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 образование
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
65,91 % авторского текста

Работа рекомендована к защите
«20» 12 2026 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы: ЗФ-309-210-2-1
Пышкина Олеся Владимировна

Научный руководитель:
Зав. кафедрой АТИТ и МОТД, к.т.н., доцент
Руднев Валерий Валентинович

Челябинск
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В условиях стремительного развития информационных технологий и их внедрения в различные сферы человеческой деятельности особое внимание уделяется информационной безопасности. Образовательные организации, которые управляют большим объемом персональных данных студентов, сотрудников и других участников учебного процесса, сталкиваются с риском утечки, несанкционированного доступа и других киберугроз. В связи с этим становится актуальным вопрос создания надежной системы защиты информации и проведения регулярных аудитов информационной безопасности.

Аудит информационной безопасности представляет собой процесс систематической оценки текущего состояния защиты информации, выявления уязвимостей и разработки рекомендаций по их устранению. Эффективный аудит способствует не только повышению уровня безопасности данных, но и созданию комфортной образовательной среды для всех участников образовательного процесса, что, в свою очередь, является самым важным фактором успешного функционирования образовательной организации.

Особенная *актуальность данной работы* обусловлена тем, что практика проведения аудита образовательных организаций требует не только формального соблюдения всех регламентов, но и глубокого и качественного анализа их внутренней системы качества. В работе рассматривается организация систематического обследования документации, включая учебные планы, методические материалы, акты проверки, договоры с поставщиками образовательных услуг, а также протоколы заседаний педагогических советов. Такой подход обеспечивает объективное выявление всех отклонений от установленных стандартов и облегчает процесс подготовки предложений по улучшению.

Целью данной работы является разработка регламента проведения аудита информационной безопасности в образовательной организации, который будет

учитывать современные требования и стандарты, а также соответствовать специфике учебного процесса выбранного учебного учреждения.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1. Изучить теоретические аспекты информационной безопасности и аудита.

2. Провести анализ существующей практики проведения аудита информационной безопасности в образовательном учреждении.

3. Разработать структуру и содержание регламента аудита, учитывая выявленные проблемы и рекомендации.

Объектом исследования выступает сам процесс обеспечения информационной безопасности в образовательной организации, включая используемые технические средства, программные комплексы и организационные меры защиты.

Предметом исследования являются методы и средства проведения аудита информационной безопасности в образовательной организации, включая оценку текущего состояния защиты информации, выявление всех уязвимостей, разработку и внедрение регламентов и нормативных документов, а также повышение уровня осведомленности и подготовки персонала и учащихся в области информационной безопасности.

Практическая значимость исследования заключается в возможности использования разработанных рекомендаций и этапов тестирования слабых мест информационной безопасности в работе образовательного учреждения. Внедрение предложенных мер позволит:

1. Улучшить защиту информации: разработанные регламенты и процедуры аудита помогут выявить и устранить уязвимости в системе информационной безопасности, что сможет повысить общий уровень защиты данных в образовательной организации.

2. Снизить риски утечки данных: применение рекомендованных методов и средств защиты позволит минимизировать риски несанкционированного

доступа и утечки конфиденциальной информации, что особенно важно для образовательных учреждений, работающих с персональными и учебными данными.

3. Повысить осведомленность персонала: включение в регламент обязательных обучающих программ и тренингов для сотрудников повысит их осведомленность и навыки в области информационной безопасности, что способствует более ответственному отношению к защите данных.

4. Адаптировать меры под специфику учреждения: рекомендации могут быть адаптированы под конкретные условия и потребности различных образовательных организаций, что делает их универсальными и применимыми в разнообразных учебных заведениях.

5. Оптимизировать процессы администрирования: разработанные этапы тестирования и мониторинга помогут оптимизировать процессы администрирования информационных систем, обеспечивая их надежность и устойчивость к внешним и внутренним угрозам.

В работе раскрываются *этапы* подготовки к аудиту: формирование рабочей группы, определение целей и объема проверки, согласование плана с руководством учреждения. Подробно рассматривается процесс выявления несоответствий в системе менеджмента качества и документах, анализируется их влияние на общее состояние образовательной организации.

Одним из ключевых *аспектов* работы является оценка технических мер, направленных на защиту информации. В образовательном учреждении активно применяется цифровая инфраструктура, что требует обязательной проверки адекватности используемых средств защиты данных обучающихся, сотрудников и административной информации. В ходе аудита анализируются особенности системы контроля доступа, резервного копирования, антивирусной защиты и использования сетевых протоколов, что позволяет обеспечить безопасность и бесперебойность учебного процесса.

Важное внимание уделяется анализу компетентности персонала. Педагогические и административные работники – это базис эффективного

функционирования образовательной организации. Аудит включает оценку квалификации, участия в профессиональном развитии, а также соответствия выполняемых обязанностей утвержденным должностным инструкциям. Одновременно исследуется мотивационная сфера учебной деятельности обучающихся через изучение участия в образовательных мероприятиях, уровня вовлеченности и удовлетворенности качеством обучения.

Применение разнообразных исследовательских методов является основой для системного аудита. Используются как количественные способы, включая анкетирование и анализ статистических данных, так и качественные – интервью, наблюдение и экспертное оценивание.

Такой многоаспектный подход способствует выявлению не только формальных несоответствий, но и глубинных причин, влияющих на эффективность образовательного процесса. При этом проблемное изложение используется для структурирования выявленных проблем, что облегчает формулировку конкретных рекомендаций. Итоговые рекомендации направлены на практическое улучшение управления и повышение уровня безопасности, что отражается в повышении доверия со стороны обучающихся и их родителей, а также в соблюдении требований контролирующих органов.

В настоящее время существует ряд методик и подходов к проведению аудита информационной безопасности. Однако, учитывая специфику образовательных организаций, многие из этих методик требуют адаптации и доработки. Зачастую учебные заведения сталкиваются с отсутствием четких регламентов, что делает процесс аудита менее прозрачным и эффективным.

Таким образом, результаты исследования могут быть использованы для повышения эффективности функционирования системы информационной безопасности в образовательных учреждениях и аналогичных организациях, что делает работу практически значимой и востребованной

Глава 1: Теоретические основы аудита информационной безопасности

1.1 Основные понятия и сущность аудита информационной безопасности

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. [5]

Образовательный процесс касается наименее защищенных от пропаганды членов общества – детей и подростков. Поэтому сама 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 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. [9]

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. [15]

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. [15]

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. [19]

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. [7]

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.

Существует большое количество научных статей и книг по рассматриваемой в данной работе теме. Широкое освещение вопросов современных информационных систем обусловлено их эффективностью и

повсеместным использованием в условиях медицинских организаций, а также объектов здравоохранения. В настоящей главе будет проведен анализ наиболее известных и распространенных литературных источников, которые освещают вопросы использования информационных систем для автоматизации процессов в условиях медицинским учреждений.

Научное издание под названием «Основы проектирования информационных систем и технологий», авторами которого являются В. В. Бова и Ю. А. Кравченко, содержит много информации об основах и принципах эффективного проектирования информационных систем и программных продуктов для автоматизации обработки информации. Еще одним популярны и известным литературным изданием по рассматриваемой тематике является книга под названием «Проектирование информационных систем».

Эта книга написана коллективом авторов во главе с В. М. Вейцманам Книга охватывает широкий спектр вопросов, среди которых: степень необходимости и эффективности финансирования таких областей развития предприятия или организации как автоматизация обработки информационных ресурсов и баз данных, формирования планов развития информационной составляющей, создание высокоэффективных информационных проектов и т. д. [17]

За счет использования авторами современных методик анализа и прогнозирования в сфере информационных технологий, ими создан алгоритм определения степени актуальности и целесообразности проведения модернизации имеющихся информационных систем. Еще одна из предлагаемых методик в данной книге позволяет определить наиболее эффективный способ повышения производительности аудита информационной безопасности.

Для того, чтобы успешно и эффективно решать поставленные задачи необходимо выполнение целого ряда операций, а именно: тщательный анализ и изучение объекта, для которого планируется создание информационной системы, создание перечня требований, которые предъявляются к разрабатываемой системе, определение перечня тех инструментов

программирования, которые в наибольшей степени способны решить поставленные перед ними задачи.

При написании данной книги коллектив авторов использовал в качестве теоретической основы опыт зарубежных и отечественных специалистов в сфере автоматизации и информационных систем. Вся содержащаяся информация в книге основана как на отечественном, так и на зарубежном опыте в сфере разработки и эксплуатации информационных систем.

Основными методиками, которые предлагаются авторами книги для проектирования и создания ИС являются: функциональный анализ, теоретическое и практическое исследование, и т. д. Системность и полнота данной книги обусловили ее широкое применение в качестве базы для создания различных обучающих программ и курсов по изучению основ создания информационных систем.

Основная преследуемая цель заключается в обеспечении высокого уровня защиты данных. В процессе реализации системы безопасности информационных ресурсов обеспечивается ее надежная защита от различных угроз в виде хищения, порчи, изменения и утечки, которые могут стать причиной значительных финансовых потерь. Под термином эффективности системы информационной безопасности подразумевается соответствие целей и результатов при организации системы безопасности информационных ресурсов.

Под термином информационная защита подразумевается комплекс мероприятий, который направлен на обеспечение необходимого уровня защиты баз данных от негативного действия вредоносного программного обеспечения, а также защиту информации от несанкционированного доступа третьих лиц.

Наличие правильной политики организационной безопасности важно в контексте развития организации в любой сфере, включая и государственный сектор. Понимание важности требований стандартов международного уровняв сфере защиты информации позволяет компании из государственного сектора вести стабильную и прогнозируемую деятельность.

Чтобы добиться безопасности в отношении собственных данных, организации в данной сфере важно создать собственные процессы управления информацией, базами данных и технологиями и впоследствии поддерживать их работоспособность на высоком уровне. Не менее важно добиться такого состояния, когда будет наблюдаться доступность и целостность создаваемой и передаваемой информации.

В РФ действует утвержденная Президентом Доктрина информационной безопасности. В основе этого документа лежит комплекс целей, принципов, а также основных направлений в сфере обеспечения информационной безопасности РФ. В основе доктрины информационной безопасности лежат следующие принципы:

- под информационной безопасностью следует понимать такую степень защищенности информационных ресурсов той или иной базы данных, при которой соблюдается баланс интересов как государства в целом, так и его граждан в частности;

- в сфере информационной безопасности основными и наиболее опасными являются преступления, направленные на подрыв и нарушение конституционных прав граждан, а также на нарушение прав в сфере информационной деятельности.

1.2 Виды аудита информационной безопасности

Аудит информационной безопасности является ключевым инструментом оценки защищенности информационных систем и выявления потенциальных угроз.

В современной практике выделяют несколько основных видов аудита информационной безопасности, каждый из которых имеет свои особенности и применяется в зависимости от конкретных целей и задач организации.

Внешний аудит представляет собой независимую оценку системы информационной безопасности, проводимую специализированными организациями или экспертами со стороны. [20] Данный вид аудита является наиболее объективным, так как выполняется независимыми специалистами, не заинтересованными в результатах проверки. Внешний аудит особенно важен при:

- Прохождении сертификаций по международным стандартам
- Проверках регуляторов
- Подготовке к публичным размещениям
- Привлечении инвестиций

Внутренний аудит осуществляется силами собственных специалистов организации. Его ключевыми преимуществами являются:

- Глубокое понимание специфики организации
- Возможность постоянного мониторинга
- Более низкая стоимость
- Быстрое реагирование на выявленные проблемы

Комплексный аудит охватывает все аспекты информационной безопасности организации. Он включает:

- Проверку технических средств защиты
- Анализ организационных мер
- Оценку физической безопасности
- Контроль кадровых процедур
- Проверку документации

Тематический аудит направлен на проверку отдельных аспектов информационной безопасности. Наиболее распространенными тематическими направлениями являются:

- Аудит парольной политики
- Проверка систем резервного копирования
- Оценка антивирусной защиты
- Анализ сегментации сети
- Контроль доступа к информации

Периодический аудит проводится на регулярной основе с установленной периодичностью (ежемесячно, ежеквартально, ежегодно). Его особенности:

- Системный подход к оценке безопасности
- Возможность отслеживания динамики
- Своевременное выявление новых угроз
- Контроль выполнения ранее выданных рекомендаций

Специальный аудит проводится в особых случаях, таких как:

- Внедрение новых информационных систем
- Изменение законодательства
- После крупных инцидентов
- При слиянии или поглощении компаний
- После масштабных обновлений систем

По форме проведения выделяют:

- Документированный аудит – основывается на анализе документации
- Практический аудит – включает тестирование на проникновение
- Комбинированный аудит – сочетает оба подхода

По масштабу проверки различают:

- Аудит отдельного подразделения
- Аудит бизнес-процесса
- Аудит информационной системы
- Аудит всей организации

Каждый вид аудита имеет свои особенности подготовки, проведения и документирования результатов. Выбор конкретного вида аудита зависит от:

- Целей организации
- Текущего состояния информационной безопасности
- Доступных ресурсов
- Требований регуляторов
- Специфики бизнес-процессов

Важно отметить, что наиболее эффективной является комплексная система аудита, включающая как регулярные плановые проверки, так и специальные аудиты по мере необходимости. При этом все виды аудита должны быть взаимосвязаны и поддерживать общую стратегию информационной безопасности организации.

В современных условиях наблюдается тенденция к интеграции различных видов аудита в единую систему управления информационной безопасностью, что позволяет обеспечить непрерывный контроль и своевременное реагирование на возникающие угрозы. [4]

1.3 Этапы проведения аудита безопасности в образовательных организациях

В современном мире образовательные организации сталкиваются с множеством угроз информационной безопасности. От сохранности персональных данных учащихся и сотрудников до защиты учебных материалов и инфраструктуры – все эти аспекты требуют тщательного контроля и регулярного аудита.

Планирование аудита является первым и одним из самых важных этапов. На этом этапе формируется команда аудиторов, определяются цели и задачи проверки, разрабатывается детальный план работ. Особое внимание уделяется специфике образовательной организации, включая:

- Количество обучающихся и сотрудников
- Используемые информационные системы
- Уровень технической оснащенности
- Существующие политики безопасности

Анализ документации включает изучение:

- Локальных нормативных актов
- Документов по информационной безопасности
- Журналов регистрации инцидентов
- Схем информационных потоков
- Документов по защите персональных данных

Основной этап

Оценка технических средств защиты проводится путем:

- Проверки антивирусного ПО
- Анализа настроек межсетевых экранов
- Тестирования систем резервного копирования
- Оценки систем аутентификации
- Проверки физической защиты помещений

Анализ организационных мер включает:

- Проверку политики паролей

- Оценку процедур приема и увольнения сотрудников
- Анализ обучения персонала по ИБ
- Проверку порядка обработки персональных данных
- Контроль доступа к информационным системам

Тестирование на проникновение позволяет:

- Выявить уязвимости в системах
- Проверить эффективность средств защиты
- Оценить риски несанкционированного доступа
- Протестировать реакцию системы на атаки

Заключительный этап

Формирование отчета содержит:

- Описание выявленных уязвимостей
- Оценку рисков
- Рекомендации по устранению недостатков
- План действий по повышению безопасности
- Сроки реализации рекомендаций

Разработка рекомендаций включает:

- Технические меры по усилению защиты
- Организационные изменения
- Предложения по обучению персонала
- Рекомендации по обновлению политики безопасности
- План внедрения новых средств защиты

Особенности образовательных организаций

Специфика образовательных учреждений требует особого внимания к:

- Защите персональных данных учащихся
- Безопасности учебных материалов
- Контролю доступа к образовательным ресурсам
- Защите результатов тестирования и экзаменов

- Безопасности систем электронного документооборота

Кадровый аспект играет особую роль, так как в образовательных организациях:

- Высокая текучесть кадров
- Частое обновление учебных материалов
- Необходимость постоянного обучения персонала
- Работа с различными категориями пользователей (учащиеся, преподаватели, администрация).

Вывод по главе 1

Аудит безопасности в образовательных организациях – это комплексный процесс, требующий системного подхода и учета специфики учреждения. Регулярное проведение аудита позволяет:

- Поддерживать необходимый уровень защищенности
- Своевременно выявлять и устранять уязвимости
- Обеспечивать сохранность важной информации
- Соответствовать требованиям законодательства
- Защищать интересы всех участников образовательного процесса

Важно понимать, что аудит – это не разовое мероприятие, а непрерывный процесс, требующий постоянного внимания и совершенствования. Только системный подход к аудиту безопасности может обеспечить надежную защиту информационных активов образовательной организации.

В современных условиях цифровизации образования роль аудита безопасности только возрастает. Образовательные организации должны не просто следовать минимальным требованиям, но и постоянно совершенствовать свои системы защиты, учитывая появление новых угроз и развитие технологий. [12]

Глава 2: Разработка и внедрение методики проведения аудита информационной безопасности в образовательной организации

2.1 Идентификация объектов аудита и поставка целей

Аудит информации безопасности в образовательной организации представляет собой комплексное исследование, целью которого является выявление уязвимостей, оценка рисков и формирование рекомендаций по улучшению состояния информационной безопасности. [22]

На первом этапе аудита необходимо четко определить объекты исследования и установить цели, которые помогут сориентироваться в процессе аудита и адаптировать его под специфические потребности организации.

Идентификация объектов аудита - это процесс, в ходе которого осуществляется выявление всех активов, процессов и систем, которые имеют отношение к информационной безопасности.

В образовательной организации объекты аудита могут включать в себя: 1. Информационные системы: это любые программные и аппаратные средства, используемые для обработки, хранения и передачи данных. В контексте образовательной организации это могут быть системы управления обучением, электронные журналы и базы данных студентов.

2. Данные: академическая информация, личные данные студентов и сотрудников, а также заметки и материалы, которые хранятся и обрабатываются в информационных системах.

3. Сетевые инфраструктуры: компоненты, обеспечивающие подключение и обмен данными, такие как маршрутизаторы, коммутаторы и точки доступа Wi-Fi. Необходимо учитывать как локальные сети, так и подключение к интернету.

4. Процессы и практики: рутинные операции и процедуры, которые могут влиять на безопасность информации, включая политику доступа к данным, утилизацию информации и обучение сотрудников по вопросам информационной безопасности.

5. Физическая безопасность: защитные меры, направленные на охрану помещений и оборудования, которые могут содержать информацию, подлежащую защите. Например, системы контроля доступа, видеонаблюдение и охрана.

В Законе РФ «О защите детей от информации, причиняющей вред их здоровью и развитию» в п.4 статьи 2 дается следующее определение информационной безопасности детей: «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию».

В этом законе дано определение информационной продукции, которая находится в обороте на территории России - это продукция СМИ, в разном виде, информация, которая распространяется через зрелищные мероприятия, через информационно - коммуникационные каналы, радио, в том числе и сеть «Интернета». Информационная безопасность связана еще с некоторыми важными понятиями. Это информационная грамотность, которая заключается в поиске, интерпретации, оценке разных видов источников информации.

Понятие «медиа-грамотность» также связано с понятием «информационная безопасность», так как предполагает грамотное использование педагогами и студентами инструментами доступа к информации, владение навыками критического анализа информации любого вида, владение навыками коммуникативного общения в информационной сфере. Педагог должен сам владеть и научить школьников грамотно воспринимать информацию, интерпретировать ее, правильно использовать. [18]

Термин «информационный иммунитет» выражает способность студентов отражать негативное влияние информационной среды. Отражение является умением выявлять информационные угрозы, определять степень их опасности и противостоять им. Можно сказать, что это должно выражаться в адекватном восприятии и оценки информации на основе нравственных и культурных ценностей.

Т.А. Малых предлагает информационную безопасность определять в двух аспектах: − защита от вредного воздействия информационной среды;

− развитие на основе системы условий, обеспечивающих позитивную социализацию и индивидуализацию ребенка.

Студент должен уметь отличать нужную информацию от вредоносной, ложной. Сегодня в педагогических исследованиях обсуждается вопрос об информационной культуре. Как и другие виды культуры, она представлена совокупностью материальных и духовных ценностей в области культуры. Для того, чтобы овладеть информационной культурой, требуется время.

Исходя из этого, информационная безопасность может пониматься как защищенность ребенка от негативного воздействия информационной продукции на здоровье, на психическое, духовное, нравственное развитие ребенка. В конечном итоге создание безопасной информационной среды, может обеспечить позитивную социализацию, индивидуализацию личности, оптимальное социальное, личностное, познавательное и физическое развитие.

Итак, термин «информация» не имеет однозначного толкования. В исследовании мы будем использовать определение, обозначенное в Федеральном законе No436 «О защите детей от информации, причиняющей вред их здоровью и развитию»: информация - это сведения (сообщения, данные) независимо от формы их представления. [24]

Базой исследования был выбран ГБПОУ «Южно-Уральский Государственный Технический Колледж».

Южно-Уральский государственный технический колледж активно внедряет практики аудита для обеспечения качества образовательного процесса. Аудит в колледже включает идентификацию объектов проверки и постановку чётких целей, что позволяет систематически оценивать соответствие деятельности учреждения установленным стандартам и выявлять области для улучшения.

Объекты аудита в колледже могут включать:

Учебно-программную документацию: рабочие учебные планы, календарные графики, программы дисциплин, профессиональных модулей, практик, государственной итоговой аттестации, фонды оценочных средств.

Методические условия организации учебного процесса: локальные акты, образовательные технологии, участие работодателей в планировании обучения. Материально-техническую базу: состояние лабораторий, мастерских, компьютерных классов, соответствие оборудования требованиям ФГОС.

Качество подготовки студентов: результаты промежуточной и итоговой аттестации, участие в чемпионатах профессионального мастерства (например, WorldSkills).

Работу педагогического состава: соответствие квалификации преподавателей требованиям, эффективность методических подходов. В ЮУрГТК особое внимание уделяется аудиту образовательных программ, особенно тех, которые входят в топ-50 востребованных профессий. Например, колледж активно развивает направления IT, строительства, машиностроения, что требует регулярного контроля соответствия программ современным требованиям рынка труда.

Цели аудита в ЮУрГТК формулируются с учётом стратегических задач учреждения и требований законодательства. Оценка соответствия: проверка соответствия учебно-программной документации и методических условий требованиям ФГОС, профессиональных стандартов и региональных нормативов.

Выявление рисков и дефицитов: анализ возможных проблем в реализации образовательных программ, например, недостаточное оснащение лабораторий или пробелы в подготовке студентов.

Разработка рекомендаций: формирование предложений по улучшению качества образования, включая корректировку учебных планов, внедрение новых технологий обучения, усиление взаимодействия с работодателями.

Подготовка к внешним проверкам: обеспечение готовности колледжа к лицензированию, государственной аккредитации и контрольно-надзорным мероприятиям.

Например, в рамках подготовки к чемпионатам WorldSkills аудит может включать оценку готовности студентов к соревнованиям, анализ эффективности тренировочных программ и состояние материально-технической базы специализированных центров компетенций.

В 2025 году в колледже проводился аудит программы подготовки специалистов по направлению «Веб-дизайн и разработка». Объектами проверки стали:

- Учебные планы и программы дисциплин.
- Лаборатории и оборудование для практических занятий.
- Результаты участия студентов в чемпионатах WorldSkills.

Цели аудита включали оценку соответствия программы международным стандартам и подготовку рекомендаций по модернизации материально-технической базы. По итогам были выявлены сильные стороны (высокие результаты студентов в соревнованиях) и предложены меры по обновлению программного обеспечения в лабораториях.

2.2 Подходы к проведению аудита и методы анализа данных

В колледже действует представительство по качеству, которое организует и проводит внутренние аудиты.

Это включает: аудит системы менеджмента качества (СМК) подразделений, проверку качества учебных занятий и классных часов, оценку

обученности студентов и независимую оценку качества образования и исследование удовлетворённости потребителей.

Аудит безопасности образовательной организации рассматриваться как конфиденциальный инструмент управления, исключающий в целях конспирации возможность предоставления информации о результатах его деятельности сторонним лицам и организациям.

Для проведения аудита безопасности предприятия может быть рекомендована следующая последовательность действий.

1. Подготовка к проведению аудита безопасности:

- выбор объекта аудита (фирма, отдельные здания и помещения, отдельные системы или их компоненты);
- составление команды аудиторов-экспертов;
- определение объема и масштаба аудита и установление конкретных сроков работы.

2. Проведение аудита:

- общий анализ состояния безопасности объекта аудита;
- регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз;
- оценка результатов проверки;
- составление отчета о результатах проверки по отдельным составляющим.

3. Завершение аудита:

- составление итогового отчета;
- разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности фирмы.

Для успешного проведения аудита безопасности необходимо:

• активное участие руководства фирмы в его проведении;

• объективность и независимость аудиторов (экспертов), их компетентность и высокая профессиональность;

• четко структурированная процедура проверки;

• активная реализация предложенных мер обеспечения и усиления безопасности. Аудит безопасности, в свою очередь, является действенным инструментом оценки безопасности и управления рисками.

Предотвращение угроз безопасности означает в том числе и защиту экономических, социальных и информационных интересов предприятия. Отсюда можно сделать вывод, что аудит безопасности становится инструментом экономического менеджмента.

В зависимости от объема анализируемых объектов предприятия определяются масштабы аудита:

- аудит безопасности всего предприятия в комплексе;

- аудит безопасности отдельных зданий и помещений (выделенные помещения);

- аудит оборудования и технических средств конкретных типов и видов;

- аудит отдельных видов и направлений деятельности: экономической, экологической, информационной, финансовой и т. д.

Следует подчеркнуть, что аудит проводится не по инициативе аудитора, а по инициативе руководства предприятия, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства предприятия является необходимым условием для проведения аудита. Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора, оказываются

задействованными представители большинства структурных подразделений компании.

Действия всех участников этого процесса должны быть скоординированы. Поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы:

- 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 предприятия обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. Если какие-то информационные подсистемы предприятия не являются достаточно критичными, их можно исключить из границ проведения обследования.

Другие подсистемы могут оказаться недоступными для аудита из-за соображений конфиденциальности.

В настоящее время используются три основных метода (подхода) к проведению аудита, которые существенно различаются между собой.

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

Данный подход является наиболее трудоемким и требует наивысшей квалификации аудитора. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками и ее применимость к данному типу ИС.

Второй метод, 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, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т.п.).

От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Необходима также методика, позволяющая оценить это соответствие. Из-за своей простоты (стандартный набор требований для проведения аудита уже заранее определен стандартом) и надежности (стандарт - есть стандарт и его требования никто не попытается оспорить), описанный подход наиболее распространен на практике (особенно при проведении внешнего аудита).

Он позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии ИС.

Третий метод, наиболее эффективный, предполагает комбинирование первых двух. Если для проведения аудита безопасности выбран подход, базирующийся на анализе рисков, то на этапе анализа данных аудита обычно выполняются следующие группы задач:

1. Анализ ресурсов ИС, включая информационные ресурсы, программные и технические средства, а также людские ресурсы.
2. Анализ групп задач, решаемых системой, и бизнес процессов.

3. Построение (неформальной) модели ресурсов ИС, определяющей взаимосвязи между информационными, программными, техническими и людскими ресурсами, их взаимное расположение и способы взаимодействия.

4. Оценка критичности информационных ресурсов, а также программных и технических средств.

5. Определение критичности ресурсов с учетом их взаимозависимостей.

6. Определение наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз.

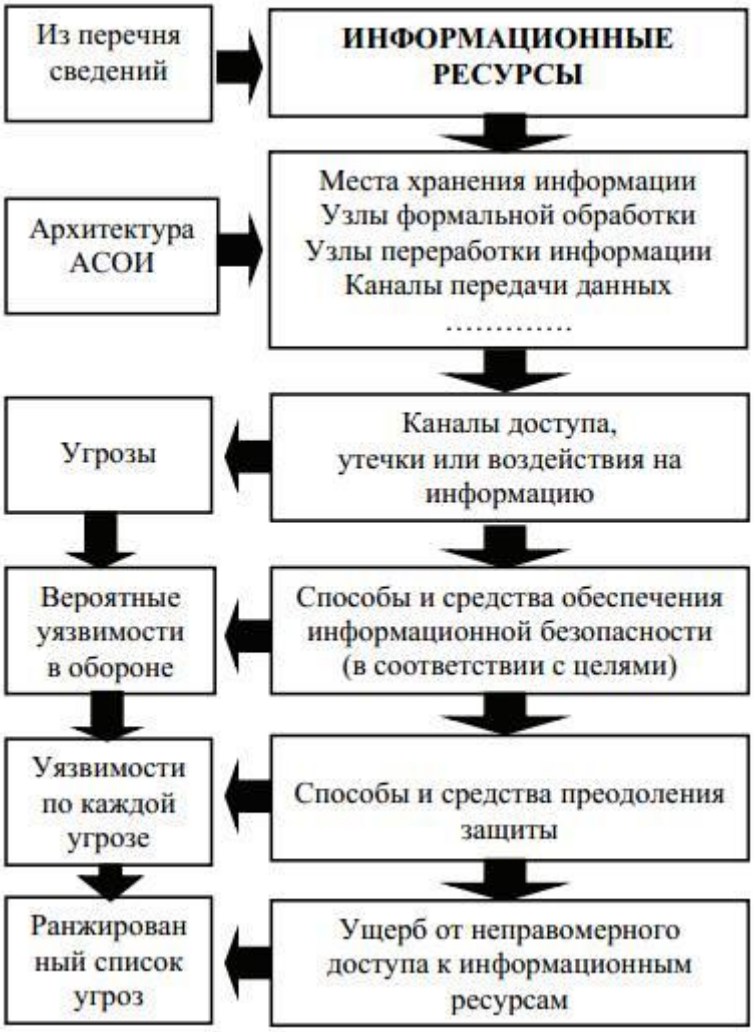
7. Оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз.

8. 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 про ранжированы 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.

При проведении аудита безопасности на соответствие требованиям стандарта, аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой ИС и ее соответствие этим требованиям.



В трудах современных философов метод все больше становится «средством реализации научного подхода к исследуемым явлениям, « в ходе практической деятельности. Метод определяется как «путь познания, опирающийся на некоторую совокупность ранее полученных общих знаний». Таким образом, в философии метод воспринимается именно как возможность познания истины. Другие науки конкретизируют и детализируют метод научного познания, рассматривая его как приемы, способы, инструменты познания предметов и явлений.

«Метод - это система принципов, приемов, правил, требований, которыми необходимо руководствоваться в процессе познания». Следовательно, общенаучные методы представляют собой специальные приемы, способы и инструменты. Вполне общепринятым можно считать и то, что каждая отрасль науки используемые приемы, способы и средства определяет как методы, а

применение методов в какой-либо отдельной отрасли науки с четкой последовательностью действий - как методику.

И все же метод следует понимать более широко: он характеризует технологию научного познания, являясь способом познавательной деятельности, ее правилом и нормой. Что касается аудита, то здесь должен использоваться довольно широкий арсенал различных методов. При этом последние, будучи по сути субъективными, могут по-разному интерпретироваться в зависимости от целей и задач, которые ставятся в той или иной ситуации перед аудитом. Обратим внимание на то, что с помощью методов (способов, приемов, инструментов) не только познается объект аудита, но, что особенно важно, упорядочивается также процесс его организации. [15]

К сожалению, в настоящее время неизвестны факты проведения кем-либо специальных исследований по вопросам методов аудита, не говоря уже о внутреннего аудита. Более того, даже в учебной методической литературе по аудиту эти вопросы как будто бы специально замалчиваются. Исключением здесь являются, пожалуй, лишь работы А.Д. Шеремета и В.П. Суйца, а также Л.Р. Смирновой. В практической работе большинство аудиторов сейчас используют лишь незначительную часть существующих методов. При такой ситуации аудит хотя и претендует на высокоинтеллектуальный вид деятельности по уровню научной обеспеченности, он по существу продолжает оставаться не чем иным, как ремеслом.

Именно поэтому возникает объективная необходимость во всестороннем изучении и научной классификации известных специалистам и возможных к использованию методов проведения аудита. Как в среде практикующих аудиторов, так и среди научных работников принято считать, что методы аудита содержатся в стандартах аудиторской деятельности. Строго говоря, это не совсем так.

Действительно, некоторые рекомендации о методах организации проведения аудита, сбора аудиторских доказательств содержатся в ряде российских стандартов аудиторской деятельности, таких как: «Аудиторские

доказательства», «Аудиторская выборка», «Действия аудитора при выявлении искажений бухгалтерской отчетности», «Использование работы эксперта». Но методы организации проведения аудита, методы сбора аудиторских доказательств — это, строго говоря, не есть методы аудита. Нельзя считать методами аудита и аудиторские процедуры. [1]

Одна из важнейших функций аудита заключается в том, чтобы своевременно выявить негативные явления в хозяйственно-финансовой деятельности проверяемой организации и способствовать их корректировке до того, как эти проблемы перерастут в кризис (до даты составления аудиторского заключения). Поэтому в аудиторской практике возникает необходимость использования различных форм осуществления, во времени и в пространстве, контроля с целью своевременной выработки для клиента направлений управления финансами и способов использования ресурсов.

Форма осуществления контроля характеризует методологические аспекты и зависимости от признака, лежащего в основе того или иного методологического подхода, выделяют различные формы проведения контроля. К таким признакам относятся время проведения контроля, источники контрольных данных, способы и приемы его осуществления. В зависимости от времени проведения аудита можно различать предварительный, текущий и заключительный (последующий) контроль.

Предварительный аудиторский контроль осуществляется до начала работ, совершения хозяйственных операций, подвергавшихся проверке, и направлен на предупреждение незаконности и нецелесообразности выполнения работ, проведения хозяйственных операций в организации. [5]

В организациях предварительный контроль используется в ключевых областях — по отношению к трудовым, материальным и финансовым ресурсам. Форма предварительного контроля играет важную роль в повышении уровня знаний хозяйственных кадров, их профессионализма, ответственности за соблюдение законности, целесообразности и эффективности использования

хозяйственных ресурсов. Предварительный контроль чаще всего проводится внутренними аудиторами и специалистами организации.

За последние годы предварительный контроль проводится также независимыми внешними аудиторами и аудиторскими фирмами путем проведения консультационной работы в данной организации, экспертизы различных схем, проектов, бизнес-планов и т.п. Особенно предварительный контроль необходим для проверки качества материальных ресурсов до их производственного использования, а также планируемых инвестиций, финансовых вложений и финансовых операций.

Эта форма контроля необходима также для разработки проектов и экспертизы уже готовых договоров различного характера для заключения с юридическими и физическими лицами, для разработки схем и проектов организации бухгалтерского учета, оптимизации учетной политики, производства продукции (работ, услуг), маркетинга, налогооблагаемых баз, бюджета и других планов организации. В аудиторской практике предварительный контроль может быть использован также для оценки существенности (материальности) в аудите.

Текущий аудиторский контроль проводится непосредственно в ходе осуществления работ или в процессе совершения хозяйственных операций и направлен на оперативное устранение недостатков, распространение (внедрение) научно обоснованного положительного опыта. Преимущества данной формы техники проведения контроля заключаются в возможности своевременного выявления и устранения допущенных ошибок в бухгалтерских проводках, при нарушении положений законодательных и нормативных актов, связанных с начислением налогов и т.д.

Текущая аудиторская проверка позволяет устранить «наследственные» (типичные для данной организации) ошибки и способствует в дальнейшем недопущению таких или аналогичных ошибок, а также позволяет свести до минимума «наследственный» (присущий) и контрольный (процедурный) риски при аудировании финансовой отчетности организации. Текущие проверки

проводят как внутренние аудиторы, так и независимые внешние аудиторы и аудиторские фирмы путем наблюдения, обследования объектов контроля, консультирования специалистов и руководителей организаций посредством абонентского обслуживания по возникающим правовым, управленческим, налоговым, аналитическим и другим проблемам.

Кроме того, текущий аудиторский контроль может проводиться аудиторами, аудиторской фирмой на данном экономическом субъекте по договоренности с ним поэтапно, например, помесячно, поквартально и т.д., т.е. не ожидая конца года, когда хозяйственные операции уже завершены и на некоторые из них повлиять фактически уже невозможно. [5]

Текущий аудиторский контроль может быть использован как при инициативном, так и при обязательном аудите с целью подтверждения достоверности данных финансовой отчетности организации в конце проверяемого года. Заключительный (последующий) аудиторский контроль осуществляется после выполнения работ и совершения хозяйственных операций. Хотя заключительный (последующий) контроль осуществляется слишком поздно, чтобы ориентировать на проблемы в момент их возникновения, тем не менее в аудиторской практике он выполняет важные функции.

Одна из них состоит в том, что заключительный контроль дает руководству организации информацию о недостатках и ошибках, рекомендации по их устранению и недопущению в будущем. Сравнивая фактически полученные и требовавшиеся результаты работы, руководство имеет возможность оценить, насколько реалистично и обоснованно были проведены работы, хозяйственные операции, составлены планы и т.д.

Эта процедура позволяет также получить информацию о возникших проблемах и сформулировать новые направления действий, чтобы избежать этих проблем в будущем.

2.3 Практическая реализация методики проведения аудита в образовательной организации

Подготовительный этап аудита в образовательной организации начинается с тщательного сбора локальных нормативных актов, регламентирующих деятельность учреждения. В эту группу документов входят устав, положения о структурных подразделениях, правила внутреннего распорядка, а также приказы, инструкции и методические рекомендации, разработанные специально для конкретного учебного заведения. Такой комплекс документов формирует юридическую основу образовательного процесса и организационной деятельности, обеспечивая единые стандарты и порядок работы.

Одновременно с нормативными актами собирается документация, связанная с системой менеджмента качества. В образовательных организациях это могут быть политики качества, процедуры проведения контроля учебного процесса, планы мониторинга эффективности педагогической деятельности, отчёты о внутреннем аудите. Анализ данных документов позволяет оценить практическую реализацию заявленных стандартов, выявить полноту и актуальность процедур, а также определить правдивость представленной информации.

Особое внимание уделяется систематичности и полноте документов. Их целостность обеспечивает возможность проведения комплексного аудита без пропусков важных аспектов. Для этого составляется перечень необходимых документов, с учётом спецификации организации и требований законодательства. При наличии недостающей информации формируется запрос на её предоставление, что предотвращает задержки в работе аудиторской группы.

На этапе подготовки также анализируется соответствие внутренних процедур установленным нормативам. Например, проверяется, соблюдается ли порядок утверждения учебных программ, корректно ли оформляются протоколы педагогических советов, ведется ли контроль над выполнением планов повышения квалификации сотрудников. Такая предварительная обработка данных помогает определить потенциальные зоны риска и обеспечить структурированный подход к последующему аудиту.

Кроме документов, подготовительный этап включает организационные задачи: определяется состав аудиторов, распределяются обязанности и устанавливаются сроки проведения проверочных мероприятий. Важно, чтобы все участники процесса имели четкое понимание целей аудита и знали порядок взаимодействия с сотрудниками образовательной организации. Это создаёт баланс между независимостью аудиторов и сотрудничеством с коллективом, что улучшает качество проверки.

Таким образом, подготовительный этап не ограничивается сбором и анализом документов, он формирует основу для последовательного и обоснованного проведения аудита. Качество и полнота подготовительной работы определяют эффективность выявления проблем и разработку рекомендаций. После подготовки документов переходят к выявлению возможных несоответствий.

Рисунок 1 — Структура локальных актов образовательного учреждения для подготовки к аудиту

После сбора документов следует выявление несоответствий. Этот процесс базируется на сравнении фактического состояния материалов и процессов с установленными нормативами и требованиями системы менеджмента качества. Один из основных методов – проверка актуальности документации.

Так, если установлено, что учебные планы не обновлялись в течение нескольких лет и не соответствуют изменениям в образовательных стандартах, это указывает на устаревшие документы, которые могут привести к неприятию аттестационными органами или снижению качества образовательных программ.

Другой распространённый пример несоответствия – отсутствие или неполнота локальных регламентов, регулирующих важные процессы. Например, если в учреждении отсутствует четко оформленный порядок проведения внутренней аттестации педагогического персонала, это может привести к неоднозначности оценок квалификаций и, как следствие, к недостаточному уровню профессионализма сотрудников. Такой пробел существенно снижает управляемость и мотивацию педагогов.

Метод сравнительного анализа протоколов педагогических советов и фактических данных обучения позволяет выявить несогласованности. Например, если протоколы заседаний не содержат информации о принятых мерах по исправлению выявленных недостатков или отсутствуют записи о рассмотрении жалоб обучающихся, это свидетельствует о формальном подходе к процессу управления качеством и слабом контроле за его реализацией.

Еще один способ выявления несоответствий – проведение опросов и интервью с сотрудниками и студентами. Наличие разногласий между официальными документами и реальными условиями работы может указывать на скрытые проблемы.

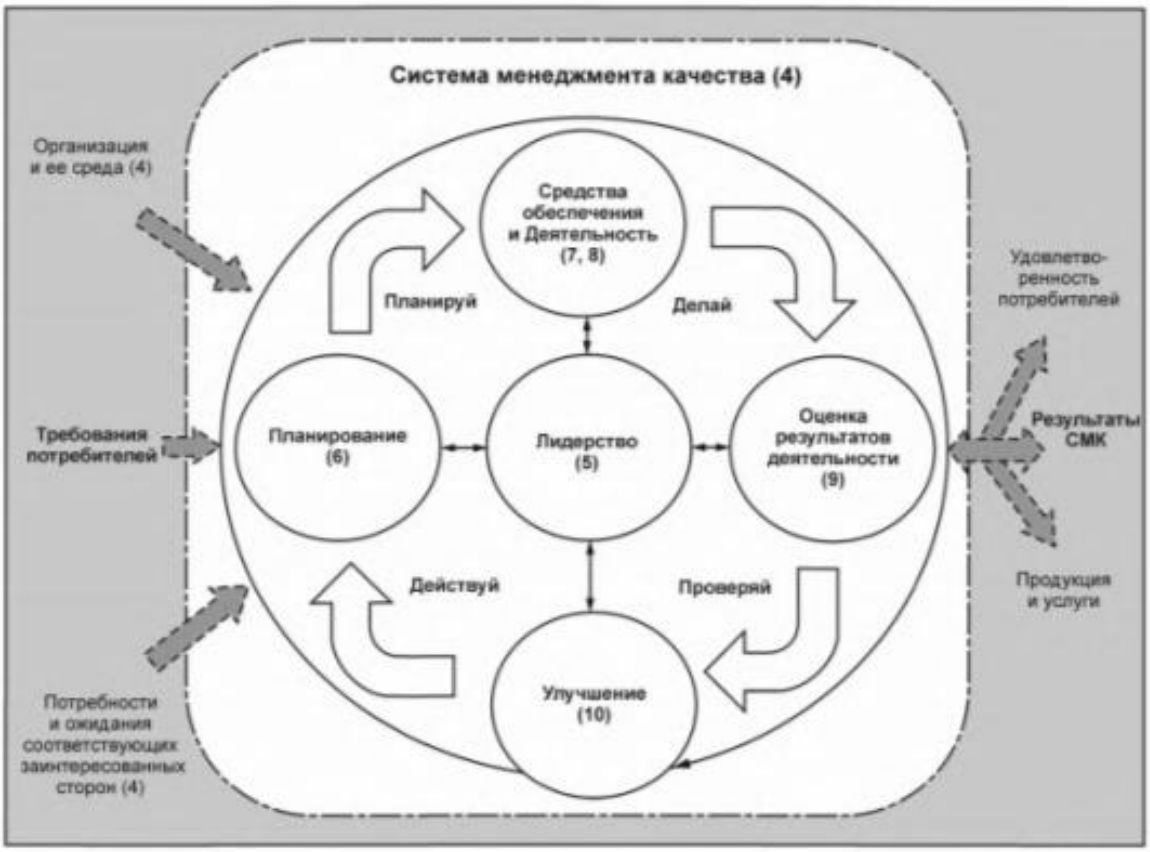
Например, формальное наличие утвержденных графиков повышения квалификации без фактического исполнения отражает разрыв между заявленной и фактической деятельностью организации.

Несоответствия могут привести к серьезным последствиям. Устаревшие документы затрудняют адаптацию к новым требованиям законодательства, что влечёт за собой риск возникновения штрафных санкций и потери аккредитации.

Отсутствие регламентов и несогласованность процессов ведут к дублированию функций, снижению эффективности управления и ухудшению образовательного процесса. Нарушения в оформлении документации могут осложнить проведение внешних проверок и вызвать недоверие со стороны обучающихся и их родителей.

Выявленные несоответствия требуют дальнейшей проверки технических мер безопасности.

Рисунок 2 — Схема системы менеджмента качества и классификатор несоответствий в документации



Примечание — Цифры в скобках являются ссылками на разделы настоящего стандарта.

Рисунок 3 — Схема системы менеджмента качества и классификатор несоответствий в документации

Далее выполняется оценка технических мер по защите информации. Этот этап направлен на анализ используемых в образовательной организации средств защиты данных, включая аппаратные и программные решения, а также их интеграцию в общую инфраструктуру безопасности.

Первым шагом является проверка настройки систем контроля доступа. Анализируются применяемые методы аутентификации пользователей: использование паролей, биометрических данных, карточек доступа или многофакторной аутентификации. В ходе аудита оценивается сложность паролей, политика их смены и наличие механизмов ограничения количества попыток входа. Недостатки в этих настройках ухудшают защиту конфиденциальной информации и увеличивают риски несанкционированного доступа.

Затем проводится анализ сети и средств защиты на уровне сетевого взаимодействия. Проверяются наличие и актуальность межсетевых экранов (фаерволов), систем обнаружения и предотвращения вторжений (IDS/IPS), а также использование зашифрованных каналов передачи данных, таких как VPN или SSL. Обращается внимание на сегментацию сети, которая минимизирует распространение возможных угроз между подсистемами и защищает критическую инфраструктуру.

Оценке подлежат средства антивирусной и антимальварной защиты. Аудитору необходимо убедиться в установленности актуальных версий программного обеспечения, регулярном обновлении баз сигнатур и наличии автоматизированных сканирований. Также проверяется использование централизованных средств администрирования для оперативного реагирования на инциденты и предотвращения распространения угроз.

Тестируются процедуры резервного копирования и восстановления данных. Анализируется регулярность создания копий, их защищенность и хранение в удалённых или защищённых средах. Эффективные меры резервного копирования позволяют минимизировать последствия сбоев и атак, обеспечивая сохранность информации и непрерывность образовательного процесса.

Особое внимание уделяется физической безопасности серверного и сетевого оборудования. В ходе проверки фиксируется наличие охраны, видеонаблюдения, систем контроля доступа к помещениям и условия хранения носителей информации. Недостаточная физическая защита может свести на нет все электронные меры безопасности.

Проводится аудит журналирования и мониторинга событий безопасности. Анализируются процедуры регистрации действий пользователей, обнаружения аномалий и реагирования на инциденты. Возможность своевременного выявления и расследования нарушений напрямую зависит от полноты и качества записываемой информации.

На завершающем этапе технической оценки проводится моделирование потенциальных угроз с использованием сканеров уязвимостей и средств тестинга. Результаты позволяют выявить скрытые дефекты в настройках и реализации защитных механизмов, что служит основой для составления рекомендаций по их устранению.

Эффективность технических мер влияет на востребованность компетенций руководящего персонала.

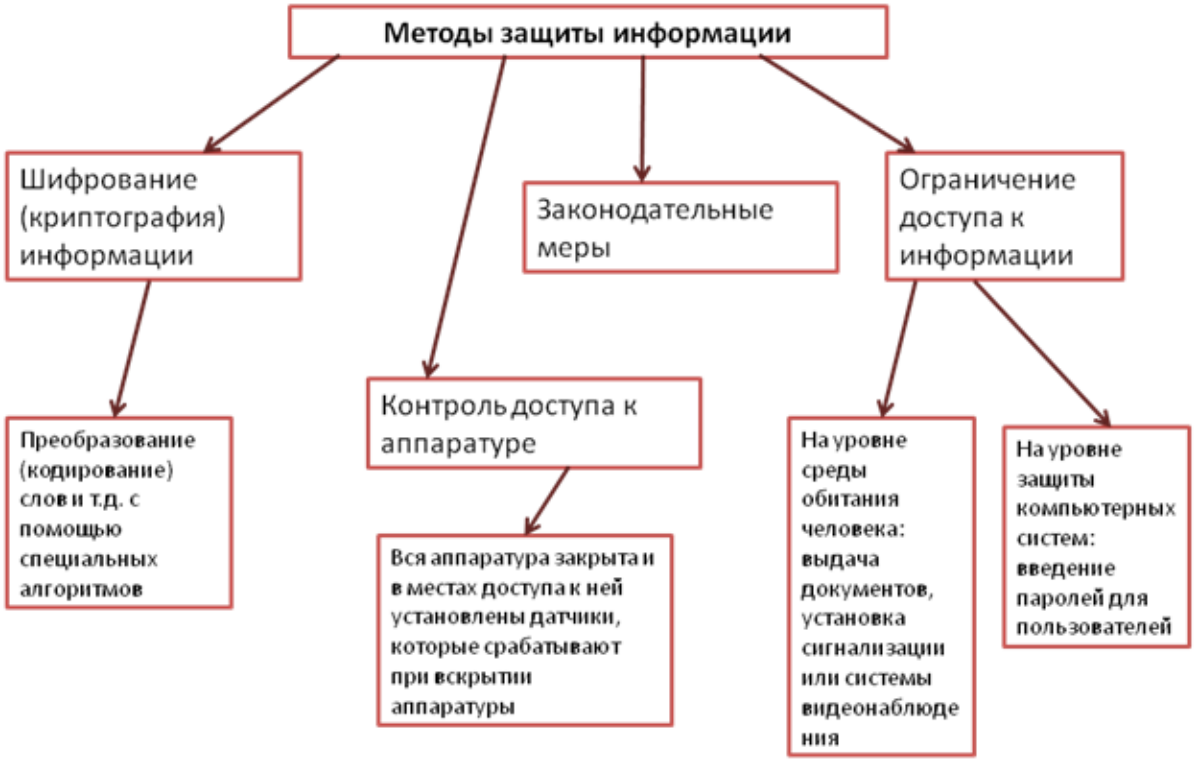


Рисунок 4 — Методы защиты информации в образовательной организации

Следующий этап — оценка компетентности педагогического и административного персонала. Оценка начинается с анализа уровня квалификации сотрудников, что предполагает проверку наличия профильного образования, сертификатов повышения квалификации и участия в методических семинарах. Проводится сопоставление фактических компетенций с должностными обязанностями и требованиями образовательного стандарта. Особое внимание уделяется умению персонала организовать учебный процесс с учетом современных педагогических технологий и индивидуальных потребностей обучающихся, что отражается в применении интерактивных методов обучения, адаптации материалов и использовании цифровых ресурсов.

Для административных работников критично оценить умение координировать деятельность учреждения, вести документацию, обеспечивать взаимодействие между структурными подразделениями и контролировать выполнение нормативных требований. Знание информационных систем и баз данных, умение работать с конфиденциальной информацией также входят в критерии оценки, поскольку от этого зависит поддержание integrity и конфиденциальности данных обучающихся.

Проверка компетентности включает анализ результатов проведения внутреннего контроля качества учебного процесса: своевременность и полнота составления отчетов, адекватность принимаемых управленческих решений, способность выявлять и устранять недостатки. Важна также способность педагогов и администрации к самообразованию и адаптации к изменениям в образовательной среде и нормативной базе.

Связь между компетентностью персонала и обеспечением информационной безопасности проявляется в осознанном соблюдении правил работы с документами и данными обучающихся, понимании рисков, связанных с обработкой персональной информации, и применении необходимых мер для предотвращения утечек. Персонал должен быть подготовлен к выявлению и своевременному реагированию на инциденты безопасности, что снижает вероятность возникновения критических ситуаций.

В итоге, оценка компетенций выявляет потенциальные пробелы в подготовке, которые могут негативно влиять на качество образовательного процесса и безопасность данных. Результаты анализа позволяют сформулировать рекомендации по совершенствованию профессионального развития сотрудников, что укрепляет устойчивость учреждения к внешним и внутренним вызовам.

Компетентность персонала напрямую связана с мотивацией обучающихся.

Рисунок 5 — Схема профессиональных компетенций учителя, отражающая ключевые навыки и умения педагогического персонала

Одним из ключевых аспектов является мотивация учебной деятельности учащихся. Она выступает основным двигателем, обусловливающим активность, настойчивость и заинтересованность в процессе получения знаний. В образовательной среде мотивация складывается под влиянием внутренних и внешних факторов, включая личностные потребности, восприятие значимости учебного материала и реакцию на педагогическое оценивание.

Педагогическое оценивание играет важную роль в формировании мотивации. Адекватная обратная связь, основанная на объективных критериях, способствует развитию у обучающихся чувства успеха и уверенности в своих возможностях. При этом конструктивная критика, ориентированная на процесс обучения, помогает формировать установки на саморазвитие и постановку достижимых целей. Напротив, демотивирующее или некорректное оценивание может вызвать снижение интереса к предмету и уменьшить учебную активность.

Формирование личностно значимых учебных задач влияет на то, насколько учебный материал воспринимается как важный и нужный для достижения личных целей. Учебные задачи, связанные с реальными жизненными ситуациями или профессиональными интересами, стимулируют внутреннюю мотивацию, способствуют развитию самостоятельности и ответственности. Важным элементом является также возможность выбора форм и методов деятельности, что позволяет студентам реализовывать индивидуальные образовательные стратегии.

Кроме того, мотивацию подкрепляют социальные факторы: поддержка преподавателей, взаимодействие с коллегами-обучающимися и признание успехов как внутри группы, так и со стороны учебного заведения в целом. Наличие положительной учебной среды способствует формированию устойчивых мотивационных установок и снижает уровень конфликтов и дезадаптации.

При анализе мотивации необходимо учитывать динамику изменения интересов и потребностей обучающихся, а также их эмоциональное состояние и

уровень стрессоустойчивости. Мониторинг этих аспектов позволяет своевременно корректировать образовательные и воспитательные стратегии.

Мотивация обучающихся требует глубокого анализа с использованием различных методов аудита.

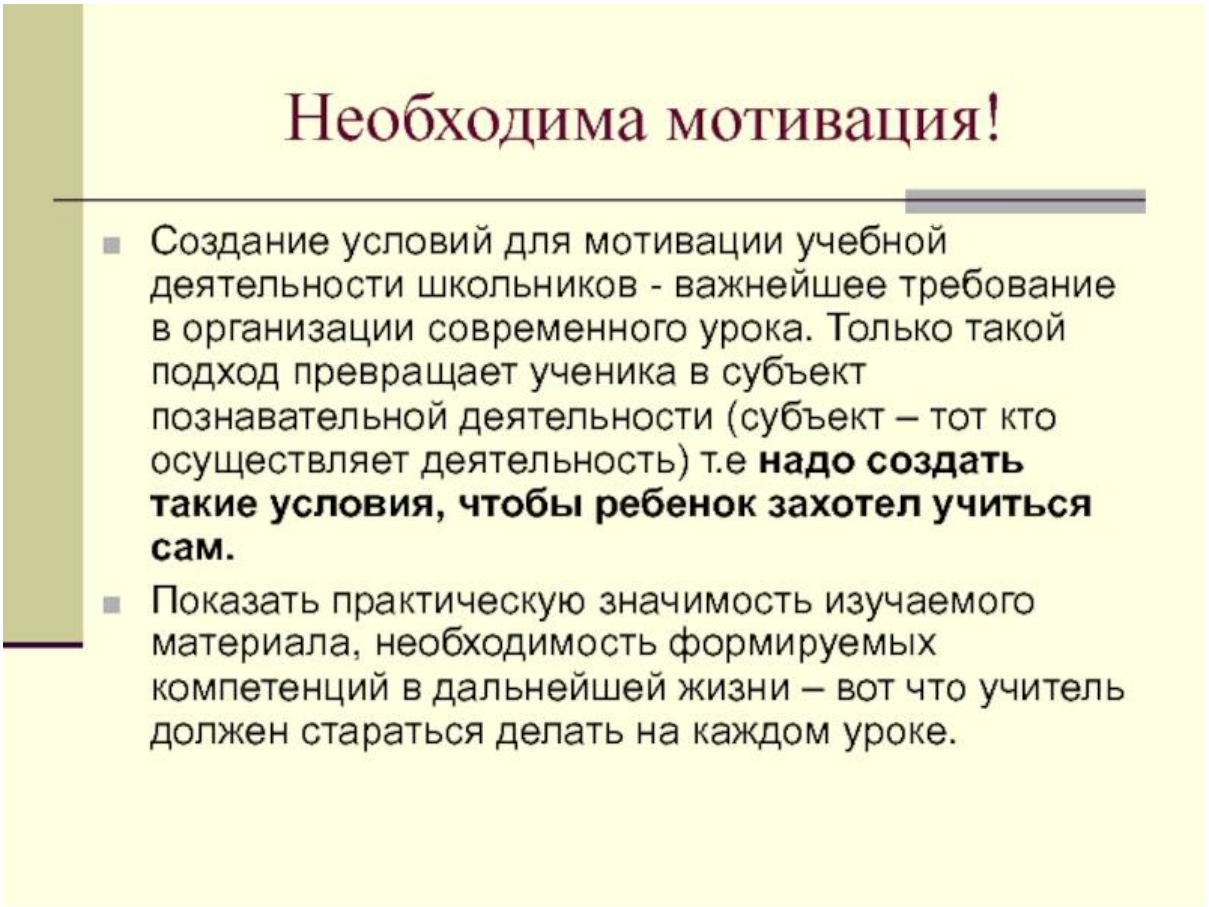


Рисунок 6 — Схемы, иллюстрирующие мотивацию учебной деятельности и её компоненты

Рисунок 7 — Схемы, иллюстрирующие мотивацию учебной деятельности и её компоненты

Ключевым методом является исследовательский подход, обеспечивающий системное выявление проблем и глубокий анализ данных в ходе аудита образовательной организации. Его суть заключается в использовании комплексных инструментов сбора, обработки и интерпретации информации, что позволяет получать объективные и обоснованные выводы о состоянии учебного и управленческого процессов.

В первую очередь применяются количественные методы, такие как анкетирование и статистический анализ, которые помогают формировать общую картину и выявить тенденции. Например, с помощью опросов можно определить уровень удовлетворённости обучающихся и сотрудников условиями работы, а количественные показатели дают возможность оценить эффективность внедрённых процедур и программ. При этом важна корректная постановка вопросов и репрезентативность выборки, чтобы избежать искажений данных.

Качественные методы включают интервью, фокус-группы и наблюдение, что даёт возможность получить развернутую информацию о внутренней культуре организации, особенностях взаимодействия и скрытых проблемах, которые трудно выявить количественными способами. Интервью с педагогами и администрацией раскрывают причины сложностей, связанные с управленческими решениями или особенностями реализации учебных планов. Наблюдение за учебным процессом и рабочей обстановкой помогает оценить соответствие практики формальным требованиям.

Основное внимание уделяется интеграции различных методов, что позволяет компенсировать ограничения каждого из них. Триангуляция данных способствует более полному и точному пониманию проблематики, исключая субъективизм и неполноту информации. Кроме того, использование современных цифровых инструментов сбора и обработки данных ускоряет проведение аудита и обеспечивает его достоверность.

Особое значение имеет систематизация полученных сведений и их структурирование в соответствии с целями проверки. При этом требуется выделить ключевые проблемные зоны с учётом внутренних и внешних факторов,

влияющих на эффективность образовательной деятельности. Изучение взаимосвязей между различными аспектами позволяет выстроить логическую модель выявленных недостатков.

Важным этапом является подготовка отчётности, оформляемой в форме, удобной для восприятия заказчиком. В отчёте отражаются не только факты, но и их причинно-следственные связи, что позволяет руководству образовательной организации принимать обоснованные управленческие решения.

Исследовательские результаты подводят к применению проблемного изложения для обсуждения обнаруженных вопросов.

Рисунок 8 — Схема технологического аудита в образовательных организациях, показывающая этапы и методы аудита

Следующий этап — применение метода проблемного изложения. Этот метод позволяет структурировать результаты аудита, выделяя ключевые проблемы, их причины и последствия. В отличие от простого описания фактов, проблемное изложение фокусируется на выявлении внутренних противоречий и недостатков, которые затрудняют эффективное функционирование образовательной организации.

В основе метода лежит логический анализ: каждое выявленное несоответствие рассматривается с позиции его влияния на качество образовательного процесса, безопасности информации или организационную культуру. Такой подход помогает избежать поверхностной оценки и перейти к глубокому пониманию системных трудностей. Для этого формулируется проблема в конкретной, ясной и однозначной форме, что облегчает восприятие и стимулирует поиск решений.

При составлении проблемного изложения важно выявить причины проблемы — технические, управленческие или человеческие факторы. Например, отсутствие регулярного обновления документации может быть вызвано недостатком ответственных лиц или несовершенством внутренних регламентов. Анализ последствий помогает оценить масштабы негативного воздействия на учебный процесс, безопасность и соблюдение нормативных требований.

Далее выявленные проблемы систематизируются по приоритетности и взаимосвязям. Это позволяет выявить непосредственные и корневые причины, что становится основой для постановки целей и задач по их устранению. Важной частью является визуализация проблемных связей, которая помогает наглядно представить круг взаимодействия различных факторов.

Проблемное изложение учитывает также особенности образовательной организации и внешние обстоятельства, что обеспечивает адаптацию рекомендаций к конкретным условиям. Такой индивидуализированный подход повышает вероятность успешного внедрения предложенных мер.

На этапе обсуждения результатов с руководством и персоналом проблемное изложение выступает инструментом коммуникации, способствующим формированию общего понимания выявленных трудностей. Оно помогает выстроить конструктивный диалог и определить ответственных за реализацию изменений.

Проблемное изложение способствует формированию конкретных рекомендаций по устранению выявленных недостатков.

Рисунок 9 — Схема проблемного изложения для структурирования результатов аудита

Завершающим этапом является формулировка рекомендаций, базирующихся на выявленных в ходе аудита несоответствиях и анализе их причин. Рекомендации структурируются по направлениям улучшения: обновление и актуализация документации, усиление технических мер защиты информации, повышение квалификации персонала, а также повышение мотивации и вовлечённости обучающихся.

Каждая рекомендация должна содержать конкретные действия, сроки реализации и ответственных исполнителей, что обеспечивает их оперативное выполнение и контроль.

Для успешного внедрения изменений разрабатывается поэтапный план, включающий подготовительный, основной и контрольный блоки. На подготовительном этапе необходимо информировать всех участников образовательного процесса о предстоящих изменениях через совещания, обучающие семинары и рассылки методических материалов. Важно обеспечить понимание целей реформ и формирование позитивного отношения к нововведениям.

Основной этап предусматривает практическое применение рекомендаций, реализуемое путем корректировки нормативных актов, внедрения новых процедур и технологий, а также проведения тренингов для персонала. При этом необходимо наладить механизм постоянного взаимодействия между различными отделами учреждения, чтобы исключить дублирование функций и обеспечить согласованность действий. Для контроля за ходом реализации формируются рабочие группы с чёткими полномочиями и инструментами мониторинга.

Контрольный этап включает оценку результатов выполненных мероприятий через внутренние проверки и анализ ключевых показателей эффективности. Выявленные отклонения требуют корректирующих мер и могут стать поводом для дополнительного аудита по узким направлениям. Такой цикл способствует непрерывному улучшению качества образовательных услуг.

Практическое внедрение выводов аудита также требует создания системы мотивации для сотрудников, стимулирующей активное участие в реализации изменений. Это может включать поощрение за инициативность, предоставление возможностей для профессионального роста и признание достижений на уровне учреждения. [5]

Результаты аудита и рекомендации оформляются в виде подробного отчёта, который служит руководством к действиям и базой для последующего стратегического планирования развития организации. Важно, чтобы данный

документ регулярно пересматривался и дополнялся с учётом новых условий и потребностей.

Таким образом, практическое применение результатов аудита выступает основой для повышения эффективности управления и качества образовательного процесса. Только через системное внедрение разработанных мер образовательная организация может добиться устойчивого развития и соответствия современным требованиям, что в конечном итоге позитивно сказывается на подготовке обучающихся и укреплении её репутации.

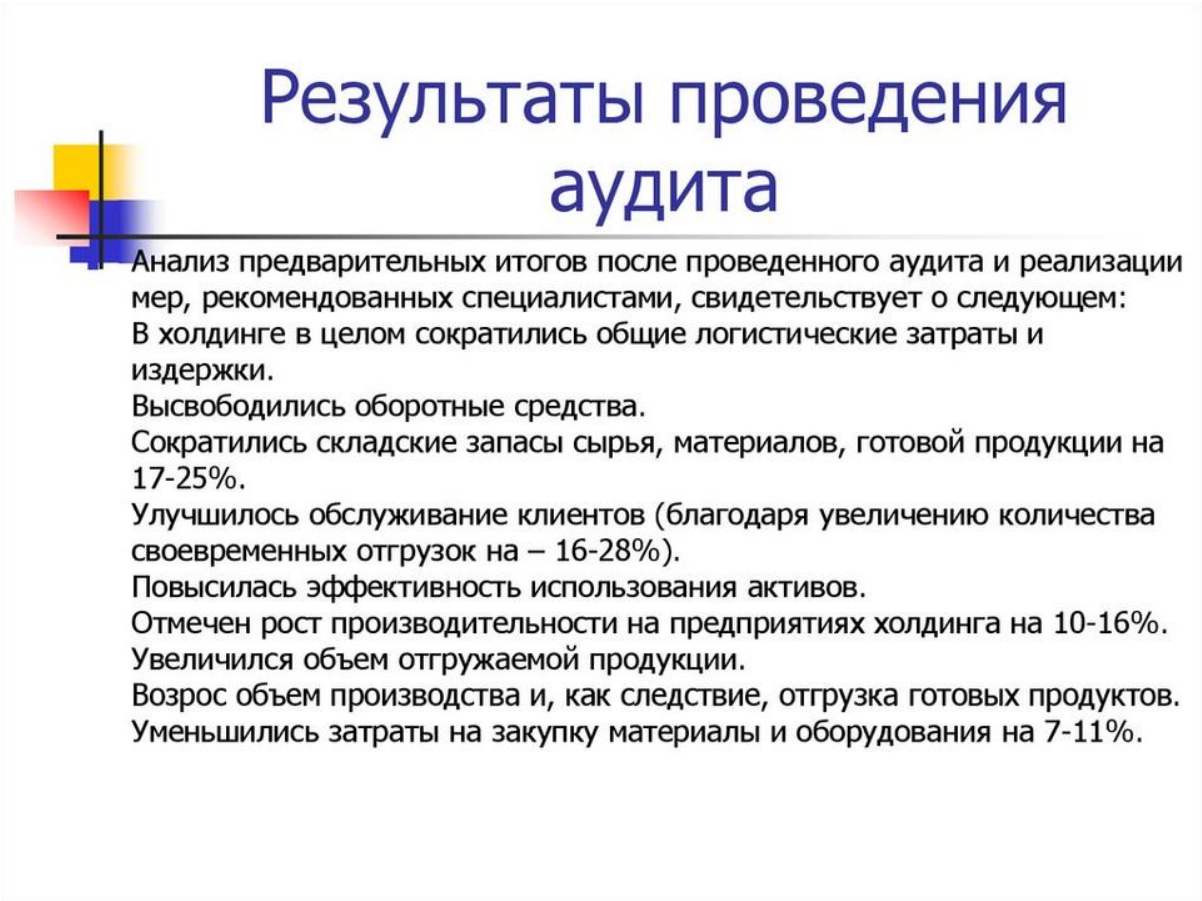


Рисунок 10 — Результаты аудита и рекомендации по повышению эффективности управления образовательным процессом

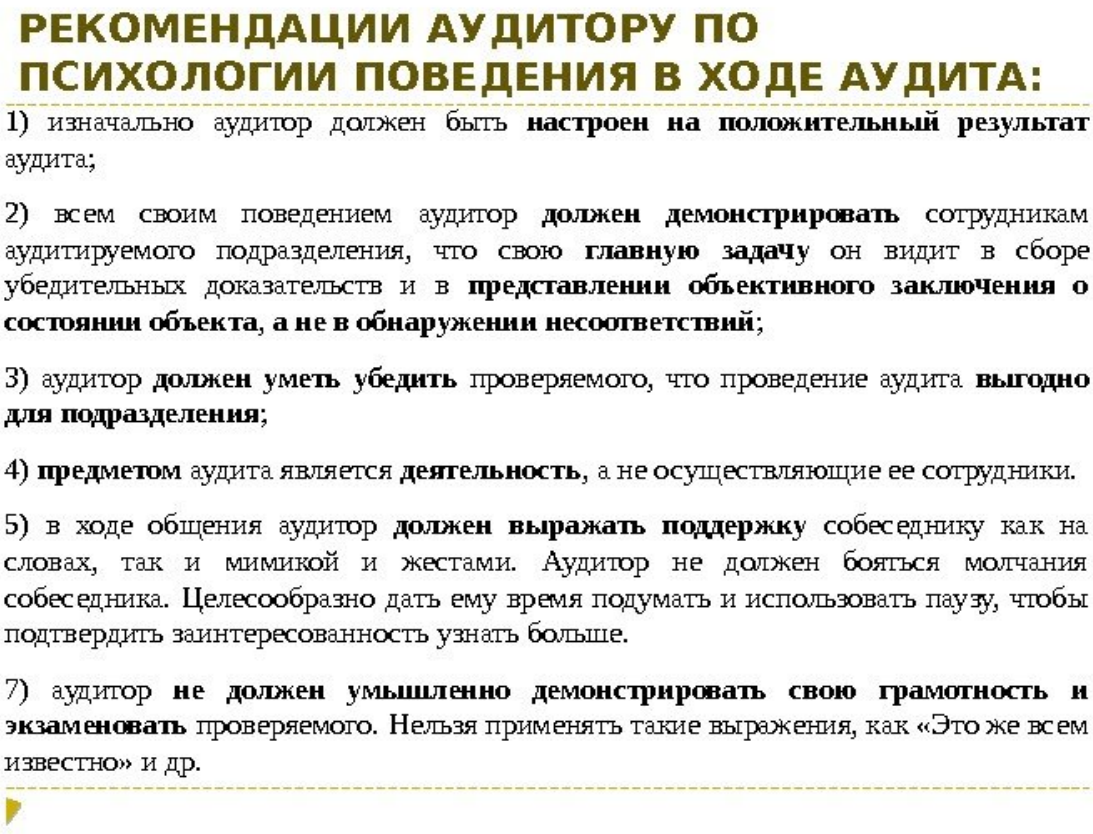


Рисунок 11 — Результаты аудита и рекомендации по повышению эффективности управления образовательным процессом

Выводы по 2 главе

Проведённое исследование позволило комплексно рассмотреть практическую реализацию методики проведения аудита в образовательной организации, выявить ключевые аспекты, влияющие на качество и эффективность учебного процесса, а также определить направления для совершенствования управленческих и технических механизмов.

Анализ нормативно-правовой базы и организационной документации продемонстрировал, что систематический и последовательный сбор материалов является необходимым условием для объективной оценки соответствия установленным стандартам и требованиям.

Выявление несоответствий в системе менеджмента качества показало, что ряд документов нуждается в актуализации, а некоторые внутренние регламенты требуют детальной проработки и чёткого оформления. Эти

пробелы отрицательно сказываются на управляемости образовательного учреждения и могут приводить к нарушениям нормативных требований, снижая эффективность контроля и координации процессов.

Оценка технических мер по защите информации выявила необходимость укрепления систем контроля доступа, повышения уровня безопасности сетевой инфраструктуры и регулярного обновления антивирусного программного обеспечения. Особое значение имеет организация резервного копирования и защита физической среды, что снижает риски утраты или компрометации данных.

Результаты аудита свидетельствуют о том, что только комплексный подход к информационной безопасности обеспечивает надежную защиту конфиденциальных данных и поддерживает стабильность учебного процесса.

Анализ компетентности педагогического и административного персонала продемонстрировал разнообразие в уровнях подготовки и владения современными образовательными технологиями. Этот фактор напрямую влияет на качество реализации учебных программ и выполнение управленческих функций. Выявленные пробелы в знаниях и навыках свидетельствуют о необходимости регулярного профессионального развития и повышения квалификации кадров.

Оценка мотивации учебной деятельности обучающихся выявила важность создания условий для формирования внутренних стимулов, развития личностно значимых целей и обеспечения поддержки со стороны педагогов. Уровень вовлечённости студентов тесно связан с эффективностью образовательного процесса и общем климатом в учебном коллективе.

Применение комплексных исследовательских методов обеспечило достоверность и полноту анализа, позволило выявить как формальные несоответствия, так и скрытые причины проблем.

Использование проблемного изложения в работе с результатами аудита позволило структурировать информацию, выделить приоритетные

направления для корректирующих действий и сформировать обоснованные рекомендации.

Разработанные рекомендации охватывают обновление нормативно-правовой документации, совершенствование технической защиты информации, развитие компетенций персонала и повышение мотивации обучающихся. Практическое внедрение данных мер должно сопровождаться поэтапным планированием, контролем и адаптацией к изменяющимся условиям, что обеспечивает устойчивое развитие образовательной организации.

Итогом исследования является понимание того, что системный и комплексный подход к аудиту, включающий различные аспекты деятельности образовательной организации, является эффективным инструментом повышения качества управления, безопасности и образовательного процесса в целом.

Кроме того, реализация предложенных рекомендаций способствует формированию устойчивой базы для дальнейшего совершенствования и адаптации учреждения к современным требованиям. В итоге это отражается на улучшении образовательных результатов и укреплении доверия со стороны обучающихся, их родителей и контролирующих органов.

ЗАКЛЮЧЕНИЕ

В настоящее время информация представляет собой весьма эффективный инструмент, с помощью которого имеется возможность воздействия на экономическую ситуацию. Успешность любого вида деятельности определяется наличием достоверной и защищенной информации. В условиях рыночной экономики наличие исключительных прав пользования той или иной информацией оказывает решающее значение в процессе борьбы за рынок.

В настоящее время существует большое число разнообразных методов защиты информации. С их помощью обеспечивается требуемый уровень безопасности и целостности баз данных. Применение тех или иных средств защиты информации определяется степенью подготовки нарушителей. Нарушения информационной безопасности имеет свою классификацию.

Они могут быть умышленными и неумышленными. В настоящее время средства защиты информационных сетей постоянно совершенствуются и развиваются. Это обусловлено тем, что информационные технологии характеризуются высоким темпом развития. На каждую новую разработку мошенников необходимо искать ответные меры тем, кто занимается разработкой систем защиты информации.

В связи с высокой скоростью появления различных инструментов для взлома систем защиты информации не всегда получается найти защитное средство защиты.

Это обусловлено следующими факторами:

– постоянное совершенствование и развитие элементной базы, разработка новых программ и приложений, с помощью которых может быть взломана система защиты информации, разработка инструментов взлома криптографических барьеров;

– постоянное усложнение сетевых архитектур, увеличение их быстродействия, рост количества клиентов сетей.

Современные условия предъявляют требования к организации процессов управлениям предприятиями различных организационных форм и видов деятельности на основы эффективных принципов, способных поддерживать предприятие на конкурентоспособном уровне.

Все разнообразие процессов, происходящих в ходе этого процесса, может быть представлено в виде набора социальных, технических, организационных и экономических проектов.

В процессе выполнения выпускной квалификационной работы получены следующие результаты:

– произведен анализ литературных источников по теме исследования;

– произведен анализ основных понятий информационной безопасности и базовых принципов ее обеспечения для образовательных организаций;

– проанализировано нормативно-правового обеспечения в области информационной безопасности;

— организация контентной фильтрации данных из Интернета на компьютерных устройствах используемых студентами;

— обеспечение антивирусной защиты и других Интернет-угроз компьютеров локальной сети организации;

— обеспечение защиты персональных данных субъектов образовательного процесса;

– произведен анализ угроз и уязвимостей базы исследования.

Рассмотрены вопросы разработки системы информационной безопасности образовательного учреждения, подготовки пакета внутренних нормативных документов и инструкций для функционирования системы информационной безопасности, выбора и организации работы контентной фильтрации, антивирусных программ на компьютерных устройствах сети колледжа, разработки системы защиты информационных ресурсов колледжа, проведение мероприятий с участием субъектов образовательного процесса для повышения уровня информационной безопасности.

Оценка мотивации учебной деятельности обучающихся выявила важность создания условий для формирования внутренних стимулов, развития личностно значимых целей и обеспечения поддержки со стороны педагогов. Уровень вовлечённости студентов тесно связан с эффективностью образовательного процесса и общем климатом в учебном коллективе.

Итогом исследования является понимание того, что системный и комплексный подход к аудиту, включающий различные аспекты деятельности образовательной организации, является эффективным инструментом повышения качества управления, безопасности и образовательного процесса в целом.

Кроме того, реализация предложенных рекомендаций способствует формированию устойчивой базы для дальнейшего совершенствования и адаптации колледжа к современным требованиям. В итоге это отражается на улучшении образовательных результатов и укреплении доверия со стороны обучающихся, их родителей и контролирующих органов.

По завершению выполнения работы необходимо отметить, что все поставленные задачи решены, цель научно-исследовательской работы достигнута.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Иванов С.П. Методика аудита в системе образования: теоретические основы и практические аспекты // Вестник педагогических наук. – 2018. – № 4. – С. 112–120.

2. Кузнецова Л.В. Организация внутреннего аудита в образовательных учреждениях // Управление образованием. – 2019. – № 2. – С. 45–52.

3. Петрова Е.М. Практические методы оценки качества образовательных процессов // Современное образование. – 2020. – № 7. – С. 68–74.

4. Сидоров А.Н. Процедуры аудита учебных заведений: анализ и внедрение // Журнал управления качеством. – 2021. – № 3. – С. 34–41.

5. Лукина Т.В. Инструменты аудита в образовательных организациях: кейс-стади // Вопросы образования и науки. – 2017. – № 6. – С. 97–103.

6. Фролова М.И. Роль аудита в повышении эффективности работы школы // Школьное образование. – 2019. – № 5. – С. 27–33.

7. Баранов Д.Г. Внедрение системного аудита в вузах: методические рекомендации // Высшее образование сегодня. – 2018. – № 1. – С. 59–65.

8. Никитина О.П. Практика проведения аудита деятельности образовательных учреждений // Современный менеджмент образования. – 2020. – № 4. – С. 85–92.

9. Морозова Н.С. Аналитические подходы к аудиту образовательных процессов // Педагогическое обозрение. – 2021. – № 8. – С. 114–121.

10. Егоров В.А. Стандарты и требования аудита в образовательных организациях // Качество образования. – 2017. – № 9. – С. 49–55.

11. Алферов, А. П. Основы теории баз данных : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин [и др.]. – 2-е изд., испр. и доп. – М.: Гелиос-АРВ, 2017. – 480 с.

12. Ахмад, Д. М., Дубравский, И. Защита от хакеров корпоративных сетей. 2017.

13. Бабенко, Л. К. Современные алгоритмы хеширования и методы их анализа: учебное пособие для студентов вузов, обучающихся по группе

специальностей в обл. информ. безопасности / Л. К. Бабенко, Е. А. Ищукова. – М.: Гелиос АРВ, 2018. – 376 с.

14. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России).

15. Белов, Е. Б. Основы информационной безопасности. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2019. – 544с.

16. Брассар, Ж. Современная криптология : [пер. с англ.] / Ж. Брассар. – М.: Полимед, 2018. – 176 с.

17. Бова, В. В. Основы проектирования информационных систем и технологий : учебное пособие / В. В. Бова, Ю. А. Кравченко ; Южный федеральный университет, Инженерно-технологическая академия. – Ростовна- Дону ; Таганрог : Южный федеральный университет, 2018. – 106 с.

18. Бэрмэн, С. Разработка правил информационной безопасности. 2016.

19. Вейцман, В. М. Проектирование информационных систем: Учебное пособие. – М.: МУБИНТ, 2018. – 214 с.

20. Вернер, М. Основы защиты информации : учебник для вузов : [пер. с нем.] / М. Вернер – М. : Техносфера, 2016. – 288 с.

21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Введ. 2006–12–27. // СПС Консультант Плюс (дата обращения: 18.03.2023).

22. Гохберг, Г. С. Информационные технологии: Учебник для студ. учрежд. сред. проф. образования / Г. С. Гохберг, А. В. Зафиевский, А. А. Короткин. – М.: ИЦ Академия, 2018. – 208 с.

23. Гудков, П. А. Защита от угроз информационной безопасности: учебное пособие / П. А. Гудков ; под ред. А. М. Бершадского. – Пенза : Издво Пенз. гос. ун-та, 2017. – 251 с.

24. Емельянова, Н. З. Проектирование информационных систем: Учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. – М.: Форум, 2018. – 432 с.

25. Коваленко, В. В. Проектирование информационных систем: Учебное пособие / В. В. Коваленко. – М.: Форум, 2018. – 976 с.

26. Кузнецов, С. Д., Основы баз данных / С. Д. Кузнецов. – М.: Бином. Лаборатория знаний, Интернет-университет информационных технологий, 2018. – 488 с.

27. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).

ПРИЛОЖЕНИЕ

«Регламент проведения аудита информационной безопасности в образовательной организации»

1. Общие положения

1.1. Настоящий регламент определяет порядок организации, проведения и документирования аудита информационной безопасности (ИБ) в образовательной организации.

1.2. Цель аудита — оценка текущего состояния ИБ, выявление уязвимостей и рисков, выработка рекомендаций по повышению защищённости информационных ресурсов.

1.3. Аудит проводится:

- планово — не реже 1 раза в год;
- внепланово — при инцидентах ИБ, существенных изменениях инфраструктуры или по решению руководства.

1.4. Ответственность за организацию аудита несёт заместитель директора по ИТ/информационной безопасности.

2. Этапы аудита

Этап 1. Подготовительный

2.1. Издание приказа о проведении аудита с указанием:

- сроков проведения;
- состава аудиторской группы;
- перечня проверяемых подразделений и систем.

2.2. Разработка плана аудита, включающего:

- цели и задачи;
- критерии оценки (стандарты ISO/IEC 27001, требования ФСТЭК, локальные регламенты);
- график мероприятий;
- методы проверки (анкетирование, интервью, сканирование, тестирование).

2.3. Информирование подразделений о предстоящем аудите.

Этап 2. Сбор информации

2.4. Анализ документации:

- политика ИБ;
- регламенты и инструкции по ИБ;
- договоры с подрядчиками;
- журналы регистрации инцидентов.

2.5. Инвентаризация ИТ-инфраструктуры:

- серверы, рабочие станции, сетевое оборудование;
- программное обеспечение (лицензионное/свободное);
- системы резервного копирования.

2.6. Опрос персонала:

- осведомлённость о правилах ИБ;
- практика работы с конфиденциальной информацией.

Этап 3. Техническая проверка

2.7. Сканирование на уязвимости:

- сетевые сервисы;
- веб-приложения;
- операционные системы.

2.8. Тестирование на проникновение (по согласованию).

2.9. Проверка настроек средств защиты:

- антивирусы;
- межсетевые экраны;
- системы обнаружения вторжений (IDS/IPS).

2.10. Анализ прав доступа к информационным ресурсам.

Этап 4. Анализ и оценка рисков

2.11. Классификация выявленных уязвимостей по уровню критичности (высокий/средний/низкий).

2.12. Оценка потенциальных угроз и сценариев реализации.

2.13. Расчёт рисков с учётом:

- вероятности реализации;
- возможного ущерба;
- существующих контрольных механизмов.

Этап 5. Формирование отчётности

2.14. Подготовка отчёта с разделами:

- краткое резюме;
- описание методологии;
- перечень выявленных уязвимостей;
- оценка рисков;
- рекомендации по устранению;
- план мероприятий с сроками и ответственными.

2.15. Презентация результатов руководству и ИТ-подразделению.

3. Роли и ответственности

3.1. Аудиторская группа (специалисты по ИБ, ИТ-аудиторы):

- проведение проверок;
- анализ данных;
- подготовка отчёта.

3.2. Ответственные подразделения (ИТ, администрация, библиотека и др.):

- предоставление документации;
- содействие в сборе данных;
- исполнение рекомендаций.

3.3. Руководство организации:

- утверждение плана и отчёта;
- выделение ресурсов на устранение уязвимостей.

4. Документирование

4.1. Обязательные документы:

- приказ о проведении аудита;
- план аудита;
- протоколы проверок;
- отчёт по результатам аудита;
- план корректирующих мероприятий.

4.2. Сроки хранения документов — не менее 3 лет.

5. Порядок устранения выявленных недостатков

5.1. В течение 10 рабочих дней после получения отчёта руководство утверждает план мероприятий.

5.2. Ответственные исполнители:

- разрабатывают детальные инструкции;
- реализуют меры в установленные сроки;
- отчитываются о выполнении.

5.3. Контроль исполнения — со стороны заместителя директора по ИТ/ИБ.

6. Заключительные положения

6.1. Регламент вступает в силу с даты утверждения директором организации.

6.2. Изменения в регламент вносятся приказом директора.

6.3. Все участники аудита обязаны соблюдать конфиденциальность полученной информации.

Чек-лист аудита информационной безопасности образовательной организации

Цель: систематическая проверка состояния ИБ по ключевым направлениям для выявления уязвимостей и соответствия нормативным требованиям.

Период проверки: _____

Аудиторская группа: _____

Объект аудита: _____

(подразделение/система/инфраструктура)

---

1. Нормативно-правовая база и документация

- Наличие актуальной **политики информационной безопасности** (да/нет, дата утверждения).
- Утверждённые **регламенты и инструкции** по ИБ (доступ, резервное копирование, инциденты и т. п.) (перечислить).
- **Договоры с подрядчиками** на обработку персональных данных (ПДн) — проверка наличия и условий.
- **Локальные акты** о защите ПДн обучающихся и сотрудников (да/нет).
- **Журналы регистрации инцидентов** ИБ за последний год (наличие, заполненность).

2. Управление доступом

- Регламентирован ли **порядок предоставления/изменения/отзыва прав доступа** (да/нет).

- Проведение **ревизии прав доступа** не реже 1 раза в 6 месяцев (да/нет, дата последней).
- Использование **многофакторной аутентификации** для критичных систем (да/нет).
- Ограничение доступа к ресурсам **по ролям** (преподаватели, студенты, техперсонал) (да/нет).
- Блокировка учётных записей уволенных сотрудников **в течение 1 рабочего дня** (да/нет).

3. Техническая защита инфраструктуры

- Установлены ли **антивирусные средства** на всех ПК и серверах (да/нет, вендор).
- Актуальность **баз антивирусов** (автоматическое обновление, да/нет).
- Наличие **межсетевого экрана** (firewall) с настроенными правилами (да/нет).
- Работа **системы обнаружения вторжений** (IDS/IPS) (да/нет).
- Резервное копирование данных:
    - регулярность (ежедневно/еженедельно/иное);
    - хранение копий вне площадки (да/нет); preparedness к восстановлению (тесты за последний год — да/нет).
- Защита Wi-Fi:
    - использование WPA2/WPA3 (да/нет);
    - раздельный доступ для сотрудников и гостей (да/нет).

4. Защита персональных данных (ПДн)

- Перечень информационных систем, обрабатывающих ПДн (актуальность, да/нет).
- Согласие на обработку ПДн обучающихся и сотрудников (наличие шаблонов, да/нет).
- Ограничение доступа к ПДн **только для уполномоченных лиц** (да/нет).
- Шифрование ПДн при передаче и хранении (да/нет, методы).
- Уничтожение носителей с ПДн (регламент, да/нет).

5. Обучение и осведомлённость персонала

- Проведение **инструктажей по ИБ** для новых сотрудников (да/нет, периодичность).
- Регулярное обучение персонала по темам: фишинг, парольная политика, инциденты (да/нет, график).
- Раздача памяток по ИБ (да/нет, актуальность).
- Тестирование знаний сотрудников (опросы/симуляции фишинга) — хотя бы 1 раз в год (да/нет).

6. Физическая безопасность

- Контроль доступа в серверные и помещения с критичным оборудованием (СКУД, охрана) (да/нет).
- Видеонаблюдение в зонах обработки конфиденциальной информации (да/нет).
- Уничтожение бумажных документов с ПДн (шредер, да/нет).

- Блокировка рабочих станций при отлучке сотрудника (политика, да/нет).

7. Управление инцидентами

- Утверждённый **регламент реагирования на инциденты** ИБ (да/нет).
- Канал оповещения об инцидентах (телефон, почта, чат) — известен ли персоналу (да/нет).
- Разбор инцидентов за последний год (количество, итоги) _____.
- Учения по реагированию на инциденты (хотя бы 1 раз в год, да/нет).

8. Внешние сервисы и аутсорсинг

- Проверка **договоров с облачными провайдерами** на соответствие требованиям ИБ (да/нет).
- Доступ третьих лиц к ИТ-инфраструктуре (регламентирован, да/нет).
- Аудит ИБ подрядчиков, работающих с ПДн (да/нет, периодичность).

9. Веб-ресурсы и онлайн-сервисы

- Наличие **сертификата SSL/TLS** на сайте организации (да/нет).
- Актуальность ПО сайта (CMS, плагины) — обновления в течение 14 дней после выхода (да/нет).
- Тестирование на уязвимости веб-приложений (хотя бы 1 раз в год, да/нет).

- Фильтрация контента для учащихся (да/нет, решение).

10. Мобильные устройства и BYOD

- Политика использования личных устройств (BYOD) для работы с корпоративными данными (да/нет).
- Мобильное управление (MDM) для корпоративных смартфонов/планшетов (да/нет).
- Шифрование данных на мобильных устройствах (да/нет).

Порядок работы с чек-листом

1. По каждому пункту укажите:
    - **Да** — требование выполнено.
    - **Нет** — требование не выполнено (обязательно поясните в графе «Комментарии»).
    - **Частично** — выполнено не в полном объёме (уточните в «Комментарии»).
2. В графе **«Комментарии»** укажите:
    - даты последних действий (например, «ревизия прав 15.03.2025»);
    - найденные недочёты;
    - предполагаемые сроки устранения.
3. По итогам заполнения сформируйте **перечень критических уязвимостей** и **план корректирующих мероприятий**.

Ответственный за аудит: _____ / _____

(ФИО) (подпись)

Дата заполнения: _____

Примечания: