МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ
ДИСЦИПЛИНАМ

Разработка регламента проведения аудита информационной безопасности образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
71 % авторского текста

Работа рекомендована к защите
«11» декабря 2024 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Симонова Анна Александровна
Научный руководитель:
к.п.н., доцент кафедры АТ, ИТ и МОТД
ППИ

Гафарова Елена Аркадьевна

Челябинск
2024

Содержание

Введение

В современных условиях, когда информационные системы присутствуют во всех сферах жизнедеятельности организации, а с учётом необходимости их связи с сетью Интернет они оказываются открытыми для внутренних и внешних угроз, проблема информационной безопасности становится одной из самой важной, не меньше чем экономическая или физическая безопасность.

В учебных заведениях хранится значительное количество чувствительных и конфиденциальных данных, начиная от исследований и заканчивая экзаменационными заданиями, финансовыми данными, различной отчетностью и личной информацией сотрудников и учащихся. Взлом или нарушение работы ИТ-систем учреждений образования может серьезно повлиять на репутацию, эффективность и непрерывность работы учреждений.

Нарушение конфиденциальности данных может повлечь за собой риски штрафов со стороны регулирующих органов за несоблюдение следующих нормативно-правовых актов:

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 27.07.2006 №152-ФЗ: «О защите персональных данных».

Осознавая глубокое понимание угроз информационной безопасности, с которыми сталкиваются образовательные учреждения, число атак на организации в сфере образования продолжают расти и регистрируются все больше нарушений в области безопасности.

Поэтому актуальным становится создание надежной системы защиты, где необходимо разработать регламенты безопасности, обучить сотрудников и учащихся, провести аудит информационной безопасности и внедрить современные средства защиты, специализирующиеся на защите от выявленных угроз.

В настоящее время не существует стандартизированной методики анализа и оценки рисков угроз информационной безопасности для образовательных организаций. Все разработанные и активно использующиеся методики являются довольно общими для организаций, работающих в различных секторах, и они носят лишь рекомендательный характер.

В связи с этим проблема исследования состоит в необходимости разрешения противоречия, состоящего в том, что, с одной стороны, существует потребность в образовательных организациях на разработку регламента оценки угроз информационной безопасности, а с другой стороны, отсутствие регламента проведения аудита информационной безопасности образовательной организации, отраслевого, предназначенного непосредственно для образовательной организации.

Актуальность темы исследования. Необходимый уровень информационной безопасности организации достигается в результате создания системы обеспечения безопасности информации. Своевременная и полная оценка существующей или создаваемой системы обеспечения безопасности информации поможет сохранить доступность, целостность и конфиденциальность информационных активов. Это возможно при условии знания состояний, характеристик и параметров используемых защитных механизмов, процессов менеджмента, осознания ИБ и понимания степени их соответствия требуемым результатам. По результатам такой оценки определяются слабые места в существующей системе защиты, даются рекомендации для ее дополнения и модернизации. Такой процесс должен

осуществляться периодически и называется аудитом информационной безопасности (ИБ).

Исследованием проблем аудита ИБ, оценки защищенности и оценки эффективности системы обеспечения безопасности информации занимались многие отечественные и зарубежные ученые: А.А. Малюк, В.А. Герасименко, В.В. Андрианов, А.А. Шелупанов, А.А. Грушо, А.П. Курило, В.В. Домарев, Moeller R и другие.

Научных работ, посвященных исследованию теоретико-методологических основ аудита ИБ в отечественной литературе имеется незначительное количество. Например, работы таких ученых, как: А.М. Астахов, Я.В. Бузанова, Н.Е. Васильева, В.Б. Голованов, Н. Данилкина, С.Л. Зефиров, А.П. Курило, А.А. Петренко, С.А. Петренко, М.Н. Черных, Г.А. Юдина, В.И. Ярочкин. Следует отметить, что существуют серьезные различия между позициями российских авторов при определении содержания аудита ИБ и методах его проведения.

Теоретический и методологический подходы к аудиту информационной безопасности находятся в стадии становления. Важность и актуальность проблемы, ее недостаточная теоретическая и практическая разработанность, применительно к сфере информационной безопасности, послужили основанием для определения темы исследования и подтверждением актуальности необходимость разработки регламента аудита ИБ различных систем, отвечающих современным требованиям обеспечения безопасности информации.

Целью исследования является разработка регламента проведения аудита информационной безопасности образовательного учреждения.

Для достижения данной цели необходимо решить следующие задачи:

1) Сформулировать уточненное определение понятия «аудит ИБ», определить цели и задачи аудита ИБ, выделить виды проведения аудита ИБ, обозначить этапы проведения аудита информационной безопасности.

2) Изучить и выявить угрозы, уязвимости и риски в системе защиты информации образовательной организации на базе исследования.

3) Разработать меры защиты информационной безопасности образовательной организации.

4) Разработать Регламент аудита информационной безопасности образовательного учреждения.

5) Разработать формы сопровождающей документации для Регламента аудита информационной безопасности, а также Политику внутреннего аудита информационной безопасности образовательного учреждения.

Объектом исследования является информационная безопасность образовательной организации.

Предметом исследования регламент аудита информационной безопасности образовательного учреждения.

Гипотеза исследования состоит в предположении о повышении эффективности системы информационной безопасности образовательной организации при проведении аудита информационной безопасности образовательной организации по регламенту, разработанному на основе научно-обоснованной методики существующих стандартов.

Научная новизна результатов исследования заключается в следующем:

1. Сформулировано уточненное определение понятия аудит информационной безопасности.
2. Разработан регламент обеспечения и проведения внутреннего аудита информационной безопасности образовательного учреждения.

3. Разработаны формы сопровождающей документации для Регламента аудита информационной безопасности, а также Политика внутреннего аудита информационной безопасности образовательного учреждения.

База исследования: Государственное бюджетное образовательное учреждение «Южно-Уральский государственный колледж», расположенный по адресу ул. Курчатова, 7, г. Челябинск.

Структура работы: Магистерская диссертация состоит из введения, трех глав, заключения, библиографического списка, состоящего из __ наименований. Работа содержит 6 рисунков, 4 таблицы. Общий объем работы составляет 136 страниц.

Глава 1. Основы проведения аудита информационной безопасности организаций

1.1. Общая характеристика автоматизированных систем

Современные образовательные организации являются не только местом хранения и передачи информации, но и развитыми технологическими предприятиями по обработке и созданию научной и учебной информации. ИТ-инфраструктура современной образовательной организации представляет собой сложную систему программных, технических, информационных средств, позволяющих получать актуальные знания в режиме реального времени, а также оптимизировать и автоматизировать организацию учебного процесса и соответствующего документационного обеспечения.

Образовательный процесс касается наименее защищенных от пропаганды членов общества – детей и подростков. Поэтому система информационной безопасности образовательного учреждения должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и гарантировать невозможность доступа в стены школы, техникума и института любой пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание учащихся в заведениях среднего полного общего и высшего образования.

В понятие информационной безопасности образовательного учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

Многообразие задач, решаемых с помощью ЭВМ, привело к появлению множества различных типов систем, отличающихся принципами построения и заложенными в них правилами обработки информации.

Система (Греч. "целое, составленное из частей, соединение") - это совокупность элементов, связанных между собой определенными отношениями и образующих определенную целостность, единство.

Под системой понимают любой объект, который одновременно рассматривается и как единое целое, и как совокупность объединенных в интересах достижения поставленных целей множества разнородных элементов. Системы различаются как по составу, так и по основным целям. Функционирование совокупности элементов или частей, связанных между собой и с внешней средой, направлено на получение конкретного полезного результата. Например, можно назвать системы образования, энергетики, транспорта, экономики и многие другие.

В информатике понятие "система" широко распространено и имеет множество значений. Чаще всего он используется для обозначения набора технических средств и программ.

Система должна быть гибкой, чтобы иметь возможность реагировать на изменяющиеся условия. Для этого используются различные технологии автоматизации элементов системы, да и самой системы в целом.

Автоматизация — это комплекс мероприятий и мероприятий технического, организационного и экономического характера. Это позволяет снизить степень участия, а также полностью исключить непосредственное участие человека в осуществлении производственного или иного технологического процесса.

В целом автоматизация означает использование технических средств и технологий для выполнения любых процессов с их помощью. Она служит

основой для фундаментальных изменений в любых предметных областях (в производстве, управлении, обучении, культуре и др.).

Основными задачами автоматизации являются:

- снижение трудозатрат в традиционных процессах и операциях;
- устранение рутинных операций;
- ускорение процессов обработки и преобразования информации;
- расширение возможностей статистического анализа и повышение точности бухгалтерской и отчетной информации;
- повышение эффективности и качества обслуживания пользователей;
- модернизация или полная замена элементов традиционных технологий;
- расширение возможностей организации и эффективное использование информационных ресурсов организации за счет применения новых информационных технологий-штрихового кодирования, RFID, RAID, CD и DVD, систем теле-доступа и телекоммуникаций, электронной почты, других сервисов Интернета, гипертекстовых, полнотекстовых и графических машиночитаемых данных и др.;
- создание возможностей для широкого обмена информацией, предоставления услуг, эффективного участия в системах сотрудничества и интеграции.

Добавление термина "автоматизированная" к понятию "система" отражает способы создания и функционирования такой системы.

Автоматизированная система (по ГОСТу) — это система, состоящая из взаимосвязанного набора организационных единиц и набора средств автоматизации, реализующих автоматизированные функции для отдельных видов деятельности.

Компонент автоматизированной системы (АС) рассматривается как элемент одного из видов программного обеспечения (технического,

программного, информационного и др.), который выполняет определенную функцию в подсистеме as и обеспечивает ее функционирование.

Перед созданием АС человек организует программу подготовительных мероприятий, поэтому требуется, в частности, специальная организационно-правовая поддержка.

В связи с производственными процессами объект и орган управления представляют собой единую человеко-машинную систему, и человек обязательно включается в схему управления.

По определению, автоматизированная система – это человеко-машинная система, предназначенная для сбора и обработки информации, необходимой для управления производственным процессом, то есть для управления коллективами людей.

Существует четыре типа автоматизированных систем:

- Охват одного процесса (операции) в организации.
- Объединение нескольких процессов в организации.
- Обеспечение функционирования единого процесса в масштабе нескольких взаимодействующих организаций.
- Реализация работы нескольких процессов или систем в масштабе нескольких организаций.

Под автоматизацией предприятий понимается не только приобретение компьютеров и создание корпоративной сети, но и создание информационной системы, включающей компьютеры, программное обеспечение и сети, а главное – организацию информационных потоков. Разнообразные автоматизированные системы, широко применяемые в различных областях человеческой деятельности, являются информационными системами. Добавление термина "информация" к понятию "система" отражает цель ее создания и функционирования.

Информационная система – это взаимосвязанный набор инструментов, методов и персонала, используемых для хранения, обработки и выдачи информации в целях достижения поставленной цели.

Под информационной системой понимается организационно упорядоченная совокупность массивов документов и информационных технологий, в том числе с использованием вычислительной техники и средств связи, реализующих информационные процессы.

Основной целью информационной системы является производство и распространение профессиональной информации. Информационные системы обеспечивают сбор, хранение, обработку, поиск, доставку информации, необходимой в процессе решения задач из любой области. Они помогают анализировать проблемы и создавать новые продукты. Они предназначены для длительного хранения, обеспечения эффективного поиска и передачи информации по соответствующим запросам. В этом смысле их обычно называют системами обработки и хранения информации.

Информационная система является системой информационного обслуживания пользователей и выполняет технологические функции по накоплению, хранению, передаче и обработке информации. Она формируется и функционирует в нормативных актах, определяемых методами и структурой, принятыми в конкретной предметной области и даже на конкретном объекте, реализуя стоящие перед ней цели и задачи.

Совокупность информации о любом объекте называется информационной базой. Информационная база присуща любому объекту независимо от уровня техники управления. Он делится на подсистемы, массивы, индикаторы, детали. Массив – это структурная единица информации, представляющая собой набор данных, связанных с одной задачей (подсистемой).

Информационная база, записанная на машинных (электронных) носителях информации и используемая для решения задач на компьютере, называется базой данных.

Информационная база является основой внутримашинного информационного обеспечения, это совокупность всех данных, подлежащих накоплению, хранению, поиску, преобразованию, доставке в установленном порядке, а также использованию для организации связи человека с компьютером.

База данных – это управляемый набор данных, который является исходной информацией для решения управленческих задач и принятия управленческих решений. База данных может содержать информацию по всем задачам, решаемым в автоматизированных системах, или по группам задач.

Обработка и выдача необходимой информации для группы пользователей или задач управления осуществляется с помощью программ управления информационной базой.

Система управления базами данных представляет собой набор языковых и программных средств, обеспечивающих формирование и ведение электронных наборов данных.

Информация – сведения (сообщения, данные) независимо от формы их представления. Это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации,

доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные системы существуют уже сотни лет и используются на практике в виде различных картотек и коллекций бумажных документов. Однако в таких системах отсутствует автоматизация обработки данных. Они позволяют только регистрировать и сохранять в систематическом виде на бумаге результаты натурных измерений. Современное понимание информационной системы предполагает использование компьютера, как основного технического средства обработки информации. В результате такие системы становятся автоматизированными.

Автоматизированная информационная система – это совокупность программно-технических средств, предназначенных для хранения и (или) управления данными и информацией, а также для производства расчетов. Это человеко-машинная система, обеспечивающая автоматизированную подготовку, поиск и обработку информации в рамках интегрированных сетевых, компьютерных и коммуникационных технологий для оптимизации деятельности в различных предметных областях и сферах управления.

1.2. Аудит информационной безопасности

Множество информационных преступлений совершается благодаря утечкам данных. Одинаково важна и информационная безопасность госучреждений, и вопросы сохранности данных в частных компаниях. Чтобы убедиться в том, что организация находится под надежной защитой, необходимо регулярно проводить аудит. Эта процедура позволяет определить слабые места, оценить возможные варианты утечек, разработать стратегии по предупреждению проблем.

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности. Аудит информационной безопасности – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как образовательной организацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита [12].

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере [12]. Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере.

Аудит позволяет оценить текущую безопасность функционирования информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности её информационных активов,

стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных. В конечном счете, грамотно проведенный аудит безопасности информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности организации.

Основная отличительная особенность обеспечения информационной безопасности в образовательной организации будет заключаться в их природе, так как защита требуется не только для личной информации, но и для образовательного процесса в целом.

Информацию, которую необходимо защищать, условно можно разделить на несколько классов:

- ✓ персональные данные студентов, профессоров и персонала, оцифрованные архивы;
- ✓ исследования, научные работы, ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- ✓ структурированная учебная информация образовательного учреждения, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Эти данные могут попасть в поле зрения злоумышленников и стать целью атак. Статистика показывает, что мошеннические действия направлены не только на хищение личной информации, но и на вмешательство в финансовую сферу организации. Последствия таких проникновений могут варьироваться от хищения научных исследований до изменения работы всей структуры. Намеренное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения. Однако не все угрозы могут исходить извне. Сами студенты также могут стать

источником ряда проблем. Случайно или намеренно от действий учащихся могут быть повреждены компьютерные системы или целые массивы данных.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- ✓ доступности в любое время для любого авторизированного пользователя;
- ✓ защиты от любой утраты или внесения несанкционированных изменений;
- ✓ конфиденциальности, недоступности для третьих лиц.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов учреждения.

Регламент информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его информационной безопасности.

Пользователь ЛВС – сотрудник образовательной организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в

установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название отдела, телефоны, E-mail и т.п.

Системный администратор – сотрудник образовательной организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети учреждения и ПК.

Средства криптографической защиты информации – средства шифрования, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и

позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (VIRTUAL PRIVATE NETWORK) – «Виртуальная частная сеть»: технология и организация систематической удаленной связи между выбранными группами узлов в крупных распределенных сетях.

Любая информационная система предполагает участие людей в ее работе. Среди персонала, связанного с информационными системами, есть такие категории, как конечные пользователи, программисты, системные аналитики, администраторы баз данных и др.

Системный аналитик – это человек, который оценивает потребности пользователей в применении компьютера, а также разрабатывает информационные системы, удовлетворяющие этим потребностям.

Специалисты по обработке данных профессионально анализируют, проектируют и разрабатывают систему.

Существует множество случаев, в которых целесообразно проводить аудит безопасности. Вот лишь некоторые из них:

- аудит с целью подготовки технического задания на проектирование и разработку системы защиты информации;
- аудит после внедрения системы безопасности для оценки уровня её эффективности;
- аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства;
- аудит, предназначенный для систематизации и упорядочивания существующих мер защиты информации;
- аудит в целях расследования произошедшего инцидента, связанного с нарушением информационной безопасности.

Технологии развиваются и изменяются, поэтому аудит требуется проводить регулярно. Он позволит выявить устаревшие решения и привести всю систему в компании к единому стандарту.

1.3. Цели и задачи аудита информационной безопасности

Аудитор в компании может реализовывать разные цели, однако, в первую очередь целями проведения аудита безопасности являются [7, 9, 10, 12]:

- получение объективных доказательств, анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы;
- оценка текущего уровня защищенности информационной системы;
- локализация узких мест в системе безопасности информационной системы;
- оценка соответствия информационной системы существующим стандартам и нормативно-правовым документам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационной системы.

Также целью специалиста часто становится определение уровня знаний сотрудников, их обучение, консультирование. Закономерным итогом может быть и обучение, если выявлен недостаток знаний.

Проверяются нормативные документы, могут быть изменены требования к уровню защищенности ИТ-инфраструктуры.

Представленные Аудитору рапорты о инцидентах системы информационной безопасности должны содержать документацию о «слабых точках» системы информационной безопасности.

Основные задачи, решаемые в ходе проведения аудита информационной безопасности:

- сбор и анализ исходных данных об организационной и функциональной структуре информационной системы компании;
- разработка и анализ существующих политик безопасности и/или других организационно-распорядительных документов по защите информации, анализ процедур обеспечения информационной безопасности на предмет полноты и эффективности;
- анализ существующих рисков связанных с осуществлением угроз информационной безопасности;
- формирование рекомендаций по разработке (или доработке) политик и процедур обеспечения информационной безопасности на основании анализа существующего уровня информационной безопасности, участие в их внедрении в работу;
- формирование предложений по использованию существующих и установке дополнительных средств защиты информации для повышения уровня надежности и безопасности информационной системы компании;
- постановка задач для ИТ – персонала, занятого в сфере информационных технологий и информационной безопасности, касающихся обеспечения защиты информации;
- участие в обучении обслуживающего персонала и пользователей информационной системы вопросам обеспечения информационной безопасности;
- участие в разборе инцидентов, связанных с нарушением информационной безопасности;
- прочие задачи.

Основные направления аудита информационной безопасности [12]:

1. Аттестация объектов информатизации по требованиям стандартов и другой нормативной документации в области информационной безопасности, например:

- аттестация автоматизированных систем, средств связи, обработки и передачи информации;
- аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
- аттестация технических средств, установленных в выделенных помещениях и т. п.

2. Контроль защищенности информации ограниченного доступа, например:

- Выявление технических каналов и способов несанкционированного доступа к информации;
- контроль эффективности применяемых средств защиты и т. п.

3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок, например:

- исследование персональных компьютеров, средств связи и обработки информации;
- исследование локальных вычислительных систем;
- оформление результатов исследований в соответствии с требованиями Гостехкомиссии Российской Федерации (РФ) и т. п.

4. Проектирование и разработка систем, документации по обеспечению информационной безопасности компании, например:

- разработка концепции информационной безопасности;
- проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
- проектирование помещений, предназначенных для ведения конфиденциальных переговоров и т. п.

В конце аудита разрабатывается план по внедрению новых технологий защиты. Стоит отметить, что аудит информационной безопасности не устраняет обнаруженных уязвимостей, а лишь фиксирует их наличие.

1.4. Виды аудита информационной безопасности

Чтобы гарантировать эффективную защиту от информационных атак злоумышленников и от потери информации, предприятиям необходимо иметь объективную оценку текущего уровня безопасности АС. Именно для этих целей и применяется аудит информационной безопасности.

Можно выделить следующие основные виды аудита информационной безопасности:

• экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;

• оценка соответствия рекомендациям Международных стандартов, а также требованиям руководящих документов ФСТЭК;

• инструментальный анализ защищенности АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечении системы;

• комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования;

В зависимости от тех задач, которые необходимо решить, каждый из вышеперечисленных видов аудита может проводиться по отдельности или в комплексе. В качестве объекта аудита может выступать как АС предприятия в целом, так и ее отдельные сегменты, в которых проводится обработка информации, подлежащей защите.

Рассмотрим более подробно различные виды аудита ИБ [16]:

Экспертный аудит представляет собой сравнение состояния ИБ с «идеальным» описанием, которое базируется на:

• требованиях, которые были предъявлены руководством в процессе проведения аудита;

• описании «идеальной» системы безопасности, основанном на аккумулированном в предприятии-аудиторе мировом и частном опыте.

При выполнении экспертного аудита сотрудники предприятия-аудитора совместно с представителями заказчика проводят следующие виды работ:

• сбор исходных данных об ИС, ее функциях и особенностях, используемых технологиях автоматизированной обработки и передачи данных;

• сбор информации об имеющихся организационно-распорядительных документах по обеспечению ИБ и их анализ;

• определение точек ответственности систем, устройств и серверов ИС;

• формирование перечня подсистем каждого подразделения компании с категорированием критичной информации и схемами информационных потоков.

Здесь важной частью проведения аудита является сбор данных об ИС путем интервьюирования представителей заказчика. Процесс делится на два этапа:

а) интервьюирование технических специалистов – сбор информации о функционировании сети;

б) опрос руководящего состава компании – выяснение требований, которые предъявляются к системе информационной безопасности.

Ключевой этап экспертного аудита – анализ проекта ИС, топологии сети и технологии обработки информации. В ходе анализа выявляются недостатки существующей топологии сети, снижающие уровень защищенности ИС.

Далее проводится анализ информационных потоков предприятия, позволяющий спроектировать систему обеспечения ИБ, которая будет соответствовать принципу разумной достаточности.

В рамках экспертного аудита производится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты и различного рода инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости, декларируемым целям и мерам ИБ. Особое внимание на этапе анализа информационных потоков уделяется определению полномочий и ответственности конкретных лиц за обеспечение ИБ различных участков/подсистем ИС. Полномочия и ответственность должны быть закреплены положениями организационно-распорядительных документов.

Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения ИБ, например:

• изменения (если они требуются) в существующей топологии сети и технологии обработки информации;

• рекомендации по выбору и применению систем защиты информации и других дополнительных специальных технических средств;

• предложения по совершенствованию пакета организационно-распорядительных документов;

• предложения по этапам создания системы ИБ;

• ориентировочные затраты на создание или совершенствование системы обеспечения информационной безопасности (СОИБ) (включая техническую поддержку и обучение персонала) [16].

Инструментальный анализ защищенности АС, или Активный аудит

Активный аудит – это исследование состояния защищенности ИС с точки зрения некоего злоумышленника, обладающего высокой квалификацией в области информационных технологии.

Активный аудит представляет собой сбор информации о состоянии системы сетевой защиты с помощью специального программного обеспечения и специальных методов. Под состоянием системы сетевой защиты понимаются лишь те параметры и настройки, использование которых помогает злоумышленнику проникнуть в сети и нанести урон предприятию. В процессе проведения данного вида аудита моделируется как можно большее количество таких сетевых атак, которые может выполнить злоумышленник.

Результатом активного аудита является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информации, доступной любому потенциальному нарушителю) сети заказчика.

По завершении данного вида аудита выдаются рекомендации по модернизации системы сетевой защиты, которые позволяют устранить опасные уязвимости и тем самым повысить уровень защищенности ИС от действий злоумышленника при минимальных затратах на ИБ.

Активный аудит необходимо проводить периодически для уверенности в том, что уровень безопасности ИС не снизился [16].

Аудит на соответствие стандартам

При его проведении состояние ИБ сравнивается с неким абстрактным описанием, приводимым в стандартах.

Официальный отчет, подготовленный в результате проведения данного вида аудита, включает следующую информацию:

• степень соответствия проверяемой ИС выбранным стандартам;

• степень соответствия собственным внутренним требованиям компании в области ИБ;

• количество и категории полученных несоответствий и замечаний;

• рекомендации по построению или модификации системы обеспечения ИБ, позволяющие привести ее в соответствие с рассматриваемым стандартом;

• подробная ссылка на основные документы заказчика, включая политику безопасности, описания процедур обеспечения ИБ, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании.

При обеспечении ИБ важно понимать, что:

• обеспечение ИБ – это непрерывный процесс, взаимоувязывающий правовые, организационные и программно-аппаратные меры защиты;

• в основе этого процесса лежит периодический анализ защищенности ИС в разрезе видов угроз и динамики их развития;

• ИС в своем развитии должна подвергаться периодическим реорганизациям, отправной точкой каждой из которых служит анализ выявленных уязвимостей при проведении аудита ИБ [16].

Дополнительные услуги. В ходе проведения аудита заказчику могут предлагается дополнительные услуги, которые напрямую связаны с оценкой состояния системы информационной безопасности, основанные на проведении специализированных исследований с использованием программно-аппаратных средств. Ярким примером является использование компаниями в своей информационной системе специализированного программного обеспечения собственной разработки. Поскольку подобное программное обеспечение является «уникальным», то и как таковых готовых, универсальных или

специализированных средств и технологий для их анализа на предмет защищенности и отказоустойчивости не существует. Поэтому в своей работе аудиторы прибегают к использованию: стресс-тестирования и/или теста на проникновение [16].

Стресс-тестирование — исследование производительности и стабильности работы системы, направленное на определение критических точек нагрузки, при которых система в момент атаки перестает адекватно реагировать на легитимные запросы пользователей. Тест на проникновение или пентест (от англ. Penetration Testing), инструмент анализа защищенности информационной системы основной целью которого является демонстрация того, к чему удалось получить доступ злоумышленнику, при текущем состоянии системы сетевой защиты.

Также, стоит более детально разобрать понятие «система тестирования» с используемом нами контексте, потому как данное понятие имеет довольно обширное определение. В общем случае, тестирование определяется как процесс, направленный на выявление характеристик информационной системы и демонстрацию различий между ее требуемым и фактическим состоянием (T.Koomen, M.Pol «Test Process Improvement»).

Первоочередными задачами тестирования являются определение соответствия предмета тестирования заданным спецификациям, а также определение пригодности объекта тестирования к выполнению тех или иных функций. В задачи тестирования не входит определение причин несоответствия заданным требованиям. Также, тестирование не обеспечивает само качество, но на его основе формируется представление о степени неопределенности качества системы.

Согласно стандарту ISO 9000 под качеством объекта тестирования понимается совокупность характеристик объекта, относящихся к его способности удовлетворить установленные или предполагаемые

требования. Другими словами, чем большему количеству требований соответствует тестируемый объект, тем выше его качество. К тому же тестирование не является отдельной деятельностью или направлением.

Тестирование — один из разделов диагностики и один из инструментов решения проблемы обеспечения качества объекта.

Полный перечень мероприятий по обеспечению качества объекта включает в себя три группы мероприятий [36]:

- Предупредительные — нацелены на предотвращение дефектов (например: методики, процедуры, шаблоны документов).
- Выявляющие — нацелены на нахождение недостатков (например, тестирование).
- Корректирующие — нацелены на устранение недостатков (например, исправление ошибок, найденные в ходе тестирования).

Таким образом, тестирование — это один из способов выявления дефектов. В свою очередь, выявление дефектов — это один из видов деятельности по обеспечению качества объекта. Тестирование определяется по-разному и зависит прежде всего от компании и/или от основных целей его проведения.

1.5. Анализ литературы и интернет-источников

1.5.1. Анализ печатных источников

На начальном этапе работы был проведен анализ большого количества информации, представленной, как в печатных источниках, так и Интернете. После глубокого изучения данного материала, было вынесено заключение о том, что полноценной информации по разработке регламента проведения аудита информационной безопасности как для предприятий, так и для образовательных учреждений как таковых не существует. Имеются отдельные наработки, в плане рассматриваемого теоретического материала по тому, как может проводится аудит информационной безопасности и какие этапы он может содержать.

Учебное пособие «Аудит безопасности фирмы: теория и практика» посвящено проблемам аудита информационной безопасности, как одного из направлений деятельности системы безопасности компании [38]. В данном учебном пособии рассматриваются как общие вопросы аудита безопасности компании, так и вопросы аудита отдельных направлений и областей информационной безопасности.

В книге «Аудит информационной безопасности» [7] рассматривается целый ряд вопросов, связанных с проведением аудита информационной безопасности на предприятии, даны основные понятия, показана роль анализа и управления информационными рисками. Также, в данной книге проводится описание международных и российских стандартов информационной безопасности, излагаются методологические основы применения стандартов ISO 15408 и ISO 17799 (ныне действующий стандарт ISO 27002-2013) для оценки рисков и управления информационной безопасностью, дана характеристика программных средств, применяемых при аудите информационной безопасности. Автор книги уделяет особое

внимание практическим вопросам методики проведения аудита информационной безопасности в компаниях различного типа и уровня.

Юрий Родичев в своем учебном пособии «Нормативная база и стандарты в области информационной безопасности» [28], рассматривает наиболее важные нормативные документы Федеральной службы по техническому и экспортному контролю (ФСТЭК), а также международные и национальные стандарты Российской Федерации (РФ) в области информационной безопасности, так как на основании рассматриваемой нормативно-правовой базы выстраивается методика проверки предприятия на предмет соответствия существующей политики информационной безопасности тому или иному закону, стандарту, постановлению и т. п.

В учебном пособии А.В. Солодянникова «Информационная безопасность автоматизированных систем» [29] раскрываются основные понятия, требования, этапы, содержание аудита, а также необходимый перечень исходных данных, необходимых для проведения аудита.

Не менее полезной является книга Александра Астахова «Искусство управления информационными рисками» [9], где генеральный директор GlobalTrust, основатель портала ISO27000.ru, эксперт по информационной безопасности, ведущий преподаватель BSI, сертифицированный аудитор (CISA), главный редактор русских переводов британских и международных стандартов по информационной безопасности, управлению рисками и непрерывностью бизнеса, знакомит с основами управления рисками ИБ, а также с эффективной практикой оценки, анализа и обработки рисков, акцентирует свое внимание на особенности проведения каждого из вида аудита и рассматривается подробная классификация оказываемых при проведении аудита услуг.

1.5.2. Анализ интернет-источников

В «лекции 12. Этапы проведения аудита» (рисунок 1.1), » [10] (рисунок 1), дается определение понятию «аудит информационной безопасности» и приводится подробная характеристика его составляющих, включая основные виды аудита. Также, автор статьи детально описывает основные этапы работ при проведении аудита в компании-заказчике, включая используемые методы и необходимый для проведения аудита перечень исходных данных.

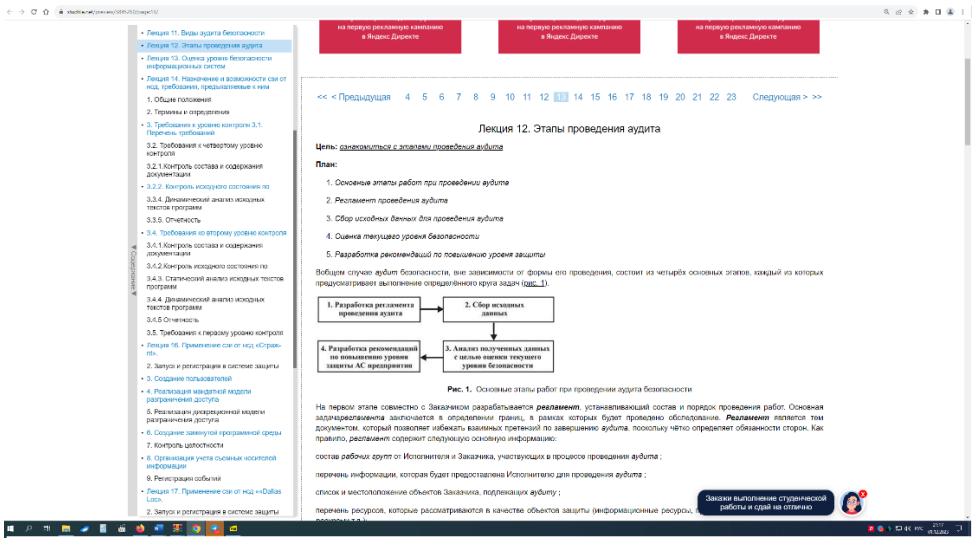

Рисунок 1.1 – Веб-портал https://studfile.net/

Александр Панасенко являясь автором другой статьи на тему «Как провести экспресс-аудит информационной безопасности» (рисунок 1.2), в которой помогает оперативно оценить общее состояние СОИБ в организации, выявить проблемные места, оценить уровень соответствия требованиям регуляторов, а также выработать стратегию комплексной защиты компании от разного рода угроз.

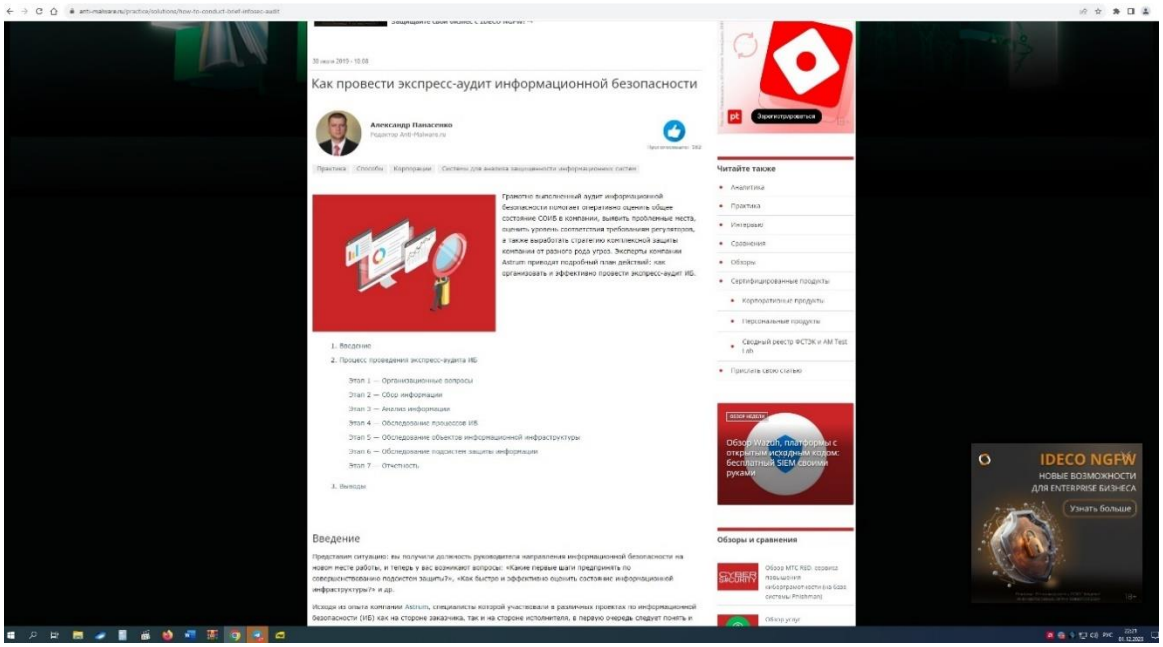

Рисунок 1.2 – Веб-портал https://www.anti-malware.ru/

Кандидат технических наук, эксперт по информационной безопасности, исполнительного директора компании «Digital Security» [30] Илья Давидович Медведовский, в своей работе под названием «Практическое применение международного стандарта информационной безопасности ISO 17799» (рисунок 1.3) описывает критерии оценки защищенности информационных систем, критерии проведения аудита безопасности информационных систем, практическое применение международного стандарта ISO 17799 (ныне действующий стандарт ISO 27002-2013). Данная работа И. Д. Медведовского нашла свою реализацию в программном продукте «Кондор».

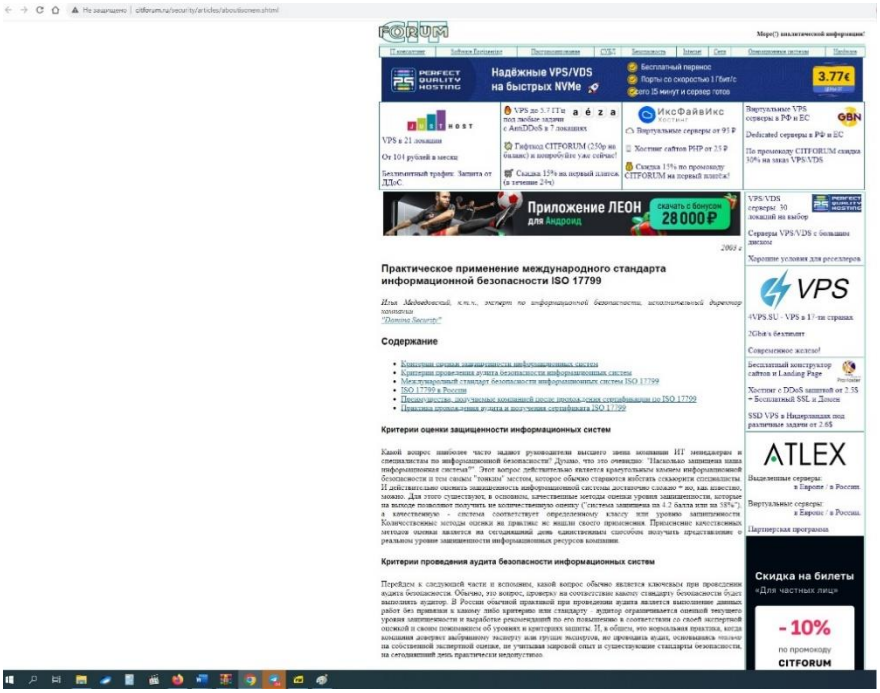

Рисунок 1.3 — Веб-портал CitForum

В своей работе «Стандарт на страже информационной безопасности» [35] (рисунок 1.4) эксперт С. И. Игнатенко раскрывает необходимость и важность использования и практическую пользу от применения международных стандартов в сфере информационной безопасности, в частности международного стандарта ISO 17799 (ныне действующий стандарт ISO 27002-2013). Эксперт информационной безопасности сообщает, что «в связи с ростом зависимости организаций от информационных систем и сервисов происходит резкое увеличение рисков, связанных с недостаточным уровнем обеспечения безопасности получения, хранения и обработки информации. Сложность информационных систем и необходимость их интеграции в общедоступные приводит к невозможности или значительному затруднению осуществления контроля над обеспечением безопасности информации и ресурсов. Возникает острая необходимость в стандартизации систем и процессов информационной безопасности»

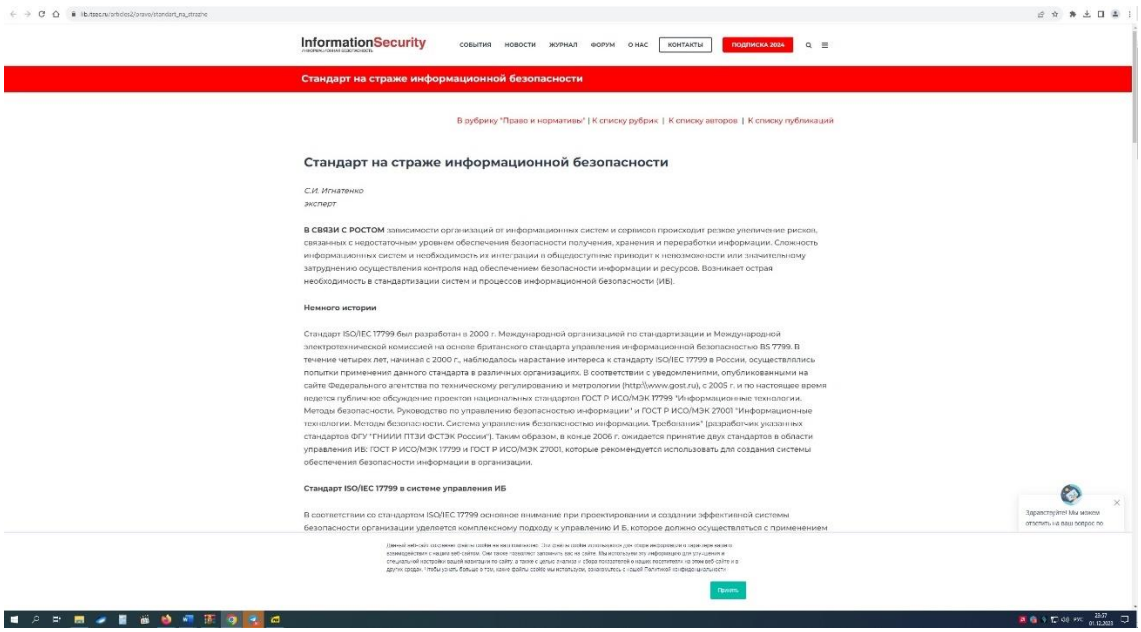

Рисунок 1.4 — Веб-портал https://lib.itsec.ru/

1.5.3. Программные продукты при проведении проверок

На практике аудиторы, занятые в сфере информационной безопасности, при проведении проверок пользуются несколькими программными продуктами:

1. Программное обеспечение RiskWatch, разрабатываемое американской компанией, является довольно мощным инструментом анализа и управления рисками, по сравнению со своими конкурентами. Также, этим его отличает крайне высокая стоимость. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности и анализа рисков:

- RiskWatch for Physical Security — служит для оценки физических методов защиты информационной системы;
- RiskWatch for Information Systems — разработано для оценки информационных рисков;

- RiskWatch RW17799 for ISO17799 — используется для оценки требованиям стандарта ISO17799 (ныне действующий стандарт ISO 27002-2013).

2. Система COBRA, разрабатываемая австралийской компанией Risk Associates — инструмент для анализа рисков и оценки соответствия информационной системы стандарту ISO 17799 (современный аналог ISO 27002-2013). COBRA реализует методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям, а также большое количество вопросников, с успехом применяемые на практике [26].

Выводы по первой главе

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

Сформулированы понятия информационной безопасности образовательного учреждения, информационных систем, автоматизированных информационных систем и т.д. Описаны основные задачи автоматизации.

Аудит информационной безопасности является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости организации от угроз информационной безопасности. Кроме того, результаты аудита являются основой для формирования стратегии развития системы обеспечения информационной безопасности организации.

Аудитор в компании может реализовывать разные цели, однако, в первую очередь проверка должна определить уровень защищенности компании, выявить риски, сформировать перечень слабых мест.

Можно выделить основные виды аудита информационной безопасности:

•экспертный аудит безопасности;

•аудит на соответствие стандартам;

•инструментальный анализ защищенности АС;

•комплексный аудит.

Проведен анализ литературы и интернет-источников по аудиту и менеджменту информационной безопасности, анализу и управлению рисками на предприятиях.

Глава 2. Обоснование теоретических и методологических аспектов обеспечения и проведения аудита информационной безопасности

2.1. Угрозы и меры защиты информационной безопасности

Под угрозами безопасности информационной системы понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными, непреднамеренными воздействиями на нее.

Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности учреждения при реализации угроз в информационной сфере.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются следующие группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

- ✓ компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
- ✓ программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
- ✓ данные, хранимые как на жестких дисках, так и на отдельных носителях;
- ✓ сам персонал, отвечающий за работоспособность IT-систем;
- ✓ дети, подверженные внешнему агрессивному информационному влиянию и способные создать в образовательном учреждении криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы, направленные на повреждение любого из компонентов системы, могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения персонала, учащихся или третьих лиц, можно назвать:

- ✓ любые аварийные ситуации, например, отключение электроэнергии или затопление;
- ✓ ошибки персонала;
- ✓ сбои в работе программного обеспечения;

- ✓ выход техники из строя;
- ✓ проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться учащиеся, служащие, конкуренты, третьи лица с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание детей, но и это не исключено. И самой серьезной опасностью станет использование школьного оборудования для вовлечения ребенка в криминал и терроризм.

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Можно выделить несколько видов несанкционированного доступа:

Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по различным каналам связи, например по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Меры защиты

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях, причем работа должна носить комплексный характер. Существует ряд методических разработок, которые позволят построить защиту образовательного учреждения на необходимом уровне.

Нормативно-правовой способ защиты информационной безопасности

В России принята «Национальная стратегия действий в интересах детей», определяющая степень угроз и меры защиты их безопасности. Действия по ограничению агрессивного воздействия на сознание ребенка должны стать основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в

этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

Морально-этические средства обеспечения информационной безопасности

В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих подростка от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо применять нормы закона «О защите прав ребенка», определяющие его права на защиту от сведений, которые могут причинить моральную травму. Необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику детей, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

Административно-организационные меры

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа детей к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа ребенка, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

Физические меры

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

Технические меры

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов.

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ учащегося на определенные сайты (контент-фильтры).

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей учеников, в ряде случаев они помогут провести аудит мер безопасности и порекомендовать современные решения. На основании анализа поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

Как правило, защита от угроз, в основном регламентируется инструкциями, разработанными и утвержденными в образовательной организации с учетом особенностей эксплуатации информационных систем организации и действующей нормативной базой учреждения.

2.2. Основные этапы проведения аудита информационной безопасности

Работы по аудиту безопасности ИС включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ—аудита автоматизированной системы, включающего в себя [9]:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- использование методов анализа рисков (необязательно);
- оценка соответствия требованиям стандартов (необязательно);
- выработку рекомендаций;
- подготовку аудиторского отчета.

Инициирование процедуры аудита. В основном инициатором проведения аудита информационной безопасности становится руководство организации, которое в наибольшей мере заинтересовано в его проведении. Аудит информационной безопасности — довольно трудоемкий, длительный и всеобъемлющий процесс, в который вовлечены очень многие, а в основном все структурные подразделения и сотрудники организации.

На этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы [9]:

- права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;
- аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
- в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники организации обязаны оказывать

содействие аудитору и предоставлять всю необходимую для проведения аудита информацию;

- На этапе инициирования процедуры аудита должны быть определены границы проведения обследования.

Границы проведения обследования определяются в следующих терминах:

- список обследуемых физических, программных и информационных ресурсов;

- площадки (помещения), попадающие в границы обследования;

- основные виды угроз безопасности, рассматриваемые при проведении аудита;

- организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, их приоритеты (в каком объеме они должны быть учтены).

План и границы проведения аудита обсуждаются на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений.

Сбор информации аудита. Данный этап проведения аудита является наиболее длительным и сложным. Это связано в основном с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации, а также на сколько полно и своевременно аудитор получает необходимую для проверки документацию от должностных лиц и уполномоченных помогать аудитору.

Качество аудита безопасности во многом зависит от полноты и точности информации, полученной в процессе сбора исходных данных. Поэтому в нее необходимо включить следующие данные, подробный перечень исходных данных представлен в таблице 2.1 [9].

Таблица 2.1 – Перечень исходных данных, необходимых для аудита безопасности

Тип информации	Состав исходных данных
Организационно-распорядительная документация по вопросам информационной безопасности	• политика информационной безопасности ИС; • руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации; • регламенты работы пользователей с информационными ресурсами ИС
Информация об аппаратном обеспечении хостов	• перечень серверов, рабочих станций и коммуникационного оборудования, установленного в ИС; • аппаратные конфигурации серверов и рабочих станций; • сведения о периферийном оборудовании
Информация об общесистемном ПО	• сведения об ОС, установленных на рабочих станциях и серверах; • сведения о СУБД, установленных в ИС
Информация о прикладном ПО	• перечень прикладного ПО общего и специального назначения, установленного в ИС; • описание функциональных задач, решаемых с помощью прикладного ПО
Информация о средствах защиты, установленных в ИС	• производитель средства защиты; • конфигурационные настройки средства защиты; • схема установки средства защиты
Информация о топологии ИС	• карта локальной вычислительной сети, включая схему распределения серверов и рабочих станций по сегментам сети; • типы каналов связи, используемых в ИС; • используемые в ИС сетевые протоколы; • схема информационных потоков ИС

Компетентные выводы относительно положения дел в организации с информационной безопасностью могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа. Первый пункт аудиторского обследования начинается с получения информации об организационной структуре пользователей ИС и обслуживающих подразделений. Назначение и принципы функционирования ИС во многом определяют существующие риски и требования безопасности, предъявляемые к системе. Далее, аудитору требуется более детальная информация о структуре ИС. Это позволит уяснить, каким образом

осуществляется распределение механизмов безопасности по структурным элементам и уровням функционирования ИС.

Получение информации о принятых в организации процедурах информационной безопасности, о функционировании и текущем состоянии информационной системы осуществляется аудитором в ходе специально проводимого интервьюирования ответственных лиц компании.

Обычно в ходе интервью аудитор задает опрашиваемым следующие вопросы:

- Кто является владельцем информации?
- Кто является пользователем (потребителем) информации?
- Кто является провайдером услуг?
- Какие услуги и каким образом предоставляются конечным пользователям?
- Какие основные виды приложений функционирует в ИС?
- Количество и виды пользователей, использующих эти приложения?

Ему понадобится также следующая документация, если таковая вообще имеется в наличии:

- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений;
- другая проектная и рабочая документация на информационную систему.

Основными методами сбора исходных данных для аудита информационной безопасности являются анкетирование, обследование и скрытый аудит, последний подразделяется на активный и пассивный.

Анкетирование. С практической точки зрения большинство стандартов по ИБ может применяться как средство аудита системы безопасности информации. При этом большинство методик, основанных на этих

стандартах в качестве механизма сбора исходных данных, рекомендуют использовать анкетирование (в том числе и анонимное анкетирование) сотрудников проверяемой организации.

Как показывает опыт проведения аудита ИБ, в России подобный метод сбора исходных данных может использоваться только в комплексе с другими, поскольку данные, получаемые при анкетировании, не отражают объективной картины состояния ИБ в организации.

Это объясняется следующими основными причинами:

боязнь сотрудников быть наказанным за предоставление «негативной» информации об организации;

желание сотрудников продемонстрировать полное выполнение должностных инструкций;

желание сотрудников дать негативную информацию о подразделении и его руководстве;

формальное отношение к заполнению анкет;

отсутствие мотивации к заполнению анкет.

Обследование. Обследование или обследование, совмещенное с интервьюированием сотрудников, является наиболее трудоемким, но и наиболее результативным механизмом сбора исходных данных для аудита информационной безопасности.

В ходе проведения обследования аудиторы оценивают степень соответствия компонентов и процессов информационной системы (нормативных и организационных документов, состава и характеристик используемых средств защиты, архитектуры и порядка эксплуатации технических средств) требованиям стандартов по ИБ и требованиям Заказчика.

В рамках обследования полностью изучаются сети и оборудование связи, арендуемые и собственные каналы связи, серверные и настольные платформы, используемое сетевое и прикладное программное обеспечение с точки зрения информационной безопасности. Кроме того, проводится анализ используемых средств защиты информации (антивирусных продуктов, межсетевых экранов, технологий виртуальных частных сетей и открытых ключей и т.п.).

Отдельным моментом служит тестирование работы служб информационной безопасности и информационных технологий обследуемой организации в вопросе обеспечения ИБ, а именно: каким образом происходит отслеживание инцидентов информационной безопасности в рамках информационной системы? Какова практика реагирования на эти инциденты, и закреплена ли она в официальных документах компании? Каков уровень подготовки специалистов компании в области ИБ?

Все это также должно быть отражено в результатах обследования.

Скрытый аудит. Основным недостатком всех процедур публичного сбора исходных данных для аудита является предоставление Исполнителю искаженных исходных данных. Типичным примером является, например, ситуация, в которой сотрудники реально не соблюдают требования должностных инструкций, но при анкетировании и интервьюировании утверждают обратное, а при работе в присутствии аудитора в точности следуют инструкциям. Подобные ситуации достаточно распространены и связаны с тем, что сотрудники организации информированы о проведении аудита. Для того чтобы их избежать, используют технологию скрытого аудита.

Скрытый аудит информационной безопасности — это процедура, являющаяся составной частью сбора исходных данных для аудита, в ходе которой аудиторы получают исходные данные без информирования

подавляющего большинства сотрудников организации о проведении аудита.

Дополнительным плюсом скрытого аудита ИБ является возможность контроля за реакцией сотрудников, ответственных за защиту информации, на действия аудиторов.

Пассивный скрытый аудит заключается в том, что процедура сбора данных для аудита ИБ маскируется под процедуры сбора исходных данных для иных целей. Наиболее часто в качестве маскирующих целей выступают:

- сбор исходных данных для внедрения системы управления качеством;
- сбор исходных данных для проектирования (реконструкции) корпоративных информационных системах (КИС);
- подготовительные работы по модернизации программного обеспечения;
- аудит информационных технологий;
- сбор исходных данных для реорганизации управления.

Целью скрытого пассивного аудита является получение максимально объективной картины в ходе наблюдения за действиями сотрудников, а также в ходе собеседования с ними.

Активный скрытый аудит подразумевает возможность доступа аудитора к ресурсам сети связи операторами ресурсам КИС. Как и пассивный, он маскируется под мероприятия, которые проводятся в компании, но не связаны с ИБ. Обычно такими мероприятиями являются:

расширение штатов — набор новых сотрудников (которые в действительности являются аудиторами);

внедрение нового программного или технического обеспечения, в ходе которого сотрудникам организации-подрядчика предоставляется доступ к сети связи и КИС;

регламентные работы по обслуживанию серверов, сетевого оборудования, иных объектов сети связи и КИС.

Целью скрытого активного аудита является получение максимального объема информации о техническом состоянии сети и объектов связи, КИС, используемых средствах защиты информации и возможностях по их преодолению. При этом важным моментом (более важным, чем при пассивном скрытом аудите) является изучение качества реагирования сотрудников, ответственных за соблюдение режима информационной безопасности, на действия аудиторов.

Анализ данных аудита. Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита [9]:

Первый подход, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, учитывающий особенности данной ИС, среды её функционирования и существующие в данной среде угрозы безопасности.

Второй подход, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, её принадлежности, а также назначения. Аудитор должен определить набор требований стандарта, соответствие которым нужно обеспечить.

Третий подход предполагает комбинирование первых двух, поэтому является наиболее эффективный. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные

требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков.

Если для проведения аудита безопасности выбран подход, базирующийся на Использование методов анализа рисков, то на этапе анализа данных аудита обычно выполняется следующий набор задач:

- анализ ресурсов организации, включая информационные ресурсы, программные и технические средства, а также людские ресурсы;
- анализ групп задач, решаемых системой, и бизнес-процессов;
- построение (неформальной) модели ресурсов организации, определяющей взаимосвязи между информационными, программными, техническими и людскими ресурсами, их взаимное расположение и способы взаимодействия;
- оценка критичности Информационных ресурсов, а также программных и технических средств;
- определение критичности ресурсов с учетом их взаимозависимостей;
- определение наиболее вероятных угроз безопасности в отношении ресурсов организации и уязвимостей защиты, делающих возможным осуществление этих угроз;
- оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществлении угроз;
- определение величины рисков для каждой тройки: угроза группа ресурсов - уязвимость.

Перечисленный набор задач является достаточно общим. Для их решения могут использоваться различные формальные и неформальные, количественные и качественные, ручные и автоматизированные методики анализа рисков. Суть подхода от этого не меняется.

Оценка рисков может даваться с использованием различных как качественных, так и количественных шкал. Главное, чтобы существующие

риски были правильно идентифицированы и упорядочены в соответствии со степенью их критичности для организации. На основе такого анализа может быть разработана система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

В случае проведения аудита безопасности на соответствие требованиям стандарта аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой организации и ее соответствие этим требованиям. Данные о соответствии организации требованиям стандарта обычно представляются в табличной форме. Из таблицы будет видно, какие требования безопасности не реализованы. Исходя из этого делаются выводы о соответствии обследуемой организации требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.

Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита. В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты. В то же время наивно ожидать от аудитора, в качестве результата проведения аудита, выдачи технического проекта подсистемы информационной безопасности, либо детальных рекомендаций по внедрению конкретных программно-технических средств защиты информации. Это требует более детальной проработки конкретных вопросов организации защиты, хотя внутренние аудиторы могут принимать в этих работах самое активное участие [9].

На последнем этапе проведения аудита информационной безопасности разрабатываются рекомендации по совершенствованию организационно-технического обеспечения предприятия. Такие рекомендации могут включать в себя следующие типы действий, направленных на минимизацию выявленных рисков:

- уменьшение риска за счёт использования дополнительных организационных и технических средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от неё. Так, например, установка межсетевых экранов в точке подключения АС к сети Интернет позволяет существенно снизить вероятность проведения успешной атаки на общедоступные информационные ресурсы АС, такие как Web-серверы, почтовые серверы и т.д.;
- уклонение от риска путём изменения архитектуры или схемы информационных потоков АС, что позволяет исключить возможность проведения той или иной атаки. Так, например, физическое отключение от сети Интернет сегмента АС, в котором обрабатывается конфиденциальная информация, позволяет исключить атаки на конфиденциальную информацию из этой сети;
- изменение характера риска в результате принятия мер по страхованию. В качестве примеров такого изменения характера риска можно привести страхование оборудования АС от пожара или страхование информационных ресурсов от возможного нарушения их конфиденциальности, целостности или доступности. В настоящее время российских компаний уже предлагают услуги по страхованию информационных рисков;
- принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для АС.

Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до

приемлемого остаточного уровня. При выборе мер по повышению уровня защиты АС учитывается одно принципиальное ограничение – стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов.

Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Он должен, по крайней мере, содержать описание целей проведения аудита, характеристику обследуемой ИС, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие её требованиям стандартов, и, конечно, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

В завершении процедуры аудита его результаты оформляются в виде отчётного документа, который предоставляется Заказчику. В общем случае этот документ состоит из следующих основных разделов:

- описание границ, в рамках которых был проведён аудит безопасности;
- описание структуры АС Заказчика;
- методы и средства, которые использовались в процессе проведения аудита;
- описание выявленных уязвимостей и недостатков, включая уровень их риска;
- рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности;
- предложения по плану реализации первоочередных мер, направленных на минимизацию выявленных рисков [9].

2.3. Требования к аккредитации компаний, занимающихся аудитом информационной безопасности

В соответствии с требованиями законодательства РФ, любая организация, использующая в своей деятельности какие-либо конфиденциальные данные, обязана обеспечивать безопасность их обработки и хранения.

Аудит информационной безопасности позволяет получить независимую качественную и количественную оценку защищенности корпоративной информационной системы, оценить ее соответствие предъявляемым нормативным и корпоративным требованиям безопасности.

Аудит информационной безопасности включает:

- Анализ защищенности информационных систем.
- Анализ угроз нарушения информационной безопасности.
- Оценку информационных рисков и воздействия на бизнес.
- Оценку соответствия требованиям стандартов.
- Аттестацию и сертификацию по требованиям безопасности информации РД ФСТЭК России.

Зачастую компании не имеют собственных квалифицированных специалистов, способных провести оценку имеющейся информационной системы, и отдают этот вид деятельности на аутсорсинг.

Прежде чем заниматься аудитом информационной безопасности, организация должна пройти аккредитацию на проведение сертификационной оценки.

Еще несколько лет назад не существовало четких требований к компаниям, осуществляющим аудит информационной безопасности.

Существуют основные требования к аккредитации организаций, предоставляющих услуги аудита информационной безопасности, существующие в настоящее время.

В первую очередь компания должна иметь лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

Под технической защитой конфиденциальной информации понимается выполнение работ или оказание услуг, определенных Постановлением Правительства РФ от 3 февраля 2012 г. № 79, в том числе аттестационные испытания и аттестация на соответствие требованиям по защите информации.

На сайте ФСТЭК можно найти и скачать реестр лицензий на деятельность по технической защите конфиденциальной информации, который содержит номера выданных лицензий, дату выдачи, срок действия, наименование лицензиата, адрес места нахождения и осуществления деятельности.

Лицензия ФСТЭК требует наличия у организации действующей лицензии ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну.

Также организация, занимающаяся аудитом информационной безопасности должна осуществлять свою деятельность в соответствии со стандартом ГОСТ Р ИСО/МЭК 27006-2008 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

Данный стандарт устанавливает требования к организациям, осуществляющим аудит и сертификацию системы менеджмента информационной безопасности. Он также может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки и других процессов аудита.

Требования ГОСТа Р ИСО/МЭК 27006-2008 содержат нормативные ссылки на следующие стандарты:

- ИСО/МЭК 17021:2006 «Оценка соответствия. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента»;
- ИСО/МЭК 27001:2005 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [20];
- ИСО/МЭК 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

Традиционная аудиторская деятельность в РФ регулируется рядом нормативных документов, например Федеральным законом от 30.12.2008 307-ФЗ: «Об аудиторской деятельности». Ее целью является проверка финансовой отчетности организации и консультационные услуги, однако при этом существует объективная необходимость правового сопровождения аудита ИБ при сохранении традиционных принципов (независимость проверки, наличие квалификационного аттестата аудитора, его деловая репутация, обязанность хранить тайну проверяемых организаций). В процессе осуществления аудиторской проверки ИБ вуза целесообразно также проверять выполнение таких правовых документов, как:

- Федеральный закон от 27.07.2006 №152-ФЗ: «О защите персональных данных»;
- Федеральный закон от 06.04.2011 №63-ФЗ: «Об электронной подписи»;
- Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности РФ»;

Одной из важных особенностей стандарта является наличие требований к компетентности персонала компании, занимающейся аудитом информационной безопасности:

- знание стандарта СМИБ и других соответствующих нормативных документов;
- понимание вопросов информационной безопасности;
- понимание оценки риска и менеджмента риска с точки зрения деятельности;
- технические знания о деятельности, подлежащей аудиту;
- общие знания нормативных требований, относящихся к СМИБ;
- знание систем менеджмента;
- понимание принципов аудита, основанных на ИСО 19011:2002;
- знание анализа эффективности СМИБ и измерения эффективности средств контроля.

2.4. Разработка методики для составления регламента проведения аудита информационной безопасности

Процесс аудита информационной безопасности является периодически независимым и документированным, проводится в целях получения свидетельств аудита и объективной оценки предприятия.

В процессе проведения аудита, происходит оценка состояния информационной системы предприятия на соответствие стандартам информационной безопасности. Ниже приведены примеры таких документов:

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (далее – РД для АС);
- «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К);
- «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (ГОСТ Р ИСО/МЭК 15408-2002 или «Общие критерии») [32];

А также зарубежные и международные стандарты:

- Международный стандарт ISO/IEC 15408 - Современный аналог данного стандарта в РФ носит ГОСТ Р ИСО/МЭК 15408 «Информационная технология (ИТ) [32]. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

В стандарте выделены 11 классов функциональных требований: аудит безопасности; связь (передача данных); криптографическая поддержка (криптографическая защита); защита данных пользователя; идентификация и аутентификация; управление безопасностью; конфиденциальность; защита функций безопасности объекта; использование ресурсов; доступ к объекту оценки; доверенный маршрут/канал.

▪ Международные стандарты ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 27002 взаимосвязаны друг с другом, потому как посвящены вопросам управления (менеджменту) информационной безопасностью.

- В стандарте ISO 27001 аккумулированы описания лучших мировых практик в области управления информационной безопасностью. Современный аналог в РФ носит название ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [30].

- Международный стандарт ISO/IEC 27002:2013 был разработан в 2005 году на основе стандарта ISO 17799. Он содержит более полное описание и рекомендации по внедрению средств управления информационной безопасностью по сравнению с ISO/IEC 27001:2013. В РФ современный аналог стандарта носит название ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [21].

На сегодняшний день оценка рисков информационной безопасности на предприятиях производится на основании международного стандарта ISO/IEC 27002 [21].

Таким образом, следует определить аспекты обеспечения безопасности, по которым будет производиться внутренний аудит: Физическая безопасность; Техническая безопасность; Защита персональных данных; Обучение и осведомленность персонала; Реагирование на инциденты; Защита от внешних угроз; Управление информационной безопасностью.

2.5. Физическая безопасность информационных объектов

Используя в работе даже самое надежное оборудование в мире- оно будет работать плохо, если оно не обеспечено стабильной электроэнергией или должным охлаждением. Отсюда возникает необходимость в обеспечении защиты от факторов окружающей среды (температуры, влажности и даже огня). В рамках процесса необходимо рассмотреть следующие вопросы:

- физическое место для расположения оборудования. Места должно быть достаточно не только для имеющегося оборудования, но и для расширения в будущем;
- физическое место для сотрудников ИТ, которые занимаются сопровождением. Так как в данном случае дело касается людей, а не оборудования, окружающая обстановка должна быть комфортна в точки зрения человеческих потребностей. Например, комфортная температура и устранение шума от техники. Здесь также необходимо учитывать требования санитарных норм;
- электроэнергия. Электрообеспечение оборудования должно быть стабильным;
- система охлаждения;
- влажность. Необходимо соблюдать допустимые пределы влажности, чтобы оборудование не вышло из строя.

Второе задача процесса – обеспечение физической безопасности, то есть защита от несанкционированного доступа к оборудованию и данным. Для предотвращения:

- ограничение физического доступа. Например, сервера могут располагаться в выделенном помещении с электронными идентификаторами для входа;
- охрана;

- видеонаблюдение;
- и т.п.

Помимо этого, в задачу обеспечения физической безопасности входит защита от естественных угроз:

- землетрясение: постарайтесь расположить дата-центр вдали от зон с сейсмической активностью;
- наводнение: постарайтесь не располагать дата-центр на первых этажах и в подвалах;
- пожар: используйте датчики дыма или температурные датчики для быстрого обнаружения угрозы. Сюда также входит разработка плана эвакуации, размещение пожаротушителей в здании и т.п.;
- утечка воды: утечка воды возможна от системы кондиционирования, помещений сверху (туалет или кухня). Старайтесь не располагать дата-центр вблизи от возможных источников воды и т.п.

2.5.1. Требования к помещениям для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение в котором будут располагаться рабочие места, оборудование ЭВМ с Видеодисплейным терминалом (ВДТ).

По требованиям СанПиН 2.2.2/2.4.1340-03 помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 лк. Освещенность поверхности экрана не должна быть более 300лк. Коэффициент пульсации не должен превышать 5 %;

2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Рабочие столы следует размещать таким образом, чтобы естественный свет падал преимущественно слева;

5. Не допускается размещение мест пользователей ПЭВМ во всех образовательных учреждениях в цокольных и подвальных помещениях;

6. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 м2 для сотрудников и обучающихся, 6 м2 для персонала по обслуживанию средств вычислительной техники и информатики (СВТИ);

7. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки.

8. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. Поверхность рабочего стола должна иметь коэффициент отражения 0,5-0,7;

9. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7 - 0,8; для стен - 0,5 - 0,6; для пола - 0,3 - 0,5;

10. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;

11. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ;

12. Профилактика компьютерной и офисной техники должна осуществляться ИТ-Администратором не реже, чем два раза в год.

2.5.2. Требования к микроклимату и уровню шума на рабочих местах

1. Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА.

В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

2. Температура воздуха в помещениях - 20°±2 °С (не более 25 °С).

3. Относительная влажность воздуха - 20-70 % (не более 75 % в холодный период, в теплый для 25 °С - не более 65 %, для 24 °С и ниже - не более 70 %).

4. Оптимальная скорость потока воздуха - 0,2 м/с (не более 0,3 м/с для холодного, 0,5 м/с для теплого периодов).

5. Запыленность воздуха помещений не должна превышать: в серверной - 0,75 мг/м3, с размерами частиц не более 3 мкм (атм. пыль, сажа, дым, споры, асбест); в помещениях обработки данных - 2 мг/м3.

6. Допустимый уровень вибрации не должен превышать по амплитуде 0,1 мм и по частоте 25 Гц.

2.5.3. Требования по вентиляции и кондиционированию воздуха

1. Кроме систем центрального отопления и вентиляции с механическим побуждением в помещениях для средств вычислительной техники и информатики (СВТИ) по требованию Заказчика устанавливаются системы кондиционирования воздуха и пылеудаления.

2. Система центрального кондиционирования воздуха здания и помещений для СВТИ должна обеспечивать в любое время года температуру, относительную влажность, скорость движения и максимально возможную рециркуляцию воздуха в рабочей зоне с параметрами не хуже, чем это указано в разделе 3

3. При подаче охлажденного воздуха непосредственно в устройства (стойки с аппаратурой) температура его на входе не должна быть ниже 14 °С, относительная влажность не более 75 %. Подача воздуха должна осуществляться по воздуховодам или из подпольного пространства. Вытяжные отверстия следует размещать над оборудованием, выделяющим тепло (особенно для ИБП).

4. В холодный период года система кондиционирования не должна допускать выпадения конденсата на поверхностях помещений.

2.5.4. Требования по электроснабжению, заземлению и к электробезопасности

1. Электроснабжение, силовое электрооборудование и электрическое освещение зданий и помещений для СВТИ необходимо выполнять по требованиям ПУЭ-2000, ВСН-59-88, а также других нормативных документов.

2. Для СВТИ сеть электропитания должна быть выделенной и помехозащищенной (ВЭПС) и выполнена по 5-проводной схеме (TN-S) в магистральной части и по 3-проводной схеме в групповой с использованием розеток с заземляющим контактом.

Технология ВЭПС и соответствующее помехозащитное оборудование на объекте будет приводит к радикальному улучшению условий работы СВТИ, практически полному исчезновению сбоев в работе и уменьшению случаев преждевременного выхода оборудования из строя, увеличению его рабочего ресурса.

3. СВТИ рекомендуется относить к группе электроприемников I категории. Такое требование актуально для образовательных организаций, использующих информационные технологии, остановка которых повлечет за собой потерю информации или прерывание процесса управления.

4. Для исключения потери информации, хранящейся на магнитных носителях (дисковых системах памяти), при кратковременном исчезновении напряжения в сетях электропитания в качестве третьего независимого источника должны предусматриваться источники бесперебойного питания (ИБП, UPS).

5. Для увеличения времени автономии при отключении электропитания или недопустимо низком его качестве можно оборудовать здание автоматическим дизель генератором (ДГ), обеспечивающим неотключаемую нагрузку СВТИ.

6. Расчет электрических нагрузок для СВТИ следует производить с учетом коэффициентов использования: для СВТИ в серверной - 0,9-1,0 (при числе серверов 3 и более); для копировально-множительной техники - 0,7-0,75; для рабочих мест - 0,5.

7. Штепсельные розетки для питания маломощных электроприемников СВТИ рекомендуют подключать по магистральной схеме, группируя по 3-5 рабочих мест (3 розетки с заземляющим проводом на одно рабочее место).

При большом количестве розеток в помещении (например, серверная) для обеспечения надежности, ремонтопригодности или технического обслуживания без отключения другой аппаратуры потребители разбиваются на вторичные группы с установкой автоматических выключателей. Автоматические выключатели групп в серверной из-за повышенной мощности СВТИ и больших пусковых токов устанавливаемого оборудования должны выбираться на большие токовые нагрузки.

8. Заземление устройств СВТИ предусматривается их технической документацией. В здании, имеющем ВЭПС, должен быть предусмотрен контур технологического заземления с сопротивлением заземления не более 1 Ом, который выполняется отдельно от защитного заземления.

9. Условия эксплуатации СВТИ должны соответствовать требованиям по защите от помех в соответствии с ГОСТ Р50839-95 "Совместимость технических средств электромагнитная. Устойчивость средств вычислительной техники и информатики к электромагнитным помехам. Требования" и ГОСТ 50628-93 "Совместимость электромагнитная машин электронных вычислительных персональных. Устойчивость к электромагнитным помехам. Технические требования". Особое внимание следует уделить требованиям к защите от: - электростатических разрядов; - наносекундных импульсных помех в цепях электропитания переменного тока и в цепях ввода/вывода; - динамических изменений напряжения

(прерывания, провалы, выбросы) сети электропитания; - микросекундных импульсных помех большой энергии в цепях электропитания.

10. Отдельные локальные вычислительные сети (центры) могут оборудоваться собственными заземлителями и молниеотводами, устройствами внутренней грозозащиты.

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

2.5.5. Специальные требования по пожарной безопасности

1. Основой для пожарной безопасности служат нормативные документы, утвержденные в установленном порядке по согласованию с ГУ Государственной противопожарной службы МВД России.

Нормы пожарной безопасности НПБ 110-99 определяют перечень зданий сооружений, помещений и оборудования, которые должны быть защищены автоматическими установками пожаротушения (АУПТ) и пожарной сигнализации (АУПС), которые проектируются в соответствии со СНиП 2.04.09-84.

Противопожарная защита устанавливается обязательно и независимо от ведомственной принадлежности, организационно-правовой формы и площади помещений.

2. Помещения для СВТИ относятся в соответствии гл. 7.4 Правил устройства электроустановок (ПУЭ) к классу пожаробезопасности П-IIа (степень огнестойкости).

3. Помещения, где установлены СВТИ (серверная), от помещений другого назначения должны отделяться несгораемыми стенами (перегородками) с пределом огнестойкости не менее 0,75 ч. Двери в этих стенах и перегородках должны быть с пределом огнестойкости не менее 0,6 ч. Зону вычислительного центра рекомендуется оборудовать как наиболее защищаемую.

4. Огнегасящим веществом должен быть газ, который имеет российский сертификат. Таким средством тушения может быть газ "игмер" (октафторциклобутан, хладон 318Ц, ТУ 2412-001-13181581-96, код К-ОКП 241249, сертификат соответствия № РОСС RU.ББ02. Н00073 от 10.04.96, одобренный НИИ медицины труда РАМН) или двуокись углерода, заправленная в модули высокого давления типа МГП. Использование фреона 114В2 (тетрафтордибромэтан) и порошковых огнегасителей в этих помещениях категорически запрещено.

5. Станция АУГП размещается в непосредственной близости от помещения серверной или в самом зале в специально оборудованном для этого шкафу. Количество баллонов с газом зависит от объема защищаемого помещения.

6. Включение системы АУГП производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма.

7. Специальные стеллажи и шкафы в серверной должны быть из несгораемых материалов. Акустическая отделка выполняется из несгораемых (трудносгораемых) материалов.

2.5.6. Требования к пропускному режиму

Пропускной и внутриобъектовый режимы устанавливаются в соответствии с Федеральным законом от 29.12.2012 №237-ФЗ «Об образовании в Российской Федерации», Федеральным законом от № 69-ФЗ «О пожарной безопасности», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности», постановлением Правительства Российской Федерации от 07 ноября 2019 №1421 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства Российской Федерации», Правилами внутреннего распорядка и другими локальными и нормативными актами Образовательного учреждения.

1. Все работники, обучающиеся и посетители обязаны входить и выходить на территорию только через контрольно-пропускные пункты (КПП), где обеспечивается проверка пропусков и документов, осмотр всех видов транспорта и обеспечивается необходимая пропускная способность.

2. КПП, в зависимости от их назначения, должны быть оборудованы надежными средствами связи, достаточным освещением, системами электронного, механического контроля доступа, турникетами, тревожной сигнализацией, техническими средствами для осмотра физических лиц при допуске их на охраняемые объекты. Въезды на охраняемые территории

оборудуются металлическими воротами и/или шлагбаумами, оснащенными автоматическими дистанционными системами управления.

3. Сотрудники Образовательного учреждения после окончания занятий, работы, закрывают окна и форточки, проверяют противопожарную безопасность помещений, выключают освещение и электроприборы, закрывают помещения, включают охранную сигнализацию (при наличии) и сдают ключи от помещений на вахту учебных корпусов. Дежурный (вахтер) делает запись в журнале выдачи (сдачи) ключей и ставит свою подпись.

4. Окна помещений нижних и подвальных этажей зданий и учебных корпусов, выходящие на неохраняемую территорию, должны быть оборудованы распашными внутренними металлическими решетками от возможного проникновения через них в здание посторонних лиц.

5. Уборка опечатываемых и сдаваемых под охрану режимных помещений Университета производится в течение рабочего дня в присутствии одного из сотрудников, работающих в этом помещении.

6. Проведение работ по надзору, техническому обслуживанию и ремонту технических систем Образовательного учреждения специалистами надзорных и подрядных организаций производится только в рабочее время с обязательным сопровождением работником подразделения, на территории которого проводятся работы.

2.5.7. Система видеонаблюдения

Система охранного теленаблюдения (СОТ) обеспечивает:

- визуальный контроль ситуации на охраняемом объекте в режиме реального времени с целью защиты объекта от несанкционированного проникновения, оперативного выявления фактов правонарушений, хищений, вандализма и принятия мер по пресечению противоправных действий, обнаружению внештатных ситуаций (задымление, возгорание,

обнаружение предметов, похожих на взрывное устройство, и т.п.) требующих принятия определенных мер для их разрешения;

- запись, архивирование видеоинформации с целью документирования событий, происходящих на охраняемом объекте, просмотра архива видеозаписей в случае чрезвычайных происшествий или, при необходимости, анализа уже произошедшей ситуации, использования во внутренних служебных проверках, проверках и расследованиях, проводимых компетентными органами, судебном делопроизводстве.

8. Порядок организации и осуществления видеонаблюдения, права и обязанности работников, обучающихся и посетителей, определяется отдельным локальным нормативном актом образовательного учреждения.

2.6. Техническая безопасность

Для выполнения требований по антивирусной защите информационных структур используется специализированное программное обеспечение (ПО), обеспечивающее надежную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении информации ограниченного доступа;
- обеспечение условий для устойчивой бесперебойной работы объектов информатизации, сетей передачи данных.

Обеспечение антивирусной защиты включает: регулярные профилактические работы; анализ ситуации проявления вредоносных программ и причины их появления; уничтожение вредоносных программ на автоматизированных рабочих местах (серверах); принятие мер по предотвращению причин появления вредоносных программ.

Состояние антивирусной защиты АРМ сотрудников и сервера можно получить при формировании отчетов специализированным программным обеспечением на основании информации, хранящейся на Сервере администрирования, которая формируется с возникновением событий, ранее отмеченных администратором информационной безопасности. Заранее сформированные шаблоны отчетов:

- Отчет о версиях антивирусных баз.
- Отчет об ошибках в работе приложений, установленных на АРМ.
- Отчет о лицензионных ключах и соблюдении установленных лицензиями ограничений.
- Отчет об уровне антивирусной защиты и т.д.

Стоит так же уделить внимание существованию системы контроля обновлений ПО, позволяющей осуществлять готовность защиты перед самыми разнообразными вредоносными программами.

Еще одним необходимым компонентом обеспечения сохранности информационных ресурсов является механизм контроля целостности, который осуществляет слежение за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием, результаты записываются в журнал антивирусного ПО.

Межсетевое экранирование используется в первую очередь в сетях, имеющих доступ к интернету, где двусторонний контроль трафика позволяет пресечь попытки несанкционированного доступа к компьютеру из локальной сети и Интернета.

Своевременное обнаружение и реагирование на аномалии в сетевой активности является важным аспектом обеспечения безопасности в организации.

Системы мониторинга и анализа сетевой активности позволяют организации следить за сетевым трафиком, обнаруживать аномалии и предупреждать о возможных угрозах безопасности. Эти системы могут анализировать общие паттерны поведения пользователей, обнаруживать необычные активности, несанкционированный доступ, атаки или попытки вторжения.

Как только система обнаруживает аномалию или потенциальную угрозу, она может сгенерировать предупреждение или даже автоматически принять меры по предотвращению инцидента, например, блокировать доступ или отправить уведомление ответственным лицам для расследования. Благодаря этому организация может оперативно реагировать на возможные атаки и минимизировать риски безопасности.

Эффективная система мониторинга и анализа сетевой активности также позволяет анализировать прошлые инциденты и предсказывать будущие угрозы, что помогает в принятии мер для предотвращения возможных инцидентов.

2.7. Обучение и осведомленность персонала

Необходимость организации устойчивой системы контроля деятельности сотрудников в рамках соблюдения нормативно-правовых отношений, является экономически выгодной процедурой, позволяющей в дальнейшем избежать реализации кадровых рисков, снизить возможные убытки.

Следовательно, организация должна быть заинтересована в проведении различных лекций, семинаров, конференций, форумов, на тему защиты информации в учебном заведении, информационных потоков; основы технической безопасности; технические средства информационной безопасности; обеспечение защиты коммерческой тайны, информации ограниченного доступа. А также в ведении журнала учета ознакомления с внутренними нормативными документами и, впоследствии, проведении проверки знаний по данному направлению.

Стоит отметить, что ответственность сотрудников является различной, в зависимости от занимаемой должности и доступа к информации ограниченного доступа, а так же закреплена в нормативно-правовых соглашениях: «Положение об информации составляющей информацию ограниченного доступа», «Должностная инструкция».

Руководству предприятия стоит уделять пристальное внимание правовой защите информации, так как риски связанные с этим направлением защиты, являются оптимально устранимыми в случае проведения соответствующих мероприятий по ознакомлению сотрудников с причинами и последствиями их действий направленных на нарушение конфиденциальности информации.

В образовательных учреждениях существует много программ обучения персонала по вопросам безопасности информации. Вот несколько популярных программ, которые широко используются:

- "Информационная безопасность для персонала образовательного учреждения" - данная программа предоставляет обучение основам безопасности информации, включая безопасное обращение с паролями, осведомленность о социальной инженерии, защиту от вредоносного программного обеспечения и т. д.
- "Защита персональных данных" - этот курс обучает персоналу образовательного учреждения правильной обработке и хранении персональных данных учеников и сотрудников согласно законодательству о защите данных.
- "Безопасность сети и интернета" - этот курс научит сотрудников основам безопасной работы в сети, включая защиту от мошенничества, фишинговых атак, вредоносного контента и других угроз в интернете.
- "Безопасность электронной почты и коммуникаций" - данный курс учит персонал образовательного учреждения ключевым аспектам безопасной коммуникации через электронную почту, мгновенные сообщения и другие каналы связи.
- "Обеспечение безопасности данных при удаленной работе" - этот курс обучает персонал основам безопасной работы в удаленном режиме, включая защиту от утечки данных, безопасность сетевого подключения и использование безопасных инструментов.
- "Политики и процедуры безопасности информации" - данный курс охватывает разработку и реализацию политик и процедур безопасности информации в образовательном учреждении, включая управление доступом, резервное копирование и восстановление данных и другие важные аспекты безопасности.

2.8. Защита от внешних угроз

1. Необходимость проведения процедуры защиты от загрузки с внешних электронных носителей (flash-накопители, CD/DVD/Blu-ray диски, внешние HDD и SSD накопители) является весьма обоснованной, в связи с существующей угрозой несанкционированного доступа в систему и игнорирования незащищенного соединения, обладающего скрытым вредоносным потенциалом. В целях устранения данного вида угроз применяются программные или программно-аппаратные средства защиты информации, с помощью которых удается настроить не только доступ разрешенных съемных носителей и блокирования не зарегистрированных носителей.

Аппаратная часть нейтрализует угрозу загрузки ОС с внешних съемных носителей, не позволяя обойти систему защиты средствами BIOS. В случае возникновения подобной ситуации плата будет блокировать работу всей системы.

Схожий механизм нейтрализации угроз несет система контроля подключения внешних устройств. Она позволяет сохранить в неизменном виде аппаратную конфигурацию компьютера во время работы, осуществить контроль над подключаемыми/отключаемыми внешними устройствами, занести событие о попытке подключения незарегистрированного устройства, а так же произвести различные сценарии реакции на данные подключения к АРМ.

Для хранения зарегистрированный (учтенных носителей) используется журнал (картотека) с регистрацией их выдачи/прием, при этом на всех носителях должна быть нанесена маркировка.

2. Ошибки в программном обеспечении. Программное обеспечение сетевого оборудования, написанное людьми, содержит зачастую ошибки, которые не представляют опасности, однако некоторые могут привести к

реализации угроз злоумышленников, например, получения контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов.

Зачастую решением данной проблемы являются выпускаемые обновления производителя.

Поэтому необходимо и в образовательных учреждениях использовать различные инструменты и методы для обновления программного обеспечения. Некоторые из них включают:

- Автоматические обновления: Образовательные учреждения могут использовать функциональность автоматического обновления, предоставляемую самими производителями программного обеспечения. Это позволяет приложениям и операционным системам автоматически загружать и устанавливать последние версии обновлений.
- Централизованное управление обновлениями: Учреждения могут использовать централизованные инструменты управления обновлениями, такие как системы управления конфигурацией, которые позволяют массово устанавливать и контролировать обновления на нескольких компьютерах и серверах.
- Облачные службы обновлений: Учреждения могут воспользоваться услугами облачных провайдеров, где обновления ПО могут быть установлены и обслуживаемыми удаленно. Это особенно полезно, когда учреждение имеет большое количество компьютеров или устройств.
- Пакетные менеджеры: На определенных операционных системах, таких как Linux, существуют пакетные менеджеры, которые упрощают процесс установки и обновления программного обеспечения.
- Ручное обновление: В случаях, когда требуется более тщательное тестирование и контроль, обновления могут устанавливать сотрудники IT-отдела или администраторы системы вручную.

- Обновления от производителей оборудования: В случае использования специализированного оборудования или устройств, таких как интерактивные доски или специфическое программное обеспечение, обновления могут быть предоставлены напрямую производителями оборудования.
- Регулярное обновление антивирусных программ и систем защиты помогает обеспечить безопасность системы, обнаруживая и предотвращая угрозы безопасности.

3. Различные DoS- и DDoS-атаки. DoS-атаки - это особый тип атак, направленных на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в ПО или легитимные операции. Другой тип атак DDoS приводит к выведению из строя большого числа АРМ. Принцип действия таких атак заключается в перегрузке канал трафиком, что приводит к блокированию передачи информации по каналам связи.

4. Компьютерные вирусы, черви, трояны, backdoor. В современных реалиях компьютерные вирусы чаще всего интегрируются с троянами и сетевыми червями и распространяются либо через электронную почту, либо посредством уязвимости в ПО. Подобные вредоносные программы выполняют функции удаленного управления, похищения информации, дальнейшего распространения, участника DDoS-атаки. Одним из методов борьбы можно назвать оперативную установку обновлений.

5. Анализаторы протоколов и прослушивающие программы («снифферы»). Уязвимость, связанная с этой группой, возникает при передаче по сети данных в открытом виде, при этом средства перехвата данных могу быть как аппаратными, так и программными. Использование протоколов осуществляющих шифрование паролей, значительно помогает справиться с уязвимостью перехвата этих паролей.

Мерой защиты будет являться:

- ограничение доступа к сети неавторизированных пользователей.
- проведение проверки на наличие оборудования, такое как межсетевые экраны, интранет-сети и системы обнаружения атак, которые могут обнаружить и предотвратить DDoS-атаки.
- использование системы DNS и CDN для распределения нагрузки и защиты от DDoS-атак. Эти службы способны определить и блокировать потенциально вредоносный трафик и обеспечивать непрерывную работу веб-сайта
- постоянное создание резервных копий важных данных и систем. Наличие процедур резервного копирования и способность восстановления после атаки.
- обновление программного обеспечения. Оборудование в образовательном учреждении должны иметь последние обновления и патчи безопасности. Это важно для предотвращения эксплойтов и уязвимостей.
- проведение симуляции DDoS-атаки на инфраструктуру, с помощью специализированных инструментов или услуг. Это поможет определить слабые места и повысить готовность к возможным атакам.

Важно понимать, что обеспечение защиты от DDoS-атак - это непрерывный процесс, и рекомендуется регулярно обновлять и повышать уровень защиты в соответствии с новыми угрозами.

Основными мерами защиты общедоступных корпоративных ресурсов локальной сети будут являться криптографические методы: шифрование информации; электронная подпись (ЭП). Механизм поиска данных вирусов сводится к поиску сигнатур, расчету контрольных сумм и эвристическому анализу (анализ действий программ).

Защитой от внешних угроз можно назвать технологию виртуальных частных сетей (VPN), позволяющую с помощью криптографических

методов, как защитить информацию, передаваемую через интернет, так и пресечь НСД в локальную сеть из вне.

Выводы по второй главе

Во второй главе магистерской диссертации были сформулированы и классифицированы угрозы, возникающие в информационных системах, а также предложены меры защиты на пяти уровнях.

Проанализированы основные этапы проведения аудита информационной безопасности :

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- использование методов анализа рисков (необязательно);
- оценка соответствия требованиям стандартов (необязательно
- выработку рекомендаций;
- подготовку аудиторского отчета.

Изложены основные требования к аккредитации организаций, предоставляющих услуги аудита информационной безопасности, существующие в настоящее время.

Рассмотрены международные стандарты и их современные аналоги РФ в области информационной безопасности, на основании которых производится оценка рисков информационной безопасности на предприятиях.

Определены и изучены аспекты обеспечения безопасности, по которым будет производиться внутренний аудит: физическая безопасность; техническая безопасность; защита персональных данных; обучение и осведомленность персонала; реагирование на инциденты; защита от внешних угроз; управление информационной безопасностью.

Глава 3. Разработка регламента проведения аудита информационной безопасности организаций

3.1. Концепция проведения аудита информационной безопасности ГБПОУ «Южно-Уральский государственный колледж»

Развитие страны в рамках национальной программы «Цифровая экономика Российской Федерации» обусловливает активное внедрение информационных технологий в вузах, повышающих эффективность образовательных, научно-исследовательских процессов и управленческой деятельности.

Появление в Образовательных учреждениях новых информационных ресурсов и сервисов (многофункциональные интернет-порталы, компьютерные классы, широкополосный интернет и локальные сети, интерактивные обучающие курсы и т. д.) увеличивает риск возникновения инцидентов информационной безопасности (ИБ), реальные последствия которых могут снижать эффективность работы учебного заведения.

Сегодня руководство серьезно заботиться об ИБ Образовательного учреждения. (сохранение информации о работе, учащихся, преподавателях, обеспечение целостности и сохранности электронных документов и т. д.), поскольку отмеченная национальная программа акцентирует на этом внимание.

Одним из важнейших факторов эффективного функционирования современного Образовательного учреждения является комплексная система ИБ, ключевым элементом которой является аудит.

В процессе проектирования комплекса мер аудита ИС Образовательного учреждения важно понимать состояние защищенности ценных ресурсов, чтобы противостоять внешним и внутренним угрозам ее безопасности. Поиск путей решения проблем должен осуществляться не только силами самого вуза, но и при помощи внешних консультантов, в

частности аудиторов. Поэтому реальную помощь может оказать независимое аудиторское исследование. В то же время при проведении такого аудита специалисты сталкиваются с проблемой сопоставления возможных расходов на обеспечение безопасности и выгод, получаемых при внедрении системы ИБ, поэтому в условиях ограниченного финансирования учебного заведения не менее перспективным выглядит внутренний тип аудита образовательного учреждения, позволяющий использовать квалифицированный кадровый контингент Образовательного учреждения при меньших затратах.

Для проведения аудита ИБ необходимо использовать комплексную концепцию, со следующими составляющими:

- Идентификация объектов проверки;
- Цели и задачи проверки;
- Предпочтительный подвид проверки;
- Рекомендуемые подходы к проведению проверки и методы анализа данных;
- Этапность проведения проверки;
- Организационно-технические основы аудиторской проверки;
- Состав результатов аудита.

Для целостного восприятия структура предлагаемой концепции представлена графически (рисунок 3.1)

Рисунок 3.1 – Структура концепции проведения аудита ИБ вуза.

1. Идентификация объектов аудиторской проверки ИБ. Принципиальной особенностью образовательных учреждений с точки зрения ИБ является необходимость обеспечения безопасности разнообразных данных в разворачиваемых компьютерных сетях, поэтому принципиальным объектом представляется информационная система образовательного заведения, базирующаяся на сетях такого рода.

2. Цели и задачи информационного аудита. Основные цели аудита ИБ образовательного учреждения можно сформулировать следующим образом:

• выявление и детальное изучение угроз ИБ и «слабых звеньев» активов объектов аудита;

• определение набора мероприятий для повышения уровня безопасности системы защиты активов объектов аудита;

• создание таких условий функционирования объектов аудита, при которых реализация инцидентов ИБ была бы невозможна.

Основной задачей информационного аудита вуза является контроль и оценка объектов аудита на соответствие требованиям к уровню их информационной безопасности.

3. Предпочтительный тип аудита для вуза. При обсуждении проблемы выбора наиболее адекватного подвида аудита ИБ будем руководствоваться терминологией и классификацией.

Аудит безопасности деятельности вуза в сфере информационных технологий целесообразно проводить экспертным путем. При его проведении выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в аудите.

Подобного типа аудит позволяет принять обоснованные решения по использованию средств защиты, оптимальных по их стоимости и возможности предотвращения угроз информационной безопасности в вузах.

Рекомендуется обратить внимание на комплексный тип аудита, который может включать в себя, наряду с экспертным аудитом, элементы таких видов, как оценка соответствия и тестирование.

Анализируя применимость аудита пассивного и активного типов, отметим, что оба подвида могут быть использованы на практике в зависимости от целей и задач конкретной проверки. Обсуждая легальность мероприятий аудита, выбор однозначно делается в пользу легального подвида на основании принципа законности в сфере ИБ. Кроме этого, аудит ИБ вуза может сочетать в себе организационно-нормативные и технические формы, что повышает его результативность.

4. Рекомендуемые подходы к проведению аудита и методы анализа данных. Наиболее адекватным практическим подходом для его реализации в учебных заведениях представляется комбинация анализа рисков и стандартов ИБ. Нормативные документы задают планку минимальному комплекту предписаний безопасности, предъявляемых к изучаемым

объектам. Специфические нюансы конкретного вуза учитываются детальной оценкой рисков для его активов. Такой подход устраняет «минусы» аудита чисто на основе анализа рисков или только на соответствие стандартам.

Поскольку аудит информационной безопасности в вузах только «набирает обороты», подобный подход вполне адекватен. Для вуза целесообразен подход на основе «серого ящика», если выбирать его тип, определяемый доступностью информации о системе для специалиста аудита. Этот вид наилучшим образом учитывает специфику организации, возможное наличие конфиденциальной информации и предпочтительный внутренний подвид аудита.

5. Этапность проведения аудита. Поэтапное проведение аудита создает возможности для более полного и объективного изучения текущего состояния и планов развития информационных технологий в конкретном Образовательном учреждении, разработки рекомендаций по усилению безопасности в сфере применения информационных технологий, а также оформления и представления результатов аудита. Именно такой подход может быть полезным для практики проведения аудиторской проверки в сфере образования.

Большинство авторов научных публикаций склонны к тому, что процесс аудита должен осуществляться в три этапа.

Тогда процесс аудита будет выглядеть следующим образом (рисунок 3.2).

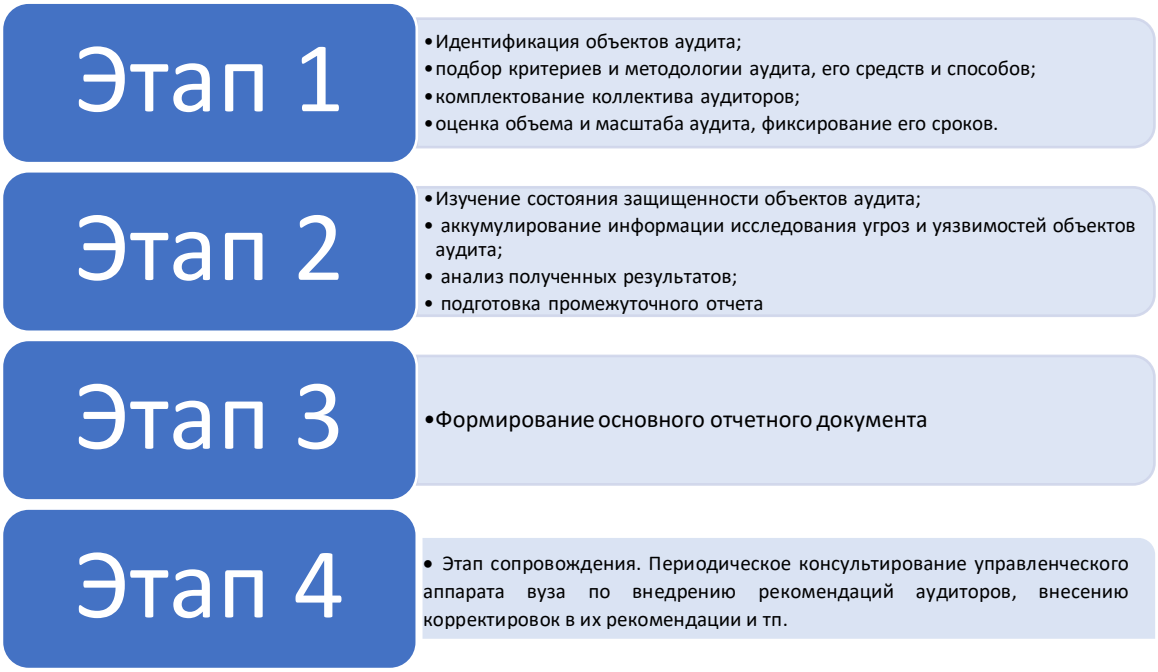

Рисунок 3.2 – Основные этапы проведения аудита ИБ

6. Организационно-технические основы аудита ИБ. Аудиторская проверка ИБ Образовательного учреждения должна основываться на базовом документе (пакете документов) организации, регламентирующем такого рода деятельность.

Порядок организованного проведения аудита отражается в плане-графике проверки, которым руководствуются в ходе непосредственной реализации процесса.

Исследования объектов аудита, если они предусмотрены планом проверки, проводятся на основании программы.

Аудит информационной безопасности Образовательного учреждения следует понимать не только как инвентаризацию используемых аппаратно-программных средств для обнаружения «пиратских» версий, но и как возможность оценки работы пользователей вуза и сотрудников служб безопасности, их трудовой дисциплины и способности внедрять и эксплуатировать новые информационные технологии.

7. Состав результатов аудита вуза. Содержание этой составляющей формируется решениями поставленных задач аудита. Результаты оформляются в виде Отчета аудит ИБ.

Проведение аудиторской проверки на базе рассмотренной концепции позволит усовершенствовать комплексную систему ИБ Образовательного учреждения и снизить уровень рисков, обусловленных возможной реализацией угроз ИБ. Уменьшение вероятности подобного рода инцидентов приведет к увеличению результативности использования современных информационных технологий в учреждении образования, что, в свою очередь, повысит эффективность функционирования вуза в целом.

3.2. Разработка регламента аудита информационной безопасности ГБПОУ «Южно-Уральский государственный колледж»

Проект Регламента проведения внутреннего аудита ИБ является важным инструментом для осуществления работы внутренней службы безопасности, ИТ отдела или отдела информационной безопасности. Данный документ будет использоваться руководителем в качестве инструкции проведения внутреннего аудита ключевых систем информационных инфраструктур Образовательного учреждения ГБПОУ «Южно-Уральский государственный колледж», в составлении Плана-графика проведения аудита ИБ, Программы проведения аудита ИБ, других сопутствующих документов.

Создание системы информационной безопасности в Образовательном учреждении требует принятия Регламента, которым будут определяться действия и обязанности аудиторов при проведении проверки аудита ИБ. А также разработкой Политики ИБ, благодаря которой будет осуществляться контроль за пользователем, проверяя его работу как во время стандартных процессов, так и в чрезвычайных ситуациях. Такие регламенты, политики, положения и другие акты решают несколько задач – упорядочивают работу с информацией, ложатся в основу политик безопасности систем, а в случае их нарушения конкретным сотрудником факт ознакомления с ними станет безусловным основанием для привлечения к ответственности.

Нормативные акты в России не настаивают на обязательном принятии регламента информационной безопасности, это решение является инициативой организации, желающей повысить степень сохранности данных в информационной системе.

Анализ нормативно-правовой базы в области защиты информационной системы показал, что в Российском Законодательстве нет документов, описывающих методику аудита ИБ. Более того отсутствуют документы,

регламентирующие процесс проведения аудита ИБ в самих образовательных учреждениях.

В этой связи разработка Регламента проведения аудита ИБ в общеобразовательном учреждении представляется одним из важнейших вопросов в сфере защиты и конфиденциальности информации. На основании этого было принято решение о разработке Регламента проведения внутреннего аудита ИБ, который при регулярном применении позволит решить проблемы, такие как: угрозы, связанные с действиями сотрудников (кадровые риски), угрозы несанкционированного проникновения, угрозы выхода из строя, сбоев аппаратного или программного ПО.

При разработке Регламента проведения аудита ИБ, Политики внутреннего аудита ИБ, а также других дополняющих документов, будем руководствоваться следующими нормативными правовыми актами:

- Конституцией РФ;
- Трудовым кодексом РФ;
- Гражданским кодексом РФ;
- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральным законом от 27.07.2006 №152-ФЗ: «О защите персональных данных»;
- Федеральным законом от 06.04.2011 №63-ФЗ: «Об электронной подписи»;
- Федеральным законом от 29.12.2012 №273-ФЗ "Об образовании в Российской Федерации";
- Федеральным законом от 30.12.2008 307-ФЗ: «Об аудиторской деятельности»;

- Федеральным законом от 29.07.2004 года №98-ФЗ «О коммерческой тайне»;
- Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";
- Письмом Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»;
- Указом Президента РФ от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных информационного обмена»;
- Указом Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности РФ»;
- Международными стандартами ISO/IEC 27000:2013 «Информационные технологии — Технологии безопасности — Системы менеджмента информационной безопасности — Требования» и ISO/IEC 27002:2013 «Информационные технологии - Технологии

безопасности - Практические правила менеджмента информационной безопасности»» [21];

- Национальным стандартом РФ ГОСТ Р ИСО 9001-2008 и ГОСТ Р ИСО/МЭК 17799-2005, ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [21];
- Гостехкомиссией «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» 2 марта 2001 г №7.2;
- Другими внутренними нормативными документами Образовательного учреждения.

Целью настоящего проекта по составлению Регламента аудита ИБ является получение достоверных данных, подкрепленных фактами и документами, которые позволили бы максимально объективно определить состояние защиты информации в Образовательном учреждении, оценить степень соответствия общим требованиям по обеспечению информационной безопасности.

Регламент проведения аудита ИБ является локально-нормативным актом (далее ЛНА). Структура регламента определяется общепринятыми нормами и стандартами информационной документации. В Российской Федерации существуют различные нормативные документы, которые регулируют структуру и содержание регламентов или подробно определяют порядок их разработки. Вот некоторые из них:

- ГОСТ Р ИСО 9001-2015 "Системы менеджмента качества. Требования".
- ГОСТ Р 7.0.97-2016 "Системы менеджмента организации. Общие требования".

- ГОСТ Р ИСО/МЭК 82079-1-2019 "Инструкции по применению. Часть 1: Структура, содержание и проектирование документации по пользованию"
- ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»
- Примерная инструкция по делопроизводству в государственных организациях (утв. приказом Росархива от 11.04.2018 № 44);
- Методические рекомендации по разработке инструкций по делопроизводству ИД-2020

При разработке Регламента проведения аудита ИБ был использован, рекомендуемый план проведения аудита ИБ, который включает в себя следующие этапы:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- использование методов анализа рисков (необязательно);
- оценка соответствия требованиям стандартов (необязательно);
- выработку рекомендаций;
- подготовку аудиторского отчета.

Разрабатывая Регламент проведения аудита информационной безопасности Образовательного учреждения ГБПОУ «Южно-Уральский государственный колледж», были учтены особенности учебных процессов, жизнедеятельности учебного заведения, его информационной инфраструктуры.

3.2.1. Основные, обязательные разделы

Титульный лист

При составлении Регламента проведения аудита ИБ за основу взята форма титульного листа, которая приведена в ГОСТ Р 7.0.97-2016.

В начале указано полное наименование Образовательного учреждения, ниже ее общепринятое сокращенное название, название ЛНА, наименование вида документа об утверждении, его дата и номер, место составления.

Содержание

Первым разделом Регламента проведения аудита ИБ, после титульного листа, идет содержание. Оно является обязательным разделом регламента и, кроме того, представляет собой хороший индикатор структурированности регламентируемого процесса.

Термины, определения и сокращения

Данный раздел Регламента проведения аудита ИБ представлен в виде табличного документа, содержит определения терминов и разъяснение сокращений, используемых в тексте регламента.

Этот раздел является одним из наиболее важных, поскольку характеризует предметную область, в которой разворачивается регламентируемый процесс.

Указанные термины в Регламенте проведения аудита ИБ это:

- термины вводимые и используемые в регламенте впервые;

- термины, используемые исключительно в рамках данного регламента, в том числе, термины, используемые для сокращения текста;

- термины общеупотребительные, но редко используемые и применяемые в регламенте.

Данные термины приведены в алфавитном порядке, чтобы было удобно и быстро находить нужное определение, когда приходится обращаться по мере чтения документа.

Общие положения

В этом разделе Регламента проведения аудита ИБ описаны назначение, цели и область применения регламента, ссылки на законы, нормативные акты и внутренние документы Образовательного учреждения, такие как Политика внутреннего аудита ИБ, на основе которых разработан данный регламент, описание ожидаемых результатов и пользы от применения, указание на все этапы, необходимые для выполнения каждого процесса, другая информация, мотивирующая сам регламент и кратко комментирующая регламентируемый процесс.

3.2.2. Инициирование процедуры

Планирование внутреннего аудита ИБ

Этап планирования внутреннего аудита ИБ предусматривает виды аудита ИБ и их периодичность.

Описана процедура проведения планового аудита ИБ, указано при каких обстоятельствах может проводиться внеплановый и выборочный аудит ИБ.

Данный этап характеризуется выпуском организационно-распорядительной документацией, в том числе составления и утверждения Плана-графика аудита ИБ на очередной период.

Этап планирования аудита ИБ является фундаментом для последующих этапов аудиторской проверки, таких как проведение аудита, сбор и анализ данных, оценка результата, подготовка рекомендаций и отчетности. Он позволяет обеспечить систематичность, эффективность и своевременность проведения аудита ИБ.

Принципы проведения аудита ИБ

В данном разделе отражены принципы, которыми необходимо руководствоваться, для обеспечения надлежащего выполнения проведения аудита.

Эти принципы обеспечивают надлежащую целостность, этичность и надежность проведения аудита. Они являются основой для достижения целей аудита и обеспечивают доверие между аудиторами, клиентами и заинтересованными сторонами.

Принципы аудита помогают установить высокие стандарты профессиональной практики и обеспечить надлежащее выполнение аудиторской работы в соответствии с этими стандартами. Они гарантируют качество проведения аудиторской проверки. Они обеспечивают согласованность и сопоставимость результатов аудита и помогают создать единый подход в индустрии. Они помогают установить надежные факты и предоставить объективное мнение о результатах аудита.

Требования к аудиторской группе

В данном разделе раскрыты общие требования к аудиторской группе. Для обеспечения полного покрытия задач аудита и ресурсов предпочтительнее создать группу аудиторов, которая будет включать в себя специалистов с разными областями знаний, чтобы покрывать все аспекты аудита.

Отражен пункт, касающийся наличия соответствующего образования и актуальных знаний у участников аудита. Важно, чтобы они были квалифицированными профессионалами с соответствующими сертификатами и лицензиями, и обладали глубокими знаниями в области информационной безопасности, так как это является важным аспектом аудита. Они должны быть в курсе последних трендов и технологий в ИБ, а также иметь опыт работы в этой области.

Участники аудиторской группы должны иметь эффективную коммуникацию и взаимодействие между собой. Каждый член группы должен знать свои обязанности и ответственности, а также уметь эффективно сотрудничать с другими участниками процесса аудита.

В данном разделе указано, что аудиторская группа должна иметь полный и безопасный доступ к необходимой информации для проведения аудита. специалисты других структурных подразделений должны предоставлять им необходимые ресурсы, инструменты и права доступа для успешного выполнения задач.

Учитывая данные требования, можно создать аудиторскую группу, которая будет эффективно выполнять свои обязанности, обеспечивать безопасность и защиту информации организации

Порядок проведения внутреннего аудита ИБ

Включает в себя необходимость составления, на основе Плана-графика внутреннего аудита ИБ - Приказа о проведении проверки и Программу аудита ИБ, утвержденных руководством Образовательного учреждения, с учетом обязательных пунктов. Проведение вводного совещания для разъяснения возникающих вопросов по подготовке и проведению аудита ИБ.

Описан процесс согласования условий и времени проведения аудита ИБ с руководителями проверяемых подразделений.

Инициирование процедуры

На данном этапе прописано, что должен быть разработана Программа аудита ИБ, определены цели, объем и задачи аудита ИБ, основываясь на требованиях Образовательного учреждения и соответствующих стандартах. Указаны методики и техники, которые будут использоваться во время аудита. Определены расписание и время, необходимые для проведения аудита ИБ. Должны иметься необходимые ресурсы, как внутренние, так и внешние, а также беспрепятственный доступ к средствам и инструментам для проведения аудита ИБ.

Должны быть определены, какие информационные системы, процессы и структуры будут включены в аудит ИБ. Уточнены, какие уровни, компоненты и активы будут подвергнуты аудиту.

Изучен предварительный План-график аудита ИБ, чтобы определить основные проблемы и риски, которые необходимо рассмотреть в процессе аудита. Это может быть связано с уязвимостями системы, несоблюдением политик и процедур ИБ, недостаточной защитой данных и т. д.

3.2.3. Сбор информации аудита ИБ

На этапе сбора информации аудита ИБ в образовательном учреждении отражено какие необходимо проводить действия:

Проведение Интервьюирования с сотрудниками учреждения, ответственными за информационную безопасность, IT-отдел и другими заинтересованными сторонами. Вопросы могут касаться политик и процедур ИБ, используемых технологий, систем хранения и защиты данных, требований к доступу и т.д.

Определение используемых информационных технологий, таких как компьютерные системы, сети, серверы, программное обеспечение и т. д. Вопросы могут относиться к конфигурации, безопасности, обновлениям и поддержке данных систем.

Определение и документирование всех информационных активов в учреждении, включая оборудование, программное обеспечение, сетевую инфраструктуру, доступы к системам и другие активы, которые могут быть целью аудита ИБ.

Изучение рабочих процессов и процедур, связанных с обработкой, хранением и передачей информации. Изучение политик ИБ, процедур шифрования, управления доступом и других контрольных механизмов.

Исследование систем безопасности и контролей, используемых для защиты информационных активов. Это может включать проверку наличия антивирусного программного обеспечения, настройку брандмауэров, использование шифрования данных и других мер безопасности.

Весь собранный материал и данные будут служить основой для последующего анализа и оценки уровня безопасности информационной системы образовательного учреждения.

3.2.4. Анализ данных аудита ИБ

Этот этап необходим для сравнения найденной информации и практик с требованиями безопасности, определенными в политиках и стандартах ИБ. Он отражает оценку уровня соответствия и выявление потенциальных уязвимостей или недостатков. Помогает выявить действующие уязвимости в системе информационной безопасности, такие как несоблюдение политик, недостаточную защиту данных, слабые пароли, неправильную настройку сети и другие угрозы. Это позволяет принять меры для устранения этих проблем и снижения рисков.

Анализ данных аудита ИБ предоставляет подробную информацию для принятия решений об улучшении безопасности информационной системы образовательного учреждения. Это может включать внедрение новых технологий, изменение политик и процедур, обучение сотрудников или внесение корректировок в организацию безопасности.

В целом, анализ данных аудита ИБ помогает определить сильные и слабые стороны системы безопасности, выявить риски и проблемы, предложить рекомендации для улучшения и обеспечить достаточный уровень защиты информации в образовательном учреждении.

3.2.5. Подготовка аудиторского отчета

Подготовка заключений по аудиту ИБ

Предоставляет информацию о состоянии безопасности образовательного учреждения заинтересованным сторонам, таким как руководство, управляющие органы, партнеры и клиенты. Это помогает обеспечить прозрачность и доверие к уровню безопасности информационной системы.

На данном этапе при необходимости предусмотрено подписание Соглашения о неразглашении конфиденциальной информации.

Подготовка аудиторского отчета

По завершении проверки подготавливается Отчет по аудиту ИБ, в соответствии с Программой аудита ИБ, при проведении внепланового и выборочного аудита ИБ отчет оформляют в виде Аналитической записки.

Данные заключения содержат выявленные недостатки, рекомендации по их устранению и предложения по улучшению безопасности информационной системы образовательного учреждения. При выявлении несоответствий оформляется Протокол несоответствий.

В целом, подготовка заключений по аудиту ИБ образовательного учреждения является важной частью процесса аудита и позволяет обеспечить прозрачность и достаточный уровень защиты информации в образовательном учреждении.

Проведение заключительного совещания

Включает в себя следующие элементы:

Аудиторами представляются понятные и ясные выводы аудита ИБ для оценки уровня безопасности информационной системы образовательного учреждения и выявленных проблем.

Сотрудники, ответственные за проверяемые процессы, должны присутствовать на совещании, с возможностью выразить свое мнение, ответить на вопросы и принять непосредственное участие в обсуждении результатов аудита ИБ источников данных и процессов.

Совещание должно включать обсуждение достоверности данных, используемых при выполнении аудита ИБ. Важно обратить внимание на источники данных, методы их сбора, обработки и проверки. Если возникают сомнения в достоверности данных, должны быть предприняты дополнительные меры для их проверки или получения подтверждения.

В ходе заключительного совещания могут возникнуть разногласия или различные точки зрения в отношении результатов аудита ИБ. Важно обеспечить конструктивное обсуждение и найти компромиссные решения. Цель состоит в том, чтобы достичь согласия по дальнейшим шагам, улучшению безопасности и предотвращению возможных рисков. В случае, если разногласия не удается разрешить, то составляется Мотивированное возражение.

В конце совещания должны быть обсуждены и утверждены заключительный Отчет по аудиту ИБ. Важно, чтобы отчет содержал полную информацию об анализе, результатах, рекомендациях и договоренностях, достигнутых на совещании. Подписание отчета подразумевает согласие со стороны руководства Образовательного учреждения, ответственного за информационную безопасность, и членов аудиторской группы, проводившей аудит.

3.2.6. Выработка рекомендаций. Порядок мониторинга исполнения Плана мероприятий

На заключительном этапе проведения аудита ИБ образовательного учреждения, формируются конкретные и практичные рекомендации, ориентированные на достижение целей безопасности. На их основе составляется План мероприятий по устранению выявленных недостатков безопасности, где определяются конкретные шаги, ответственные лица и

сроки выполнения каждого мероприятия. План должен быть адаптирован под особенности организации и ее ресурсные возможности.

Руководители объекта принимают на себя ответственность и организуют работу подразделения по устранению выявленных несоответствий, согласно Плану мероприятий, а также по принятию мер, направленных на предотвращение их возникновения в будущем.

После завершения работ по устранению недостатков безопасности, рекомендуется составить График повторного аудита, который позволит оценить эффективность проведенных мероприятий и проверить соответствие безопасности установленным требованиям. Графики повторных проверок составляются аудиторами, по согласованию с руководителями проверяемых подразделений, на основе приоритетов и уровня рисков.

3.2.7. Заключительные положения

В данном разделе описываются условия вступления в силу данного Регламента проведения аудита ИБ, а также порядок внесения изменений.

3.2.8. Приложения

В этом разделе регламента приводится служебная и вспомогательная информация о регламентируемом процессе в количестве 11 (Одиннадцати) приложений.

3.3. Экспертная оценка внедрения регламента проведения внутреннего аудита ИБ образовательной организации

Выявление возможных рисков при внедрении Регламента производится на основе анализа изменений текущей обстановки в стране, а также рисков, которые могут негативно повлиять на деятельность ГБПОУ «ЮУрГТК», что в конечном итоге, приведет к остановке процесса внедрения Регламента. Таким образом, необходимо, используя следующий алгоритм оценки, рассчитать уровень угрозы при реализации выделенных рисков.

Выделены следующие шесть основных рисков и путей их реализации:

1. УПиЭХФ - ухудшение политических и экономических характеристик и факторов:
   - реформы в экономике и политике,
   - изменение законодательства.
2. ВФМО - влияние форс-мажорных обстоятельств:
   - стихийные бедствия и природные катаклизмы).
3. РП - риски персонала:
   - влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей),
   - влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей),
4. ИНБ - изменение или недостаток бюджета:
   - задержки финансирования,
   - отсутствие денежного резерва для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)
5. ИХОО - изменение характеристик образовательной организации:
   - возникновение негативного отношения сотрудников,
   - здравоохранение и медицина, условия отдыха.
6. НОР - недостаточная организованность работ:

- срыв графиков работ, невыполнение сроков,
- нехватка рабочей силы,
- недооценка стоимости работ и использование финансов для других целей.

Процесс проведения оценки разбивается на ряд этапов.

1-й этап. Сбор данных. Каждый из экспертов оценивает риски при внедрении Регламента, с использованием шкалы из следующих пяти лингвистических оценок: несомненно (НС) высокая вероятность; весьма вероятно (ВВ); вероятно (ВР); маловероятно (МВ); невероятно (НВ). Было выбрано пять экспертов. От экспертов были получены экспертные оценки, приведенные в таблице 3.1 (оценки, проставленные i-м экспертом, записаны в соответствующем столбце).

Таблица 3.1 – Оценки экспертов

Объект оценки	Эксперт				
	1-й	2-й	3-й	4-й	5-й
УПиЭХВ	МВ	НВ	МВ	МВ	МВ
ВФМО	ВВ	ВВ	ВР	ВВ	ВВ
РП	ВВ	НС	НВ	НВ	ВВ
ИНБ	НС	ВР	НС	НС	НС
ИХОО	ВР	ВВ	ВВ	ВВ	НС
НОР	МВ	НВ	ВВ	МВ	ВВ

2-й этап. Числовая интерпретация лингвистических оценок. Для этого воспользуемся шкалой Харрингтона, на которой каждой оценке сопоставляется некоторый интервал: НС – интервал (0,7; 1); ВВ – интервал (0,5; 0,7); ВР – интервал (0,25; 0,5); 4); МВ – интервал (0,05; 0,25); НВ – интервал (0; 0,05). Лингвистическая оценка заменяется средним значением интервала, сопоставленного ей; т. е. оценке НС сопоставляется число 0,85, оценке ВВ – 0,6, ВР – 0,375, МВ – 0,15, НВ – 0,025. Тогда полученная на

этапе 1 таблица лингвистических оценок может быть заменена следующей числовой таблицей (таблица 3.2).

Таблица 3.2 – Числовая интерпретация оценок экспертов

Объект оценки	Эксперт				
	1-й	2-й	3-й	4-й	5-й
УПиЭХВ	0,15	0,025	0,15	0,15	0,15
ВФМО	0,6	0,6	0,375	0,6	0,6
РП	0,6	0,85	0,025	0,025	0,6
ИНБ	0,85	0,375	0,85	0,85	0,85
ИХОО	0,375	0,6	0,6	0,6	0,85
НОР	0,15	0,025	0,6	0,15	0,6

3-й этап. Обработка результатов. Дальнейшая обработка данных может производиться на основе различных алгоритмов. Рассмотрим три возможных способа обработки.

В качестве результирующих оценок для каждого компонента берутся средние значения по всем экспертам xi , i – порядковый номер оцениваемого объекта (т. е. средние значения по каждой строке). Расположив объекты в порядке убывания их оценок, получаем (в скобках указаны результирующие оценки их уязвимости: ИНБ (0,755); ИХОО (0,605); ВФМО (0,555); РП (0,42); НОР (0,305); УРиЭХВ (0,125). Таким образом, наиболее вероятный риск связан с финансированием ИНБ (результирующая оценка 0,755), наименее вероятно – это риски изменений в стране УРиЭХВ (оценка 0,125).

В качестве меры оценки степени согласованности мнений экспертов, выбираем коэффициент вариации, поскольку объем данных (5 наблюдений) мал. Для это го для каждого из объектов вычисляется среднеквадратичное отклонение. Получаем:

$\sigma_{Пр} = 0{,}056$, $\sigma_{ВФМО} = 0{,}101$, $\sigma_{РП} = 0{,}375$, $\sigma_{ИНБ} = 0{,}53$, $\sigma_{ИХОО} = 0{,}168$, $\sigma_{НОР} = 0{,}174$

Отсюда по формуле

$$\Delta_j = \frac{\delta_j}{\max\limits_k(\delta_k)} = \frac{\sum\limits_{i=1}^{K}\left|x_{ij} - \hat{x}_i\right|}{K \max\limits_{i,k}(\left|x_{ik} - \hat{x}_i\right|)}. \quad (1)$$

где x_{ij} – есть оценка i-го объекта j-м экспертом,

$\hat{x}_i$ – результирующая оценка i-го объекта, полученная после обработки результатов экспертного оценивания,

K – объектов; на основе проведения экспертной процедуры с участием N экспертов,

δ_j – абсолютная оценка.

получаем следующие значения для коэффициентов вариации, выраженные в процентах (т. е. результирующее значение умножается на 100 %)

$\rho_{УПиЭХВ} = 44{,}8$ %; $\rho_{ВФМО} = 18{,}2$ %; $\rho_{РП} = 89{,}29$ %; $\rho_{ИНБ} = 70{,}2$ %; $\rho_{ИХОО} = 27{,}77$ %; $\rho_{НОР} = 89{,}84$ %.

Для интерпретации и анализа полученных результатов воспользуемся одной из существующих шкал интерпретации значений коэффициента вариации. Если вычисленное значение коэффициента вариации ρ будет меньше 0,3, то степень согласованности мнений экспертов считается приемлемой, результаты экспертизы принимаются в качестве оценки степени уязвимости соответствующего компонента, и экспертная процедура по оценке данного компонента прекращается. При значении коэффициента ρ в интервале (0,3; 0,7) степень согласованности мнений является средней, и решение о приемлемости или неприемлемости результатов принимают организаторы экспертной процедуры. При значении ρ больше 0,7 степень согласованности мнений низкая, и результаты экспертной процедуры не могут быть приняты в качестве оценок исследуемых характеристик.

На основе полученных значений коэффициентов вариации делаем вывод: мнения экспертов по возникновению рисков персонала, изменению или недостатку бюджета и недостаточной организованности работ сильно разнятся, степень согласованности низкая, поэтому применительно к этим параметрам экспертную процедуру продолжаем. Результаты экспертной процедуры по оценке вероятности возникновения рисков политических и экономических факторов, влияния форс-мажорных обстоятельств, изменение характеристик образовательной организации принимаются.

Для продолжения экспертной процедуры всем пятерым экспертам было предложено привести свои аргументы по возникновению рисков персонала, изменению или недостатку бюджета и недостаточной организованности работ, по которым степень согласованности мнений экспертов оказалась низкой. Затем применительно к этим параметрам экспертную процедуру повторили сначала. Были получены следующие результаты (таблица 3.3).

Таблица 3 – Результаты повторного оценивания

Объект оценки	Эксперт				
	1-й	2-й	3-й	4-й	5-й
ИНБ	ВВ	НС	ВР	ВР	ВВ
РП	НС	ВВ	НС	НС	НС
НОР	МВ	МВ	ВР	МВ	ВВ

После аналогичной обработки данных получаем следующие значения коэффициентов вариации;

$\rho_{РП} = 13{,}98\ \%$, $\rho_{ИНБ} = 39{,}54\ \%$, $\rho_{НОР} = 39{,}32\ \%$.

Степень согласованности мнений экспертов является приемлемой, и результаты экспертной процедуры принимаются в качестве оценок риска вероятности.

Таким образом, на основании произведенных расчетов риски изменения или недостатка финансирования являются наиболее критичными для внедрения регламента. Так же риски недостаточной организованности работ.

Расчет вероятности реализации рисков позволит администрации образовательной организации разработать необходимые мероприятия для успешного внедрения внутреннего аудита информационной безопасности.

Выводы по третьей главе

По результатам выполненных работ разработан Регламент проведения внутреннего аудита ИБ Образовательного учреждения ГБПОУ «Южно-Уральский государственный колледж», а также Политика внутреннего аудита ИБ ГБПОУ «Южно-Уральский государственный колледж».

При составлении регламента была учтена комплексная концепция, со следующими составляющими:

- Идентификация объектов проверки;
- Цели и задачи проверки;
- Предпочтительный подвид проверки;
- Рекомендуемые подходы к проведению проверки и методы анализа данных;
- Этапность проведения проверки;
- Организационно-технические основы аудиторской проверки;
- Состав результатов аудита.

Регламент был сформирован для осуществления работы внутренней службы безопасности, ИТ отдела или отдела информационной безопасности, на основании сведений об информационной системе, бизнес-процессах, потоках информационных активов и актуальных рисках информационной системы.

Проведена экспертная оценка на выявление возможных рисков при внедрении Регламента, на основе анализа изменений текущей обстановки в стране, а также рисков, которые могут негативно повлиять на деятельность ГБПОУ «Южно-Уральский государственный колледж».

Расчет вероятности реализации рисков позволит администрации образовательной организации разработать необходимые мероприятия для успешного внедрения внутреннего аудита информационной безопасности.

Использование данного Регламента позволяет грамотно провести аудиторскую проверку информационной безопасности, тем самым снизить риск административной, уголовной, гражданско-правовой, дисциплинарной ответственности образовательного учреждения.

Таким образом, разработанный Регламент проведения внутреннего аудита ИБ ключевых систем информационных инфраструктур позволяет, с точки зрения отдела внутренней безопасности, оценить защищенность потоков информации ограниченного доступа и принять своевременные меры по нейтрализации существующих угроз.

Заключение

В заключение хотелось бы сказать о том, что все поставленные в выпускной квалификационной работе задачи были решены в полном объеме. Цель достигнута. Была подтверждена актуальность исследования, степень разработанности темы исследования, теоретическая и практическая значимость работы. В результате выполнения выпускной квалификационной работы были разработаны:

1. Регламент проведения внутреннего аудита ИБ Образовательного учреждения ГБПОУ «Южно-Уральский государственный колледж»;
2. План-график внутреннего аудита ИБ;
3. Приказ о проведении проверки;
4. Программа аудита ИБ;
5. Примеры разработанных вопросов;
6. Отчет по аудиту ИБ;
7. Аналитическая записка;
8. Протокол несоответствия ;
9. Мотивированное возражение;
10. План мероприятий;
11. Соглашение о неразглашении конфиденциальной информации;
12. Политика внутреннего аудита ИБ ГБПОУ «Южно-Уральский государственный колледж».

Хочется отметить, что используя данный Регламент проведения внутреннего аудита ИБ, с участием собственного квалифицированного персонала Образовательного учреждения, позволяет учебному заведению снизить финансовые издержки на его реализацию при возможном минимальном снижении качества проводимых работ.

Рекомендуемая оценка изменений, которые произойдут в системе ИБ с момента предыдущей проверки, позволит донести до администрации образовательной организации динамику уровня

информационной безопасности, состояние объектов аудита и системы их защиты по сравнению с предыдущей проверкой и, соответственно, необходимость внедрения последующих мероприятий.

Применение положений, предложенным Регламентом проведения аудита ИБ на практике, позволит проводить мониторинг исполнения федеральных законов и программ в образовательном заведении и согласовывать местные практики с нормативными документами вышестоящего уровня.

В процессе работы над выпускной квалификационной работой были решены следующие задачи:

- было сформулировано уточненное определение понятия «аудит ИБ», определены цели и задачи аудита ИБ, выделены виды проведения аудита ИБ, обозначены этапы проведения аудита информационной безопасности;
- была проанализирована литература и интернет-источники по аудиту и менеджменту информационной безопасности, анализу и управлению рисками на предприятиях;
- были изучены нормативные правовые акты РФ, международные стандарты в области информационной безопасности;
- был разработан Регламент аудита информационной безопасности образовательного учреждения;
- были разработаны формы сопровождающей документации для Регламента аудита информационной безопасности, а также Политику внутреннего аудита информационной безопасности образовательного учреждения.

Проведение аудита информационной безопасности является одним из наиболее эффективных инструментов по получению объективной информации о текущем уровне защищенности от всевозможных угроз, с целью их предупреждения и избежание ущерба.

Именно поэтому оценка рисков на предприятиях различного уровня должна проводится на регулярной основе специалистами или руководством организации для достижения максимальной отдачи и повышения уровня информационной безопасности организации.

Список используемых источников

1. Anti-Malware — информационная безопасность для профессионалов // Anti-Malware [Электронный ресурс] — Режим доступа — http://www.anti- malware.ru (дата обращения: 27.11.2023).

2. Accounting — О концепции проведения аудита информационной безопасности в вузе // Accounting [Электронный ресурс] — Режим доступа — https://accounting.fa.ru/jour/article/viewFile/286/279 (дата обращения: 02.12.2023).

3. Cfin – пишем регламент: рекомендации по разработке // Cfin [Электронный ресурс] — Режим доступа — https://cfin.ru/management/people/instructions/rules.shtml (дата обращения: 29.11.2023).

4. Drupal // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Drupal (дата обращения: 27.11.2023).

5. Profiz – регламент о том, как составлять регламенты // Profiz [Электронный ресурс] — Режим доступа — https:// https://www.profiz.ru/sr/6_2022/kak_sostavit_reglament/#_ftnref3 (дата обращения: 04.12.2023).

6. WordPress // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/WordPress (дата обращения: 25.11.2023).

7. Аверченков В.И. Аудит информационной безопасности [Текст]: учебное пособие для вузов / В.И. Аверченков. — 3-е изд., стереотип. — Москва: ФЛИНТА, 2016. — 269 с.

8. Анализ рисков в управлении информационной безопасностью // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/upravlenie- riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi- bezopasnostyu (дата

обращения: 22.11.2023).

9. Аудит безопасности информационных систем // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti (дата обращения: 03.11.2023).

10. Аудит информационной безопасности — основа эффективной защиты предприятия // ДиалогНаука [Электронный ресурс] — Режим доступа — https://dialognauka.ru/press-center/article/4753/ (дата обращения: 10.11.2023).

11. Аудит информационной безопасности // IBS [электронный ресурс] — Режим доступа — https://www.ibs.ru/it-infrastructure/information-security/audit- informatsionnoy-bezopasnosti/ (дата обращения: 12.11.2023).

12. Аудит информационной безопасности // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (дата обращения: 01.11.2023).

13. Аудит информационной безопасности // Контур [Электронный ресурс] — Режим доступа — https://kontur.ru/security/features/audit-ib/ (дата обращения: 05.11.2023).

14. Аудит информационной безопасности. Анализ защищенности систем и приложений // Pentestit [Электронный ресурс] — Режим доступа — https://www.pentestit.ru/audit/ (дата обращения: 21.11.2023).

15. Аудит корпоративной безопасности // Group-IB [Электронный ре- сурс] — Режим доступа — https://www.group-ib.ru/audit.html (дата обращения: 21.11.2023).

16. Виды аудита информационной безопасности // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс] — Режим доступа — http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi- bezopasnosti/vidy-audita-informacionnoi-bezopasnosti (дата

обращения: 18.11.2023).

17. ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] Режим доступа — https://docs.cntd.ru/document/1200044768 (дата обращения 25.11.2023).

18. ГОСТ 12.4.009-83. Межгосударственный стандарт. Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание // КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=9134#0 (дата обращения 25.11.2023).

19. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — https://docs.cntd.ru/document/1200006921 (дата обращения 15.11.2023).

20. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200058325 (дата обращения 25.11.2023).

21. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» // Электронный фонд правовой и норматив- но-технической документации [Электронный ресурс] — Режим доступа — http://docs.cntd.ru/document/1200103619 (дата обращения 25.11.2023).

22. Обследование (аудит) ИСПДн // Контур [Электронный ресурс]

— Режим доступа — https://kontur.ru/security/features/ispdn/ (дата обращения: 23.11.2023).

23. Общие критерии оценки защищенности информационных технологий, Общие критерии // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/Общие_критерии#Общие_критерии_в_России/ (дата обращения: 03.11.2023).

24. Практическое применение международного стандарта информационной безопасности ISO 17799 // CitForum [Электронный ресурс] — Режим доступа — http://citforum.ru/security/articles/aboutisonew.shtml (дата обращения: 25.11.2023).

25. Проведение и организация аудита безопасности информации в организации// StudFiles [Электронный ресурс] — Режим доступа — https://studfile.net/preview/9348846/ (дата обращения: 18.11.2023).

26. Программные средства проверки политики безопасности на соответствие ISO 17799 // IXBT [Электронный ресурс] — Режим доступа — https://www.ixbt.com/cm/iso17799-cobra-kondor012004.shtml (дата обращения: 18.11.2023).

27. Риски информационной безопасности // ARinteg [Электронный ресурс] — Режим доступа — https://arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html (Дата обращения: 23.11.2023).

28. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: учебное пособие / Ю.А. Родичев. — Санкт- Петербург: Питер, 2017 — 256 с.

29. Солодянников А.В. «Информационная безопасность автоматизированных систем» [Текст]: учебное пособие для вузов / А.В. Солодянников. – СПб: ГУ-ВШЭ, 2020 — 108 с.

30. Сертификация по ISO 27001 // Digital Security [Электронный ресурс] Режим доступа — https://dsec.ru/certification/iso-27001/ (дата

обращения: 24.11.2023).

31. Стандарт BS 7799-1 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/BS_7799-1/ (дата обращения: 26.11.2023).

32. Стандарт ISO/IEC 15408 // Википедия [Электронный ресурс] — Режим доступа — http://www.lghost.ru/lib/security/kurs2/theme02_chapter04.htm/ (дата обращения: 26.11.2023).

33. Стандарт ISO/IEC 17799 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/ISO/IEC_17799/ (дата обращения: 26.11.2023).

34. Стандарт ISO/IEC 27001 // Википедия [Электронный ресурс] — Режим доступа — https://ru.wikipedia.org/wiki/ISO/IEC_27001/ (дата обращения: 26.11.2023).

35. Стандарт на страже информационной безопасности // InformationSecurity [Электронный ресурс] — Режим доступа — http://www.itsec.ru/articles2/pravo/standart_na_strazhe (дата обращения: 25.11.2023).

36. Тестирование, как метод контроля качества усвоения учебного материала учащимися // Педагогическая мастерская [Электронный ресурс] — Режим доступа — http://открытыйурок.рф/статьи/500954/ (дата обращения: 23.11.2023)

37. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 01.01.2024) // КонсультантПлюс [Электронный ресурс]. – https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 24.11.2023).

38. Ярочкин В.И. Аудит безопасности фирмы: теория и практика [Текст]: учебное пособие для вузов / В.И. Ярочкин, Я.В. Бузанова. — Москва: Академический проект, 2005. — 352 с.