводится обычно раз в год с целью подтверждения достоверности годовой отчетности. Внутренний аудит может осуществляться и чаще.

К преимуществам внутреннего аудита можно отнести:

1. Возможность проведения проверки всех систем внутреннего контроля организации в постоянном режиме.

2. Возможность более глубокого и детального погружения аудитора в проблемы и суть проверяемых участков, так как он работает внутри организации и знает все слабые и сильные стороны.

К недостаткам внутреннего аудита можно отнести:

1. Принцип независимости внутреннего аудитора всегда можно поставить под сомнение, так как он в любом случае — сотрудник компании.

2. Разовый внешний аудит может быть дешевле, чем постоянные затраты на содержание в штате внутреннего аудитора.

К преимуществам внешнего аудита можно отнести:

1. Более высокий, чем при внутреннем аудите, уровень объективности заключения.

2. Более высокая, чем при внутреннем аудите, эффективность работы аудиторов, обусловленная жесткими временными рамками.

3. Результаты аудита можно использовать для рекламы предприятия.

К недостаткам внешнего аудита можно отнести:

1. Незнание внешними аудиторами производственных особенностей проверяемого предприятия.

2. Конфиденциальная информация не может быть использована в отчете об аудите.

3. Выборочность аудита, исключающая возможность полного обследования системы качества.

Вопрос № 3

Внешний аудит информационной безопасности (ИБ) — способ получить объективную оценку надежности ИТ-инфраструктуры, узнать степень ее устойчивости к угрозам как на уровне сети, так и на уровне отдельных компонентов информационной системы.

Некоторые виды аудита ИБ выполнить внутренними силами либо очень дорого, либо вообще невозможно из-за процедурных особенностей, стоящих перед аудиторами задач. Поэтому полагаться только на внутренний аудит довольно рискованно.

Внешний аудит рекомендуется проводить ежегодно с целью проверки и корректировки действующих в компании стратегических процедур обеспечения ИБ.

Во внешнем аудите ИБ в первую очередь должны быть заинтересованы собственники бизнеса и руководители компании. Им необходима уверенность, что их коммерческая деятельность ведётся в защищенном, контролируемом пространстве. Кроме того, внешний аудит повышает уровень доверия к организации со стороны партнёров и клиентов.

В ситуациях, когда не хватает квалификации собственных специалистов, внешний аудит становится единственным вариантом решения проблем информационной безопасности.

Таким образом, **нельзя** осуществлять только внутренний аудит организации, так как внешний аудит информационной безопасности поможет по-настоящему понять, насколько уязвима ИТ-инфраструктура той или иной организации, независимо от нее самой.

Задание № 1.

Согласно п. 35 и п. 36 «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235) в рамках контроля состояния безопасности «значимых» объектов КИИ должен осуществляться внутренний контроль организации работ по обеспечению их безопасности, и эффективности принимаемых организационных и технических мер.

**1 Подготовка и планирование аудиторской проверки.**

1.1 Определение объема проверки, масштаба аудита и установление конкретных сроков работы.

1.2 Планирование аудита и составление программы аудиторской проверки.

**2 Проведение аудита.** Выполнение плана должно проходить в присутствии сотрудников отдела информационных технологий и с их помощью.

2.1 Общий анализ состояния безопасности объекта аудита, а также регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз.

2.1.1 Анализ состояния информации, хранящейся и обрабатывающейся в организации.

2.1.1.1 Определение возможности утечки информации через человеческий фактор, например, не получает ли кто-либо из сотрудников доступ к информации, являющейся необходимой для его работы в организации.

2.1.1.2 Получение информации о том,  не попадает ли информация, требующая особого контроля, на информационные ресурсы открытого доступа.

2.1.2 Анализ состояния информационных ресурсов, на которых хранится информация, используемая организацией.

2.1.2.1 Установление правильности предоставления доступа тех или иных пользователей к информационным ресурсам, то есть не получает ли какой-либо пользователь доступ с правами, которые для выполнения его работы избыточны.

2.1.2.2 Проверка соответствия паролей пользователей и администраторов требованиям безопасности (длина не менее 8 символов, использование как минимум одной цифры, одной заглавной буквы и одной строчной, а также одного специального символа, при этом пароль не должен быть осмысленным).

2.1.2.3 Проверка хранения информации, подлежащей охране, на собственных серверах организации, а не в облачных хранилищах.

2.1.2.4 Определение наличия специализированного программного обеспечения, фиксирующее все действия пользователей при обработке информации на информационном ресурсе.

2.1.3 Анализ состояния информационных каналов, по которым перемещается информация.

2.1.3.1 Проверка необходимого установления шифрованного SSL-соединения с применением действующих сертификатов, а также логина и пароля, соответствующего требованиям информационной безопасности.

2.1.3.2 Необходимость выяснения, не используется ли передача информации, подлежащей охране, через шлюзы, установленные на территории организации, в нешифрованном виде.

2.1.3.3 Проверка требований WLAN.

2.1.3.3.1 Поддержка стандартов шифрования WPA2 или WPA-PSK беспроводной сети.

2.1.3.3.2 Беспроводная сеть закрыта.

2.1.3.3.3 Беспроводная сеть не публична.

2.1.3.4 Проверка использования соединений, обеспечивающими SSL-шифрование передаваемой информации по сертификату в сочетании с логином и безопасным паролем (VPN-соединения).

2.1.3.5 Проверка регулярного обновления ПО шлюзов/ маршрутизаторов, списков вредоносных сайтов, соответствия паролей административных учётных записей, используемых для управления шлюзами/маршрутизаторами, озвученным ранее критериям безопасности.

2.1.4 Анализ состояния программного обеспечения, используемого для обработки информации.

2.1.4.1 Проверка соблюдения лицензионности, то есть для свободного (бесплатного) программного обеспечения в наличии должна быть GNU/GPL-лицензия.

2.1.4.2 Проверка соответствия пароля озвученным ранее критериям безопасности, когда во время использования ПО необходим ввод паролей тех или иных пользователей организации.

2.1.4.3 Проверка регулярного обновления антивирусных систем и систем обнаружения вредоносного программного обеспечения.

2.1.5 Анализ состояния юридической и технической документации.

2.1.5.1 Проверка наличия полного комплекта документации по всему используемому программному и аппаратному обеспечению, причём версия документации должна соответствовать версии используемого программного обеспечения.

2.1.5.2 Следует сверить схему обработки информации: каждому событию обработки или передачи информации должен соответствовать регламент, описывающий действия пользователя или процесс обработки информации программным обеспечением.

2.1.6 Анализ состояния средств физической защиты информации.

2.1.6.1 Необходимость установления, кто имеет доступ в помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также где хранится документация, не имеют ли туда доступ неавторизованные лица. Список сотрудников, имеющих доступ в эти помещения, должен быть строго ограничен.

2.1.6.2 Необходимость проверки на предмет сохранения своего функционирования в полном объёме при отключении питания системы СКУД и системы видеонаблюдения.

2.1.6.3 Необходимость проверки на предмет оснащения системой автоматического пожаротушения помещения, где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также где хранится документация.

2.1.6.4 Необходимость проверки на предмет оснащения системой резервного питания, автоматически включающейся при отключении основного источника питания, где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также где хранится документация.

2.1.6.5 Необходимость проверки на предмет оснащения системой поддержания постоянной температуры (системой охлаждения воздуха), где установлено оборудование обработки и хранения информации и оборудование каналов связи, а также где хранится документация.

2.2 Составление отчета о результатах проверки по отдельным составляющим, то есть документирование аудита информационной безопасности.

2.2.1 Документирование процесса, подтверждение выполнения каждой проверки записями в электронном журнале аудита и скриншотами, фотографированием в режиме впечатывания даты и времени выполнения фотографии в снимок.

**3 Заключительный этап аудиторской проверки**

3.1 Составление итогового отчета.

3.1.1 Составление отчёта с указанием всех обнаруженных уязвимостей и выявленных недостатков, а также выдача рекомендаций по их устранению, исходя из лучших практик и рекомендаций по информационной безопасности.

3.1.2 В случае закрытия каких-либо уязвимостей в ходе аудита указание в отчёте в отдельном списке с пометкой, как и кем именно закрыта уязвимость или устранён недостаток.

3.2 Разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности финансовой организации.