ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ СТАБИЛЬНОСТИ: УКРЕПЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ В УЗБЕКИСТАНЕ НА ОСНОВЕ ПРАКТИКИ РАЗВИТЫХ СТРАН

Олия Шералиевна КУВАТОВА
старший преподаватель
Ташкентский государственный экономический университет
Ташкент, Узбекистан

Мухриддин Бахриддинович ХУСЕНОВ
студент
Ташкентский государственный экономический университет
Ташкент, Узбекистан

Аннотация

В рамках данной статьи рассматриваются актуальные вызовы в сфере киберугроз, а также анализируются подходы развитых стран к формированию систем кибербезопасности. Полученные результаты показывают необходимость адаптации лучших зарубежных практик с учетом национальных реалий. В дальнейшем предполагается разработка конкретных рекомендаций и стратегий, ориентированных на долгосрочную цифровую безопасность страны.

Ключевые слова: кибербезопасность, национальная безопасность, цифровые технологии, экономика Узбекистана, международный опыт, устойчивое развитие.

Ривожланган мамлакатлар тажрибаси орқали Ўзбекистонда иқтисодий барқарорликни таъминлашда киберхавфсизликнинг аҳамияти

Олия Шералиевна КУВАТОВА
катта ўқитувчи
Тошкент давлат иқтисодиёт университети
Тошкент, Ўзбекистон

Мухриддин Бахриддинович ҲУСЕНОВ
талаба
Тошкент давлат иқтисодиёт университети
Тошкент, Ўзбекистон

Аннотация

Ушбу мақолада кибертаҳдидлар соҳасидаги долзарб муаммолар кўриб чиқилади ва ривожланган мамлакатларнинг киберхавфсизлик тизимларини шакллантиришга ёндашувлари таҳлил қилинади. Олинган натижалар миллий воқеликни ҳисобга олган ҳолда илғор хорижий тажрибани мослаштириш зарурлигини кўрсатади. Келгусида мамлакатнинг узоқ муддатли рақамли

хавфсизлигига қаратилган аниқ тавсиялар ва стратегиялар ишлаб чиқилиши кутилмоқда.

Таянч сўзлар: киберхавфсизлик, миллий хавфсизлик, рақамли технологиялар, Ўзбекистон иқтисодиёти, халқаро тажриба, барқарор ривожланиш.

В XXI веке, стремительно развивающемся в направлении цифровых технологий, кибербезопасность превратилась в одну из ключевых проблем не только для отдельных стран, но и для каждого человека. Человечество, стремясь упростить свою жизнь с помощью современных технологий, одновременно сталкивается с ростом новых видов угроз, сопровождающих эти удобства. Масштабные кражи данных, ущерб, наносимый цифровой инфраструктуре, а также мелкие кибератаки, происходящие по всему миру, заставляют нас постоянно сохранять бдительность и предпринимать своевременные меры в сфере кибербезопасности.

Сегодня обеспечение экономической стабильности государства напрямую связано с уровнем кибербезопасности. Как известно, экономическая инфраструктура как развитых, так и развивающихся стран все чаще опирается на цифровые системы для финансовых операций, торговых связей и ключевых сервисов. Даже незначительные атаки на эти системы могут вызвать серьезные проблемы – от подрыва доверия потребителей до угрозы общей экономической нестабильности. Именно поэтому кибербезопасность играет важную роль в обеспечении устойчивости и процветания страны.

Наряду с другими государствами, Узбекистан активно внедряет цифровую трансформацию. Согласно Указу Президента Республики Узбекистан от 5 октября 2020 года №УП-6079, в стране определены стратегии активного развития цифровой экономики, ее интеграции во все сферы – начиная с государственного управления и заканчивая образованием, здравоохранением и сельским хозяйством [1]. Однако с расширением цифровой инфраструктуры закономерно возрастает и уровень киберугроз. Несмотря на то, что в соответствии с Постановлением Президента

Республики Узбекистан от 15 июня 2020 года №ПП-4751 «О мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан» [2] в стране уже предпринимаются определенные шаги, необходимо разрабатывать новые меры по укреплению кибербезопасности. Это особенно важно в условиях растущей сложности киберугроз, ведь для обеспечения безопасности населения, национальной стабильности и экономической устойчивости Узбекистану следует создать прочную киберзащиту.

Кибербезопасность – относительно новый термин, которому в разные периоды давались различные определения. Она также классифицируется по степени угрозы и потенциальному ущербу. В частности, Walls (2013) первоначально определил кибербезопасность как защиту IT-технологий и опирающихся на них систем [3]. Позднее Brazilay (2013) дополнил это определение, отметив, что кибербезопасность – это не только защита, но и способность противостоять потенциальным рискам [4].

В своих исследованиях Böhme (2019) подробно проанализировал влияние киберугроз на домохозяйства, малый бизнес и национальную экономику – от финансовых потерь и сбоев в деятельности до ущерба для репутации и цепной реакции на рынке [5].

На международном форуме «Цифровая безопасность», проведенном Организацией экономического сотрудничества и развития (ОЭСР) в 2021 году, был представлен обобщенный опыт развитых стран в области кибербезопасности. Были предложены общие стратегии, направленные на развитие инноваций в государственных структурах и укрепление человеческого капитала [6]. Кроме того, с выходом технологий искусственного интеллекта на новый уровень, на глобальном форуме ОЭСР «Цифровая безопасность – путь к процветанию 2024», состоявшемся в 2023 году, вопросы кибербезопасности были признаны одними из наиболее актуальных [7].

В данной статье представлены ключевые понятия и аналитические данные о значении кибербезопасности в эпоху цифровых технологий, а также ее роли в обеспечении экономической стабильности государства. В процессе анализа в основном использовались статистические данные. В дополнение к этому применялись эмпирические методы: рассмотрен опыт развитых стран, на основе которого сделаны соответствующие выводы.

Для того чтобы глубже понять среду кибербезопасности, необходимо разобраться в масштабах угроз, их разновидностях и динамике. Киберугрозы охватывают широкий спектр – от заражения вредоносными программами до взлома платежных систем, фишинговых атак и сложных хакерских вмешательств. Эти угрозы год за годом видоизменяются, усложняются и требуют своевременного реагирования. Умение классифицировать и различать типы кибератак становится важным элементом эффективной защиты.

Кибератака – это преднамеренное вмешательство, направленное на нарушение конфиденциальности, целостности или доступности информации в компьютере, системе, веб-сайте или личных устройствах. Цели кибератак могут включать следующее:

- получение несанкционированного доступа к устройствам и завладение содержащейся в них информацией;
- полный вывод из строя систем, нанесение серьезного ущерба, включая полную остановку работы сайтов;
- незаконные действия от имени другого пользователя путем взлома его устройства;
- заражение корпоративных сетей вирусами и вредоносным кодом с целью дестабилизации всей системы;
- попытка доступа к системе без разрешения руководства, изменение или уничтожение данных, изменение внешнего вида интерфейса системы.

1-Таблица.

Виды кибератак и их методология

Тип киберугрозы	Мелкие атаки	Кража данных	Киберпрес тупления	Хакерские действия	Масштабные атаки
Цель	Создать угрозу, временно нарушить работу	Экономическая и политическая выгода	Финансовая выгода	Ущерб репутации, политические цели	Парализация всей деятельности
Пример	Спам-боты, DDoS	Целенаправлен ные организованные атаки	Кража с банковских карт и счетов	Отключение веб-сайтов	Кража или полное уничтожение данных
Характер	Автоматиз ированный	Постоянный, спланированный	Частый, создаёт ситуации	Спланированны й	Критические ситуации
Целенапра вленность	✕	☑	☑	☑	☑

Это в основном автоматизированные атаки, при которых с помощью бот-сетей к системе отправляется непрерывный поток запросов, чтобы временно вывести ее из строя. Одним из самых распространенных примеров является DDoS-атака. В таких случаях сервер перегружается и перестает работать корректно до тех пор, пока специалисты не устранят угрозу. На это время пользователи испытывают затруднения в доступе к системе.

Кража данных. Данный вид атак направлен на незаконное получение личной информации граждан, финансовых отчетов компаний и другой критически важной информации. Это уже квалифицируется как организованная киберпреступность, осуществляемая целенаправленно. В отличие от простых атак, злоумышленники используют как внутренние, так и внешние уязвимости системы для обхода ее защитных механизмов.

Киберпреступления сегодня являются одной из самых распространенных форм атак, жертвами которых может стать абсолютно любой человек. Этот вид преступной деятельности зачастую выглядит довольно простым, а жертвы становятся уязвимыми из-за низкой цифровой грамотности. Преступники используют электронную почту, SMS-сообщения, телефонные звонки, мессенджеры и социальные сети, рассылая сообщения со зловредными ссылками. Основная цель таких атак – получить доступ к личным данным пользователей и завладеть денежными средствами с их

банковских счетов. В случае, если жертва использует устройство, принадлежащее какому-либо учреждению, это может повлечь за собой более серьезные последствия уже для самой организации.

Хакерские атаки – это менее распространенная, но хорошо спланированная и потенциально крайне разрушительная угроза. Чаще всего они совершаются анонимными группами с целью нанести удар по репутации известных брендов или государственных организаций.

Масштабные кибератаки зачастую имеют политическую мотивацию и осуществляются в крупных объемах. Ярким примером могут служить кибератаки, организованные хакерскими группами двух стран в ходе войны между Россией и Украиной, начавшейся в 2022 году, направленные против государственных инфраструктур [8], [9].

По данным Всемирного экономического форума (WEF), в 2023 году число киберпреступлений в мире значительно возросло, а общий ущерб от них составил 11 триллионов долларов США. В публикации также подчеркивается, что эта цифра будет расти, и к 2027 году может достичь 27 триллионов долларов США. [10]

Ниже приведены наиболее крупные хакерские атаки 2023 года, приведшие к значительным финансовым потерям:

В начале 2023 года международная почтовая служба Великобритании **Royal** подверглась кибератаке, из-за чего была парализована работа около 11 500 почтовых отделений. Хакеры пытались вымогать у компании 80 миллионов долларов США.

Было сообщено о краже персональных данных примерно 40 миллионов избирателей, хранившихся в базе Избирательной комиссии Великобритании.

Американская развлекательная компания **Caesars Entertainment**, управляющая сетью казино, также стала жертвой хакеров. В результате кражи пользовательских данных, чтобы предотвратить их утечку на черный рынок, компания согласилась выплатить выкуп в размере 15 миллионов долларов США.

Согласно статистическим данным международной организации , составленным по 177 странам, Узбекистан занял 94-е место, что свидетельствует о низком уровне кибербезопасности, особенно с учетом стремительного роста цифровых технологий в стране (см. таблицу 2).

№	Название страны	Национальный индекс кибербезопасности	Уровень цифрового развития
1	Бельгия	94.81	74.07
2	Литва	93.51	67.34
3	Эстония	93.51	75.59
4	Чехия	90.91	69.21
5	Германия	90.91	80.01
…	…	…	…
92	Мексика	37.66	51.46
93	Вьетнам	36.36	47.69
94	**Узбекистан**	**36.36**	**49**
95	Южная Африка	36.36	49.24

В условиях стремительного развития в нашей стране данный показатель остается относительно низким, что может создать благоприятную почву для действий даже слабоорганизованных преступных групп с недобрыми намерениями.

Меры по защите от киберугроз всегда оставались актуальной темой. Индивидуальные пользователи должны быть бдительны, чтобы защитить свои данные и личные средства, а компании, банки и финансовые учреждения – чтобы сохранить свою репутацию, государственные органы – ради защиты граждан и обеспечения национальной безопасности. Одним из самых важных и эффективных способов снижения количества жертв кибератак по всей стране является повышение цифровой грамотности населения. Хотя это не может гарантировать полное устранение рисков,

каждый человек, осознавая возможные последствия своих действий, сможет избегать различных ловушек, спам-сообщений и зараженных файлов. Несмотря на важность этого процесса, он сопряжен с рядом трудностей и является лишь начальным этапом в обеспечении кибербезопасности. К ним относятся:

Разработка образовательных стандартов. Анализ статистики на уровне страны по видам атак и их жертвам позволяет целенаправленно разрабатывать специальные обучающие программы. Однако из-за высокой трудоемкости некоторые страны делят население на возрастные группы и начинают обучение с молодежи, прививая культуру этичного использования интернета. Примером успешного применения такой модели служат Великобритания, Австралия, Эстония и Сингапур. В Великобритании в рамках Национального центра кибербезопасности (NCSC) реализуется проект **CyberFirst**, в рамках которого подростки делятся на возрастные группы 7–11, 11–14 и 14–18 лет, и проходят различные курсы, тренинги, практические занятия и соревнования, обучающие основам безопасности в интернете с раннего возраста.

Также, помимо государства, в вопросах повышения цифровой грамотности должны участвовать и все финансовые учреждения. В целях снижения собственных рисков они обязаны организовывать дополнительные занятия, профилактические мероприятия и тренинги для своих сотрудников.

Планирование и подготовка. Кибербезопасность – это не вопрос «если», а «когда». Это неизбежный процесс, на который должно обращать внимание каждое предприятие, интегрированное с цифровыми технологиями. Это включает сотрудничество с надежными IT-компаниями, использование официальных операционных систем, разработанных проверенными организациями, внедрение надежных систем защиты, а при необходимости – двухфакторной аутентификации. Такая подготовка позволяет организациям осуществлять четкий контроль за своими системами и в случае угроз

защищать свои критически важные точки, соблюдая все необходимые стандарты.

Выявление и восстановление. Быстрая реакция при кибератаке позволяет минимизировать ущерб. Организация должна оперативно определить, какая часть ее системы (например, сервер) подвергается атаке и изолировать ее до нанесения ущерба – поместить в своеобразный «карантин». Это впоследствии упрощает процесс восстановления.

Солидарность. Кибербезопасность – это не только задача узкого круга специалистов, но и проблема, касающаяся каждого человека и организации в стране. Совместное проведение действий в этой сфере может привести к высоким результатам за короткое время.

Кроме вышеуказанных этапов существуют и простые, но важные **правила этики интернет-пользования**, которых следует строго придерживаться. Известно, что во многих учреждениях Узбекистана предоставление услуг, ведение отчетности и операционной деятельности осуществляется через интернет с использованием программ Microsoft Office (Word, Excel, PowerPoint и др.) и ОС Windows. К сожалению, наблюдается практика использования пиратских версий этих программ. Избегание лицензионных платежей, установленных производителями программного обеспечения может показаться безобидным, но это, во-первых, незаконно, а во-вторых, подвергает риску как саму организацию, так и данные ее клиентов.

Так, например, одной из наиболее обсуждаемых новостей в четвертом квартале 2023 года стала утечка данных почти **200 000 граждан Узбекистана**, причиной которой, как сообщалось, стало использование именно таких пиратских программ.

По мере того, как мир продолжает стремительно развиваться в сфере цифровых технологий, тема кибербезопасности становится одной из самых актуальных. Сегодня наиболее распространенными видами кибератак являются фишинг, DDoS-атаки, различные типы компьютерных вирусов, кража данных и крупномасштабные хакерские атаки. Эти угрозы

представляют собой серьезную проблему как для развитых, так и для развивающихся стран. Для Узбекистана, реализующего собственные перспективные стратегии, это также имеет важное значение.

В проекте **«Узбекистан – 2030»**, предложенном Президентом Республики Узбекистан, подчеркивается необходимость интеграции цифровых технологий во все сферы. Однако важно понимать, что подобная трансформация также увеличивает вероятность появления новых внешних угроз. Поэтому реформы в области кибербезопасности должны занимать приоритетные позиции в процессе достижения стратегических целей. Нестабильное состояние кибербезопасности может не только снизить позиции Узбекистана в международных рейтингах, но и поставить под угрозу внутреннюю национальную безопасность, вызвать экономические проблемы и распространение паники среди населения.

Достижение устойчивого состояния кибербезопасности в пределах одной страны – задача непростая, но она закладывает фундамент для будущего роста. Как показано в данной статье, первым и важнейшим шагом является повышение индивидуальной осведомленности граждан. Каждый должен осознать свою личную ответственность за собственные действия в цифровой среде и обладать базовыми знаниями о киберугрозах.

Примеры развитых стран показывают, что киберобразование должно начинаться с подросткового возраста и включать разнообразные образовательные программы, конкурсы и тренинги. На следующих этапах эту ответственность следует расширять: сначала на уровне предприятий и организаций, затем на уровне всей страны.

В заключение можно сказать, что каким бы сложным ни казался этот процесс, он играет ключевую роль в реализации стратегий будущего Узбекистана. Решение проблем в области кибербезопасности требует многогранного подхода с участием государственных структур, частного и экономического сектора, научного сообщества и самих граждан.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Указ Президента Республики Узбекистан от 5 октября 2020 года №ПФ-6079 «О Стратегии “Цифровой Узбекистан – 2030” и мерах по ее эффективной реализации».

2. Постановление Президента Республики Узбекистан от 15 июня 2020 года №ПП-4751 «О дополнительных мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан».

3. Walls, A., Perkins, E., & Weiss, J. (2013). *Definition: Cybersecurity*, 5. https://www.gartner.com/doc/2510116/definition-cybersecurity

4. Barzilay, M. (2013, 5 августа). *Простое определение кибербезопасности*.

Глобальный форум по цифровой безопасности во имя процветания, 7 июня 2021 года.

Глобальный форум по цифровой безопасности во имя процветания, 2024 год.

8. M

.

H

“*Россия–Украина: активность пророссийских хактивистов спустя два года*".

https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/

"*2023 год стал переломным для киберпреступности – вот как можно повысить безопасность систем*".