EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 7.899 www.in-academy.uz

THE STATE POLICY OF THE REPUBLIC OF UZBEKISTAN IN THE FIELD OF COUNTERING CRIMES IN THE FIELD OF DIGITAL TECHNOLOGIES AND SECURITY

Sadullaev Gayrat Abdujabbor ugli
Doctoral student at the Faculty of Postgraduate Education of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan. https://orcid.org/0009-0000-6241-1137
Khamrakulov Lochinbek Erkinjon ugli
Applicant
https://doi.org/10.5281/zenodo.11399956

ARTICLE INFO

Received: 23th May 2024
Accepted: 30th May 2024
Online: 31th May 2024

KEYWORDS

Personality, information security, crime, threat, integrated approach, analysis.

ABSTRACT

This article discusses the main problems and solutions in the field of personal information security. Problems such as constantly changing threats, a shortage of qualified specialists, the difficulties of international cooperation and a low level of awareness about cybersecurity require an integrated approach. The measures aimed at adapting to new threats, developing educational programs, strengthening international cooperation and increasing the level of safety culture among the population and organizations are analyzed.

ГОСУДАРСТВЕННАЯ ПОЛИТИКА РЕСПУБЛИКИ УЗБЕКИСТАН В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ

Саъдуллаев Гайрат Абдужаббор угли
Докторант факультета послувузовского образования Академии МВД Республики Узбекистан. https://orcid.org/0009-0000-6241-1137
Хамракулов Лочинбек Эркинжон угли
Соискатель
https://doi.org/10.5281/zenodo.11399956

ARTICLE INFO

Received: 23th May 2024
Accepted: 30th May 2024
Online: 31th May 2024

KEYWORDS

Личность, информационная безопасность, преступление, угроза, комплексный подход, анализ.

ABSTRACT

В данной статье рассматриваются основные проблемы и пути решения в области информационной безопасности личности. Проблемы, такие как постоянно меняющиеся угрозы, дефицит квалифицированных специалистов, сложности международного сотрудничества и низкий уровень осведомленности о кибербезопасности, требуют комплексного подхода. Анализируются меры, направленные на адаптацию к новым угрозам, развитие образовательных программ, усиление международного сотрудничества и повышение уровня культуры безопасности среди населения и организаций.

Проводимая судебно-правовая реформа по гуманизацию уголовного законодательства в Новом Узбекистане, получает новый импульс. В современных условиях масштабы гуманизации уголовного законодательства намного шире, нежели чем мы это представляем. В стране проводятся кардинальные реформы в сфере образования. Развития образовательных систем непременно способствует повышению правосознания и правовой культуры населения, что неизбежно обуславливает экономии репрессивных мер, применении наказаний не связанных с лишением свободы виновным лицам, совершившие преступление.

Цифровые технологии, искусственный интеллект, криптоэкономика и другие стали основным катализатором глобализации. Не зря ООН назвала цифровые технологии как *«эффективное средство достижения всех 17 целей в области устойчивого развития»*. Глобальное развитие с использованием цифровых технологий поэтому и называют цифровым будущим[1].

С другой стороны, с развитием общества новые виды преступления. В современных условиях, в мировом масштабе, распространенным является преступления в сфере компьютерных технологии и безопасности, приобретают определённый силы различные проявления религиозного экстремизма и сепаратизма. В будущем эти преступления могут создавать серьезную опасность для всего человечества.

В Конституции Республики Узбекистан закреплено, что государство создает условия для обеспечения доступа к всемирной информационной сети Интернет (*статья 33*)[2].

К сожалению, современные технологии стали использоваться злоумышленниками ради достижения преступных целей. Возник феномен киберпреступности, который по своим масштабам и степени общественной опасности намного опережает традиционную преступность.

Согласно статистическим данным экспертно-аналитической компании STATISTA в 2023 году ущерб от киберпреступности составил около 8,15 триллионов долларов США![3] Это больше, чем ВВП Японии, Германии, Индии, Великобритании и Франции.

Государственная политика в области противодействия киберпреступности направлена на создание эффективного механизма выявления и расследования преступлений, привлечение виновных к ответственности, а также защиту интересов личности, общества и государства в виртуальном и цифровом пространстве.

В статье 54 Конституции указывается, что обеспечение прав и свобод человека — высшая цель государства[4]. Поэтому правовая политика в сфере противодействия киберпреступности должна быть направлена именно на защиту прав и свобод человека в киберпространстве.

[1] un.org/ru/un75/impact-digital-technologies
[2] https://lex.uz/docs/6445147
[3] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
[4] https://lex.uz/docs/6445147

По научным исследованиям становится ясно, что в нашем национальном уголовном законодательстве преступления, подрывающие или посягающие на общественные отношения, входящие в состав информационной безопасности личности, не систематизированы.

Тот факт, что преступления, посягающие на информационную безопасность личности, имеют более специфический характер, чем другие преступления, в том числе тот факт, что эти преступления могут быть совершены в режиме онлайн как с территории одной страны, так и с территории другой страны, приводит к росту трансграничной преступности и указывает на наличие системных проблем в уголовно-правовых и организационно-правовых механизмах в этой области в странах мира.

В результате проведенных исследований следует отметить, что в связи с тем, что большинство преступных деяний совершается средствами информационных технологий, а также через Интернет, уголовная ответственность устанавливается с добавлением части или пункта в качестве дополнения к указанным статьям.

Кроме того, современные реалии общественного развития, переход технологических процессов к электронным методам управления, придание юридической силы актам, осуществляемым с помощью компьютерных технологий, также создали условия для использования этих процессов для совершения преступлений в сфере информационных технологий.

Незаконное вмешательство в работу компонентов телекоммуникационных сетей, компьютерных программ, работающих в их среде, незаконное изменение и уничтожение компьютерной информации может нарушить работу крайне важных элементов государственной инфраструктуры и создать угрозу гибели большого количества людей, нанесения имущественного ущерба в крупном размере или иных общественно опасных последствий.

Исходя из вышесказанного, можно отметить, что данный вид преступлений посягает на отношения, обеспечивающие законное, безопасное использование информационных технологий. Следовательно, сопутствующим объектом данного вида преступлений являются общественные отношения, обеспечивающие общественную безопасность и общественный порядок.

Уголовный кодекс Республики Узбекистан[5], который был принят первым среди стран СНГ, предусматривал ответственность за нарушение правил информатизации. В 2007 году государство усилило ответственность за совершение незаконных действий в области информатизации и передачи данных[6]. Была введена отдельная глава XX[1] – Преступления в сфере информационных технологий. Эта глава в 2007 году предусматривала шесть составов преступлений, в 2019 и 2024 году были включены еще три состава. Кроме того, предусматривается более строгая ответственность за совершение 13 составов преступлений с использованием информационных технологий.

[5] https://lex.uz/docs/111457
[6] https://illp.uz

В настоящее время эта сфера также эволюционирует. Согласно концепции совершенствования Уголовного и Уголовного законодательства Узбекистана, утвержденной Президентом Республики Узбекистан в 2018 году[7], необходимо пересмотреть нормы, регулирующие ответственность в области информационных технологий, учитывая глобальный технологический прогресс, а также расширить категории преступлений, которые связаны с компьютерными преступлениями. В настоящее время разрабатываются изменения в законодательстве, направленные на гармонизацию норм в этой области.

Постановлением Президента Республики Узбекистан от 14 сентября 2019 года № ПП–4452 было создано ГУП «Центр кибербезопасности», находящееся в ведении Службы государственной безопасности Республики Узбекистан[8].

Так, Центр кибербезопасности осуществляет сбор, анализ и накопление данных о современных угрозах информационной безопасности, выработку рекомендаций и предложений по оперативному принятию эффективных организационных и программно-технических решений, обеспечивающих предотвращение актов незаконного проникновения в информационные системы, ресурсы и базы данных государственных органов и организаций.

Своевременное оповещение национальных пользователей сети Интернет о возникающих угрозах информационной безопасности в национальном сегменте сети Интернет, а также оказание консультационных услуг по защите информации является основными задачи Центра[9].

Центр ежегодно публикует итоговый отчет о кибербезопасности в стране. В отчете можно увидеть проблемы и рекомендации по минимизации рисков при использовании современных технологий.

В свою очередь, для обеспечения соблюдения законодательства на национальном информационном пространстве необходимо совершенствовать деятельность и круг задач Центра кибербезопасности. Для эффективного противодействия киберпреступности необходимы следующие комплексные и многогранные подходы:

1. Постоянный мониторинг и анализ новых киберугроз.
2. Внедрение передовых технологий для обнаружения и предотвращения атак, таких как машинное обучение и искусственный интеллект.
3. Регулярные обновления систем безопасности.
4. Развитие образовательных программ и курсов по кибербезопасности.
5. Стимулирование сотрудничества между образовательными учреждениями и индустрией кибербезопасности.
6. Введение государственных и частных грантов и стипендий для подготовки специалистов.
7. Гармонизация законодательства различных стран для упрощения процесса привлечения киберпреступников к ответственности.

[7] Постановление Президента Республики Узбекистан, от 14.05.2018 г. № ПП-3723 // https://lex.uz/docs/3734183
[8] Постановление Президента Республики Узбекистан, от 14.09.2019 г. № ПП-4452 // https://lex.uz/docs/4665551
[9] https://csec.uz/ru/company/

8. Проведение образовательных кампаний для граждан и организаций о важности кибербезопасности.
9. Внедрение регулярных тренингов и симуляций кибератак для сотрудников организаций.
10. Выделение дополнительных бюджетных средств на развитие кибербезопасности.
11. Привлечение частных инвестиций и партнерств для финансирования исследований и разработок в области кибербезопасности.
12. Разработка стандартов безопасности для Интернета вещей и других новых технологий.

Эти меры помогут создать более устойчивую и защищенную цифровую среду, снизить риски киберпреступности и повысить уровень безопасности личности, общества и государства.

Учитывая вышеуказанного, можно сделать вывод, что государственная политика Республики Узбекистан в области противодействия преступлениям в сфере цифровых технологий и безопасности личности, общества и государства должна быть направлена на создание более устойчивую и защищенную цифровую среду, снижение риска киберпреступности и повышение уровня безопасности личности, общества и государства.

References:

1. un.org/ru/un75/impact-digital-technologies
2. https://lex.uz/docs/6445147
3. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
4. https://lex.uz/docs/6445147
5. https://lex.uz/docs/111457
6. https://illp.uz
7. Постановление Президента Республики Узбекистан, от 14.05.2018 г. № ПП-3723 // https://lex.uz/docs/3734183
8. Постановление Президента Республики Узбекистан, от 14.09.2019 г. № ПП-4452 // https://lex.uz/docs/4665551
9. https://csec.uz/ru/company/
10. Расулев А., Саъдуллаев Г. Вопросы международного сотрудничества по противодействию киберпреступлениям //in Library. – 2021. – Т. 21. – №. 1. – С. 81-84.
11. Расулев А. К., Саъдуллаев Г. А. Правовые меры реагирования по противодействию киберпреступлениям и подготовка кадров в сфере информационной безопасности //Проблемы управления (Минск). – 2020. – №. 3. – С. 62-68.