

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ. КИБЕРБЕЗОПАСНОСТЬ**Машарипова Нодира Нуржановна***Хорезимская область, город Ургенч,**средняя школа № 15*

Аннотация: В данной статье рассматриваются ключевые аспекты безопасности в сети Интернет и актуальные вопросы кибербезопасности. Уделено внимание основным угрозам, с которыми сталкиваются пользователи в цифровом пространстве, таким как вирусные атаки, фишинг, утечка данных и несанкционированный доступ. Также обсуждаются современные методы защиты, включая использование антивирусного программного обеспечения, двухфакторной аутентификации, шифрования данных и повышения уровня осведомленности пользователей. Особое внимание уделено важности формирования цифровой культуры и соблюдения этических норм в киберпространстве. Предлагаемые рекомендации направлены на минимизацию рисков и создание безопасной среды для работы и общения в Интернете.

Ключевые слова: интернет-безопасность, кибербезопасность, защита данных, фишинг, антивирус, цифровая культура.

В современном мире интернет стал неотъемлемой частью жизни каждого человека. Мы используем его для работы, общения, получения информации, совершения покупок и развлечений. Однако вместе с развитием технологий возрастает и количество угроз, связанных с использованием интернета. Кибербезопасность становится одной из важнейших проблем современного общества, требующей повышенного внимания как от пользователей, так и от организаций.

Интернет предоставляет огромные возможности, но он также является пространством, где каждый может столкнуться с киберпреступностью. Фишинг, вирусы, кража данных, взломы аккаунтов — все это примеры угроз, с которыми мы можем столкнуться в цифровой среде. Нередко даже самые продвинутые пользователи становятся жертвами злоумышленников, поскольку киберпреступники используют всё более изощренные методы.

Одной из главных причин уязвимости пользователей является недостаточная осведомленность о рисках. Многие не уделяют должного внимания защите своих данных: создают слабые пароли, передают конфиденциальную информацию в ненадежных сетях или игнорируют обновления программного обеспечения. Эти, казалось бы, мелкие ошибки могут привести к серьезным последствиям, таким как утечка личной информации или финансовые потери.

Основные угрозы в интернете:**1. Вирусные атаки и вредоносные программы**

Вредоносные программы могут нанести ущерб устройствам пользователей, похищать данные и блокировать доступ к системам.

2. Фишинг

Кибермошенники используют социальные инженерные методы, чтобы обманом получить конфиденциальную информацию, такую как пароли и данные банковских карт.

3. Утечка данных

Часто возникают инциденты, связанные с нарушением конфиденциальности данных из-за взломов или недостаточных мер защиты.

4. Несанкционированный доступ

Хакеры могут получить доступ к системам без разрешения, что приводит к утрате контроля и значительным убыткам[1]

Кибербезопасность — это не только технические меры, но и культура ответственного поведения в интернете. Каждый пользователь должен соблюдать базовые правила безопасности: использовать антивирусные программы, избегать подозрительных ссылок, регулярно обновлять устройства и приложения, а также проверять надежность сайтов перед вводом личных данных.

На уровне организаций и государства кибербезопасность также играет ключевую роль. Компании обязаны защищать данные своих клиентов и сотрудников, а также обучать их основам информационной безопасности. Государства, в свою очередь, должны разрабатывать и внедрять законодательные меры для предотвращения киберпреступлений, а также создавать условия для международного сотрудничества в этой сфере.

Интернет предоставляет нам безграничные возможности, но с ними приходит и ответственность. Безопасность в сети — это не только защита от угроз, но и осознанное использование технологий. Каждый из нас может внести свой вклад в создание более безопасного цифрового пространства, следуя простым, но важным правилам. Лишь совместными усилиями мы сможем минимизировать риски и обеспечить комфортное и безопасное пребывание в интернете.

Интернет — это неотъемлемая часть нашей жизни, и от нас зависит, насколько безопасным будет его использование. Кибербезопасность требует постоянного внимания, обучения и адаптации к новым вызовам. Соблюдение правил, повышение грамотности пользователей и сотрудничество на всех уровнях — ключевые аспекты, которые помогут защитить нас и наше цифровое пространство.

Одной из основных причин уязвимости является недостаточная киберграмотность пользователей. Многие люди не уделяют должного внимания защите своих устройств и данных, используя слабые пароли, переходя по подозрительным ссылкам или передавая конфиденциальную информацию через незащищенные каналы связи. Такие ошибки часто приводят к утечке личной информации, финансовым потерям и другим неприятным последствиям.

Кибербезопасность начинается с базовых правил:

1. **Использование надежных паролей.** Пароли должны быть сложными, содержать комбинации букв, цифр и специальных символов.

2. **Обновление программного обеспечения.** Регулярное обновление приложений и операционной системы помогает защитить устройства от уязвимостей.

3. **Установка антивирусных программ.** Антивирусы и фаерволы служат дополнительным барьером от вредоносных атак.

4. **Осознанное поведение в интернете.** Избегайте переходов по подозрительным ссылкам, не открывайте подозрительные вложения и не вводите личные данные на незнакомых сайтах[2].

Однако кибербезопасность — это не только ответственность пользователей. Организации и государственные структуры также играют важную роль в создании безопасной цифровой среды. Компании должны внедрять современные системы защиты данных, проводить обучение сотрудников основам информационной безопасности и обеспечивать надежность своих сервисов. Государства, в свою очередь, должны разрабатывать законодательство, направленное на предотвращение киберпреступлений, а также сотрудничать с другими странами для борьбы с угрозами глобального масштаба.

Кроме того, важно развивать киберграмотность населения. Школы, университеты и другие образовательные учреждения должны обучать основам безопасного поведения в интернете. Подобные знания помогут не только защитить себя, но и сформировать культуру осознанного использования цифровых технологий.

Кибербезопасность — это вызов современности, требующий совместных усилий всех участников цифрового пространства. Следуя простым правилам, повышая осведомленность и принимая меры предосторожности, мы можем значительно снизить риски и создать более безопасное интернет-пространство. Интернет — это мощный инструмент, и его использование должно быть не только удобным, но и безопасным.

REFERENCES:

1. Акбаров Д.Э. Обеспечение информационной безопасности криптографические методы и их применение // Ташкент, 2008, -Б. - 394.
2. Ганиев С.К., Каримов М.М., Худойкулов З.Т., Кадыров М.М.. Термины и понятия информационной безопасности на русском, узбекском и английском языках. толковый словарь языков // Ташкент 2017,-Б. - 480.
3. Фергюсон Н., Шнайер Б. Практическая криптография // Нью-Йорк: Wiley, 2003. – С. – 432.