ISSN 3060-4567

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА: ЦИФРОВАЯ КУЛЬТУРА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УЗБЕКИСТАНЕ

Муминова Муслимахон Маъсуджон кизи
Студентка 1 курса факультета иностранных языков
Ферганского государственного университета
Научный руководитель: ***Мирзаакбаров Дильшодбек Давлатбоевич***
Старший преподаватель кафедры информационных технологий
Ферганского государственного университета

Аннотация: *В данной статье рассматриваются вопросы безопасного использования интернета, цифровой культуры и обеспечения информационной безопасности в Узбекистане. С распространением интернета и развитием информационных технологий проблемы кибербезопасности стали актуальными. В статье анализируются основные интернет-угрозы, киберпреступления, вредоносные программы и фишинговые атаки. Также подчеркивается необходимость развития цифровой культуры и обучения пользователей основам информационной безопасности. Обсуждаются основные методы безопасного поведения в сети, а также будущие стратегии кибербезопасности в Узбекистане. Статья акцентирует внимание на инициативах и мерах, предпринимаемых для повышения уровня информационной безопасности и развития цифровой культуры.*

Ключевые слова: *интернет-безопасность, кибербезопасность, информационная безопасность, цифровая культура, фишинг, вредоносные программы, киберпреступления, информационные технологии, антивирусные программы, цифровая экономика.*

Сегодня интернет стал неотъемлемой частью нашей жизни и необходимым инструментом для деятельности в различных сферах. Интернет

ISSN 3060-4567

открыл перед нами широкие возможности для обучения, ведения бизнеса, торговли, общения и обмена информацией. Однако с увеличением использования интернета в Узбекистане, вопросы кибербезопасности приобрели особую актуальность. Помимо огромных плюсов, интернет также приносит с собой риски, которые могут сильно повлиять на безопасность как отдельных пользователей, так и целых организаций. Особенно это касается таких угроз, как киберпреступления, вредоносное программное обеспечение, фишинг, кража личных данных и атаки на интернет-ресурсы.

Ситуация в сфере киберугроз становится более сложной, с каждым годом количество инцидентов в области информационной безопасности увеличивается. Поэтому эффективное использование интернета, развитие цифровой грамотности и обеспечение информационной безопасности стали неотъемлемой частью общественной жизни. В этой статье рассматриваются основные проблемы интернет-безопасности, текущее состояние информационной безопасности в Узбекистане и важные достижения в сфере цифровой культуры.

Основные угрозы интернет-безопасности

Угрозы, возникающие при использовании интернета, многочисленны и разнообразны. Самые распространённые из них следующие:

- *Киберпреступления* — это действия, направленные на взлом компьютерных систем, кражу данных, манипуляцию информацией или нанесение финансового ущерба пользователям. Киберпреступники часто нацелены на получение личных данных, мошенничество, кражу банковских реквизитов. В последнее время такие преступления становятся всё более изощрёнными и трудноуловимыми.

Пример: в 2020 году в Узбекистане были зафиксированы кибератаки на банковские системы, в результате которых было украдено несколько миллионов сумов, а также произошло массовая утечка личных данных пользователей.

- *Вредоносное программное обеспечение (Malware)* — это программы, созданные с целью разрушения или повреждения системы, кражи информации

ISSN 3060-4567

или получения несанкционированного доступа к устройствам. Вредоносные программы могут попасть на компьютер или мобильное устройство разными способами, что влияет на стабильность работы системы и может привести к утечке конфиденциальных данных.

Пример: в 2017 году вирус WannaCry поразил сотни тысяч систем по всему миру, нанеся ущерб как частным пользователям, так и целым организациям, включая медицинские учреждения, которые стали жертвами атаки.

- *Фишинг* — это метод обмана, при котором мошенники пытаются получить доступ к личным данным пользователя через поддельные электронные письма или сайты, которые имитируют надежные источники. Этот метод остается одним из самых популярных среди киберпреступников, поскольку его относительно легко осуществить.

Пример: в 2019 году в Узбекистане была зафиксирована кража данных банковских карт через поддельные сайты и объявления, что привело к значительным финансовым потерям для граждан.

- *DDoS-атаки (Distributed Denial of Service)* — это атаки, в ходе которых серверы интернет-ресурсов или веб-сайтов перегружаются большим количеством запросов, что приводит к их сбоям и временному отключению. Подобные атаки обычно нацелены на определённые организации или конкурентов с целью вывести их онлайн-ресурсы из строя.

Пример: в 2020 году в Узбекистане несколько интернет-сервисов подверглись DDoS-атакам, что привело к сбоям в их работе и нарушению предоставления услуг для пользователей.

Состояние информационной безопасности в Узбекистане

С развитием технологий и расширением цифровых услуг в Узбекистане информационная безопасность становится особенно важным вопросом. Для того чтобы обеспечить безопасность работы в интернете, в стране принимаются различные меры, как на уровне государства, так и на уровне частных организаций:

- *Законодательство*: Важным шагом в направлении обеспечения безопасности стало принятие Закона «Об информационной безопасности в 2018 году. Этот нормативный акт направлен на защиту информационных систем и предотвращение киберугроз в стране.
- *UZCERT (Компьютерная команда реагирования на инциденты)* — это организация, которая занимается мониторингом и анализом состояния сетевой безопасности, предупреждением угроз и устранением инцидентов в сфере кибербезопасности. Она активно сотрудничает как на национальном, так и на международном уровнях для повышения уровня защиты информационных систем.
- *Служба государственной безопасности* — эта структура реализует государственную политику в области информационной безопасности, а также занимается выявлением и нейтрализацией киберугроз. Помимо этого, она разрабатывает меры по защите важных государственных и коммерческих информационных систем.

Роль цифровой культуры и образовательных инициатив

Интернет-безопасность зависит не только от технических решений, но и от уровня цифровой грамотности населения. Формирование цифровой культуры и обеспечение должного уровня образования в области информационной безопасности являются важнейшими аспектами защиты граждан в цифровом пространстве.

- *Цифровая культура* — это понимание основ безопасного поведения в интернете, уважение к нормам цифрового этикета, а также защита личных данных от неправомерного использования. В Озбекистане в образовательных учреждениях внедряются новые подходы к развитию цифровой культуры среди школьников и студентов, включая аспекты безопасности в интернете и психологическую подготовку.
- *Образование в области информационной безопасности* — во многих школах и вузах страны уже проводят уроки, направленные на обучение безопасному использованию интернета и защите личной информации. Это

ISSN 3060-4567

необходимая составляющая для формирования осведомленности среди молодежи о важности безопасности в цифровом мире.

Основные методы безопасного использования интернета

Для безопасного поведения в интернете необходимо соблюдать как технические, так и поведенческие меры предосторожности:

- *Использование надежных паролей и двухфакторной аутентификации (2FA):* пароли должны быть достаточно сложными (не менее 8 символов, включающих буквы, цифры и специальные символы). Двухфакторная аутентификация обеспечивает дополнительный уровень безопасности, что значительно снижает вероятность несанкционированного доступа к личным данным.
- *Антивирусные программы и брандмауэры:* регулярное обновление антивирусного ПО и использование межсетевых экранов (фаерволов) помогают защитить устройства от вредоносных программ и вирусов.
- *Осторожность с подозрительными ссылками:* следует избегать переходов по сомнительным ссылкам и использовать только проверенные источники информации. Это поможет предотвратить фишинговые атаки и другие формы мошенничества.

Будущие стратегии кибербезопасности Узбекистана

В рамках цифровой трансформации и развития электронного правительства Узбекистан продолжает внедрять новые подходы в сфере кибербезопасности:

- *5G сети и новые киберугрозы:* с внедрением технологий 5G открываются новые возможности для повышения скорости передачи данных, но одновременно это создает новые угрозы для защиты данных и инфраструктуры. Необходимы дополнительные меры безопасности для защиты высокоскоростных сетей от атак.
- *Блокчейн-технологии:* использование блокчейн-технологий может значительно повысить уровень защиты информации, так как эта технология

обеспечивает прозрачность и безопасность транзакций. Развитие блокчейн-технологий в Узбекистане набирает популярность и представляет собой важный шаг в укреплении информационной безопасности.

Заключение

Безопасное использование интернета — это ответственность каждого пользователя. Усилия государства, образовательных учреждений и частного сектора в области цифровой безопасности и повышения цифровой грамотности имеют ключевое значение для создания безопасной цифровой среды. Совместная работа всех заинтересованных сторон позволит значительно повысить уровень защиты и минимизировать риски, связанные с киберугрозами.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Хасанова Д.Ш. Формирование цифровой культуры у молодежи: проблемы и перспективы. – Научно-практический журнал «Информационное общество», 2023.

2. https://www.mass.gov/info-details/know-the-types-of-cyber-threats

3.https://cwgsecurity.uz/xakerlar-foydalanadigan-usullar-kiber-tahdidlar-turlari/

4. Закон Республики Узбекистан «Об информационной безопасности» №ЗРУ–482 от 11.12.2018 года.

5. https://www.kaspersky.ru/resource-center/threats/types-of-malware