# **РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ: ПЕДАГОГИЧЕСКИЕ ОСНОВЫ ДЛЯ ЗАЩИТЫ ДАННЫХ**

**Т. И. Кочергина**,

*сотрудник* *ФСО России*

**Л. А. Кузнецова**,

*кандидат педагогических наук,*

*доцент кафедры профессионального обучения, бизнеса и технологии. ФГБОУ ВО "Орловский государственный университет имени И. С. Тургенева"*

*Аннотация.*

В современных реалиях нашего информационные технологии занимают центральное место в образовательном процессе. Учебные заведения активно используют электронные ресурсы, онлайн-курсы и цифровые платформы, что значительно обогащает образовательный опыт. Однако с развитием технологий возникает необходимость в обеспечении информационной безопасности. В этой статье рассмотрим, как информационная безопасность влияет на учебный процесс и какие методы можно применять для защиты данных.

*Ключевые слова:*

Уроки технологии, цифровая трансформация, цифровая среда, формирование навыков, информационная безопасность, правила безопасного поведения в интернете, социальная ответственность, освоение информационных технологий, педагогические методы и навыки.

**Введение.**

В эпоху цифровых технологий и интернет-пространства вопросы информационной безопасности стали неотъемлемой частью образовательного процесса. Обучающиеся, впервые сталкивающиеся с миром виртуальной информации, должны понять, насколько критично уметь защищать свои данные и личную информацию.

Информационная безопасность — это важный компонент образования в современном цифровом обществе. Для обучающихся это не просто набор правил, а целая культура, которая поможет им безопасно ориентироваться в мире информации, развивать критическое мышление, защищать свою личную жизнь и, возможно, строить карьеру в одной из самых актуальных областей. Понимание и внедрение принципов информационной безопасности становятся важной основой для формирования ответственных и информированных граждан.

1. Угрозы в цифровом мире

Современные студенты живут в мире, где данные стали одним из самых ценных ресурсов. Угрозы, такие как фишинг, вирусы, кибербуллинг и утечки личной информации, могут значительно повлиять на личную и академическую жизнь. Осознание этих угроз является первым шагом к формированию безопасного поведения в сети.

2. Развитие критического мышления

Обучение информационной безопасности помогает развивать у школьников критическое мышление. Они учатся анализировать информацию, различать надежные источники и выявлять потенциальные угрозы. Это важно не только для защиты данных, но и для формирования навыков, необходимых для успешной жизни в информационном обществе.

3. Защита личной информации

В условиях активного использования социальных сетей и цифровых платформ обучающиеся должны осознавать важность защиты своей личной информации. Применение основ информационной безопасности помогает им: создавать надежные пароли, управлять настройками конфиденциальности, понимать риски, связанные с публикацией личной информации в открытом доступе.

4. Подготовка к будущей карьере

Кибербезопасность — это не только актуальная область знаний, но и перспективная профессия. Обучение основам информационной безопасности позволяет учащимся задуматься о возможной карьере в этой сфере. Знания о защите данных могут стать конкурентным преимуществом на рынке труда.

5. Формирование ответственности и этики

Знания в области информационной безопасности формируют у обучающихся чувство ответственности за свои действия в сети. Они понимают, что их поступки могут иметь последствия не только для них, но и для окружающих. Этические аспекты использования информации становятся важной частью их образовательной программы.

Занятия проводимые при подготовке педагогического состава включают в себя:

1. Повышение осведомленности.

Первыми шагами на пути к безопасному обучению являются повышение осведомленности студентов и педагогов о возможных угрозах. Темы семинаров и уроков могут включать: основы кибербезопасности, опасности фишинга и советы по их предотвращению, важность создания надежных паролей и использования многофакторной аутентификации.

2. Интеграция программ по информационной безопасности в учебные курсы.

Разработка и включение специализированных курсов по информационной безопасности в учебные программы позволяет учащимся понять важность защитных мер. Эти курсы могут охватывать темы, такие как: защита личных данных, безопасная работа с мобильными устройствами, правила поведения в социальных сетях.

В современном мире существует ряд угроз информации, которые представляют собой действия или обстоятельства, которые могут привести к конфиденциальности, целостности или доступности данных. Основные категории угроз информации вытекают из нарушения основных постулатов информационной безопасности таких, как целостность, достоверность, доступность и конфиденциальность. Обобщенная таблица угроз информации представлена на рисунке 1.



Рис.1. Обобщенное представление угроз информации

Также можно рассмотреть некоторые основные методы защиты данных.

1. Шифрование

Шифрование данных является одним из основных методов защиты информации. Применение алгоритмов шифрования помогает защитить конфиденциальность данных студентов и преподавателей. Учебные заведения должны использовать шифрование для хранения и передачи личной информации.

2. Регулярное обновление программного обеспечения

Обновление программного обеспечения — важный аспект кибербезопасности. Учебные заведения должны обеспечивать регулярное обновление всех устройств и систем для защиты от уязвимостей, которые могут использовать злоумышленники.

3. Политика безопасности

Создание и внедрение политики информационной безопасности в учебных заведениях — необходимый шаг. Она должна включать правила доступа к данным, использование электронных ресурсов и меры по реагированию на инциденты.

4. Обучение персонала

Необходимо регулярное обучение преподавателей и административного персонала по вопросам информационной безопасности. Это поможет им быть в курсе последних тенденций и методов защиты данных.

5. Адаптация к новым технологиям

С каждым годом образовательные технологии продолжают эволюционировать. Использование искусственного интеллекта, больших данных и облачных вычислений требует непрерывного обновления подходов к информационной безопасности. Учебным заведениям следует: анализировать риски, связанные с новыми технологиями, внедрять адаптивные системы мониторинга, способные реагировать на новые угрозы в реальном времени.

6. Создание культуры безопасности

Формирование культуры безопасности в учебных заведениях — ключевой аспект обеспечения защиты данных. Это включает в себя: привитие ответственности за безопасность информации у студентов и сотрудников, стимулирование активного участия в мероприятиях по повышению безопасности, таких как конкурсы или хакатоны по кибербезопасности.

7. Сотрудничество с внешними экспертами

Работа с профессиональными организациями в области кибербезопасности может значительно повысить уровень защиты данных. Эти организации предлагают: проведение тренингов и семинаров для студентов и преподавателей, аудит текущих систем безопасности учебного заведения.

8. Использование безопасных платформ для дистанционного обучения

С переходом на дистанционное обучение важность выбора безопасных платформ для взаимодействия становится критически важной. Учебные заведения должны: оценивать платформы по стандартам безопасности, убедиться, что используются зашифрованные соединения и соблюдаются права пользователей.

 Рассмотрим несколько популярных программ и их сравнение.

1. CISSP (Certified Information Systems Security Professional)

Описание: Программа CISSP является одной из самых известных в области информационной безопасности. Она охватывает восемь доменов, таких как управление безопасностью, управление рисками, безопасность сетевой архитектуры и т.д.

Преимущества: признана во всем мире, широкий спектр знаний и навыков, подходит для управленцев и специалистов с опытом.

Недостатки:

Требует значительных затрат времени (не менее 35 часов на подготовку).

Для получения сертификата необходим опыт работы в области безопасности.

2. CompTIA Security+

Описание: Это базовый курс, охватывающий ключевые концепции кибербезопасности, подобные сетевой безопасности, угрозам и уязвимостям, а также управлению безопасностью.

Преимущества: доступен для новичков в области ИБ, поиск работы после сертификата легче, так как он признается работодателями, подходит для индивидуального изучения.

Недостатки:

Менее глубокая программа по сравнению с CISSP.

Нацелен на общее понимание, а не на специализированные навыки.

3. Certified Ethical Hacker (CEH)

Описание: Программа CEH фокусируется на методах взлома и тестировании на проникновение, обучая студентов этичным способам выявления уязвимостей.

Преимущества: практическое уклонение на тестирование систем, высокий уровень востребованности среди работодателей.

Недостатки:

Требует предварительных знаний в области информационных технологий. Может потребовать дополнительных курсов для более глубокого понимания.

4. (ISC)² SSCP (Systems Security Certified Practitioner)

Описание: Эта программа предназначена для тех, кто хочет начать карьеру в информационной безопасности и содержит ключевые концепты, такие как контроль доступа, оценка рисков и защита данных.

Преимущества: подходит для начинающих специалистов, фокусируется на практическом применении знаний.

Недостатки:

Не так широко известна, как CISSP. Меньшая глубина охвата по сравнению с более специализированными программами.

Существуют различные методики обучения школьников информационной безопасности на уроках технологии, которые должны быть интерактивным и основанным на реальных сценариях. Ниже представлены несколько эффективных методик, которые могут быть использованы для обучения этой важной теме.

1. Игровые методики

Использование игр — один из наиболее эффективных способов обучения. Примеры включают:

Киберигры: Создание мини-игр, где ученики могут защищать виртуальные объекты от кибератак или выполнять задания, касающиеся безопасности данных.

2. Проектное обучение

Проектная методика позволяет учащимся исследовать конкретные вопросы информационной безопасности, работая над реальными проектами:

Создание презентаций или видеороликов по темам, таким как создание надежных паролей или распознавание фишинга.

Разработка собственных проектов по защите данных, где ученики могут предложить решения для улучшения безопасности в школе.

3. Мастер-классы и практические занятия

Практические занятия помогают учащимся получить конкретные навыки:

Практикумы по созданию и управлению безопасными паролями, настройке двухфакторной аутентификации и использованию антивирусного ПО. Мастер-классы по использованию программ для шифрования данных или виртуальных частных сетей (VPN).

4. Сценарные задания и кейс-стадии

Использование сценарных заданий позволяет ученикам развивать аналитические навыки:

Разбор реальных инцидентов кибербезопасности с последующим обсуждением, как можно было бы избежать этих ситуаций.

Создание групповых проектов, где учащиеся должны оценить риски и предложить меры безопасности на примере вымышленной организации.

5. Обучение через сотрудничество

Работа в группах помогает развивать навыки взаимодействия и ответственности:

Создание команд для решения задач по кибербезопасности, где каждый член имеет свои обязанности.

Проведение обсуждений в малых группах о важности безопасного поведения в сети, а также о возможных последствиях неосторожных действий.

6. Интеграция лекций и семинаров

Сочетание теории и практики:

Проведение лекций по основам кибербезопасности, после которых следуют практические занятия с использованием реальных примеров.

Приглашение специалистов в области информационной безопасности для проведения семинаров или вебинаров.

### Заключение

Информационная безопасность не должна рассматриваться как дополнительная опция в образовательном процессе — это основа, на которой можно строить доверительную и безопасную среду обучения. Методики обучения информационной безопасности школьников на уроках технологии должны сочетать элементы теории и практики. Обучение информационной безопасности имеет важное значение для защиты данных и систем. Выбор программы зависит от уровня подготовки учащегося и конкретных целей. Каждая программа предлагает уникальные преимущества и недостатки, что позволяет подобрать подходящий курс в зависимости от требований и интересов учащихся.

**Литература**

*Статьи из журналов и периодических изданий*

1. Бутенко, И. А. (2022). Основы информационной безопасности: учебное пособие для школьников. – Москва: Издательство «Научная книга». – 21-24 с.
2. Герасимова, Н. В. (2021). Кибербезопасность: вызовы и решения для образовательных учреждений. – Санкт-Петербург: Питер.
3. Кравченко, А. С. (2019). Информационная безопасность в школе: методические рекомендации. – Киев: Киевский университет.

*Книги, монографии*

1. Монахов, С. В. (2018). Обучение информационной безопасности: практическое руководство для педагогов. – Екатеринбург: Уральское издательство.
2. Петров, А. И. (2022). Информационная безопасность: как защитить себя в цифровом мире. – Новосибирск: Сибирское издательство.
3. Романов, Д. А. (2021). Современные технологии защиты информации в образовательных учреждениях. – Ростов-на-Дону: ЮФУ.