

Научный руководитель:

Россова Ю.И.,

кандидат педагогических наук, доцент,

доцент кафедры «Дошкольного и начального образования»

АФ ННГУ им. Лобачевского

Россия, г. Арзамас

Автор:

Челышев А.М.,

студент,

2 курс, факультет «Дошкольного и начального образования»

АФ ННГУ им. Лобачевского

Россия, г. Арзамас

СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

***Аннотация:** Статья посвящена способам обеспечения информационной безопасности в образовательной организации. Рассмотрены вопросы разработки системы информационной безопасности образовательного учреждения, подготовки пакета внутренних нормативных документов и инструкций для функционирования системы информационной безопасности.*

***Ключевые слова:** Информационная безопасность, образовательная организация, образовательная среда, данные, угроза.*

***Annotation:** The article is devoted to the ways of ensuring information security in an educational organization. The issues of developing an information security system for an educational institution, preparing a package of internal*

regulations and instructions for the functioning of the information security system are considered.

Key words: *Information security, educational organization, educational environment, data, threat.*

В современном мире, где информационные технологии проникают во все сферы жизни, защита данных становится одной из приоритетных задач для образовательных организаций. В условиях стремительного роста числа киберугроз и утечек информации, важность обеспечения информационной безопасности в учебных заведениях не вызывает сомнений. Образовательные учреждения, являясь хранилищами личной и учебной информации, должны не только реагировать на возникающие угрозы, но и активно внедрять эффективные методики и технологии для их предотвращения.

В этом контексте исследование методик и технологий, направленных на защиту информации в образовательных учреждениях, становится особенно актуальным. Оно охватывает широкий спектр решений, включая программные и аппаратные средства, а также организационные меры, такие как обучение сотрудников и студентов основам информационной безопасности. Комплексный подход, включающий правовые аспекты и разработку внутренних регламентов, позволяет создать надежную защиту от несанкционированного доступа и утечек данных.

Это позволяет не только защитить информацию, но и создать безопасную образовательную среду, способствующую развитию цифровых компетенций у студентов и сотрудников.

Современное общество переживает эпоху цифровизации, когда информационные технологии становятся неотъемлемой частью всех аспектов жизни, включая образование. В условиях постоянного роста киберугроз и увеличения числа инцидентов, связанных с утечками данных, обеспечение информационной безопасности в образовательных организациях приобретает

критическую важность. Учебные заведения, хранящие личные данные учеников и сотрудников, а также образовательные материалы, должны не только реагировать на возникающие угрозы, но и активно внедрять стратегии и технологии для их предотвращения.

Исследование методов и технологий, направленных на защиту информации в образовательных учреждениях, становится особенно актуальным в свете этих вызовов. Оно охватывает разнообразные аспекты, включая программные и аппаратные решения, такие как обучение персонала и студентов основам информационной безопасности.

В конечном итоге, данное исследование направлено на формирование рекомендаций по внедрению комплексной системы безопасности, что является необходимым шагом для адаптации образовательных учреждений к вызовам цифровой эпохи.

В условиях стремительного развития цифровых технологий образовательные организации сталкиваются с необходимостью обеспечения информационной безопасности. В условиях стремительного развития цифровых технологий образовательные организации сталкиваются с необходимостью обеспечения информационной безопасности. Важность этой проблемы невозможно переоценивать, поскольку утечка данных может привести к серьезным последствиям как для учеников, так и для самого учебного заведения.

Одним из ключевых способов обеспечения информационной безопасности является внедрение комплексной системы защиты информации, которая включает в себя как технические, так и организационные меры. Технические меры могут включать использование современных программ, межсетевых экранов и систем обнаружения вторжений, которые помогают предотвратить несанкционированный доступ к данным.

Организационные меры, в свою очередь, предполагают разработку и внедрение политики безопасности, обучение сотрудников и учеников основам цифровой безопасности, а также регулярные проверки и аудит систем безопасности. Важно, чтобы все участники образовательного процесса осознали свою роль в обеспечении безопасности информации и знали, как действовать в случае инцидента.

Кроме того, стоит обратить внимание на необходимость защиты личных данных учеников. В соответствии с законодательством, образовательные организации обязаны обеспечивать конфиденциальность и безопасность таких данных. Это требует внедрения дополнительных мер, таких как шифрование информации и ограничение доступа к ней.

Таким образом, комплексный подход к обеспечению информационной безопасности в образовательных организациях включает в себя как технические, так и организационные меры, направленные на защиту данных и предотвращение угроз. Важно, чтобы эти меры были адаптированы к специфике каждого учебного заведения и постоянно обновлялись в соответствии с новыми вызовами в области информационной безопасности. В дополнение следует также рассмотреть важность создания культуры безопасности в образовательной среде. Это подразумевает не только обучение учеников и сотрудников основам информационной безопасности, но и формирование у них осознание важности защиты информации. Регулярные тренинги и семинары могут помочь повысить уровень осведомленности о потенциальных угрозах, таких как фишинг, вредоносное ПО и др.

Еще одним важным аспектом является сотрудничество с внешними экспертами и организациями в области информационной безопасности. Это может включать в себя консультации, совместные проекты и участие в конференциях, что позволит образовательным учреждениям быть в курсе последних тенденций и угроз в области информационной безопасности.

Партнерство с профессиональными компаниями также может обеспечить доступ к современным инструментам и технологиям защиты информации.

Также стоит упомянуть о необходимости соблюдения стандартов и норм в области информационной безопасности. Это может включать в себя как национальные, так и международные стандарты, которые помогут образовательным учреждениям выстраивать свою политику безопасности на основе лучших практик.

В заключение, обеспечение информационной безопасности в образовательных организациях требует комплексного подхода, который включает в себя как технические, так и организационные меры, а также активное участие всех участников образовательного процесса. Только так можно создать безопасную и защищенную среду для обучения и развития. Важным элементом стратегии обеспечения информационной безопасности является внедрение современных технологий защиты данных. Использование шифрование, двухфакторной аутентификации и систем обнаружения вторжений может значительно повысить уровень безопасности. Эти технологии помогают предотвратить несанкционированный доступ к конфиденциальной информации и защищают данные учеников и студентов.

Список литературы:

1. Петрова А.В. Проблемы информационной безопасности в образовательных учреждениях: вызовы и решения [Электронный ресурс] // Вестник образования. – 2023. – URL: <http://vestnik-obrazovaniya.ru/articles/2023-1> (дата обращения: 29.11.2025)
2. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. - М.: Академия, 2006
3. Кузнецов И.Н. Актуальные вопросы защиты информации в образовательных организациях [Электронный ресурс] // Научный журнал

«Информационные технологии». – 2022. – URL.- <http://it-journal.ru/articles/2022-3> (дата обращения: 29.11.2025)

4. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет. М., [Электронный ресурс] // 2004. URL: <http://www.ioso.ru/distant/library/publicationymfobez.htm> (дата обращения: 29.11.2025)