К ВОПРОСУ ФОРМИРОВАНИЯ ОРГАНИЗАЦИОННО-ПРАВОВЫХ ОСНОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Иканов Азамат Агзамович
доктор философии по юридическим наукам (PhD),
начальник Центра научно-прикладных исследований Университета
общественной безопасности Республики Узбекистан

АННОТАЦИЯ

В данной статье рассматривается важность создания эффективных организационно-правовых основ обеспечения кибербезопасности в Республике Узбекистан. Автор утверждает, что быстрый рост цифровых технологий и растущая зависимость от информационных систем сделали кибербезопасность жизненно важной заботой правительств, предприятий и частных лиц. В статье рассматривается текущее состояние кибербезопасности в Узбекистане и определяются некоторые из основных проблем, стоящих перед страной в этой области. В заключение статьи освещаются некоторые ключевые стратегии, которые Узбекистан может предпринять для укрепления своей позиции в области кибербезопасности и защиты своих граждан и критически важной инфраструктуры от киберугроз.

Ключевые слова: кибербезопасность**,** киберугрозы, цифровые технологии, организационно-правовые основы.

ON THE ISSUE OF FORMATION OF ORGANIZATIONAL AND LEGAL FOUNDATIONS FOR ENSURING CYBERSECURITY IN THE REPUBLIC OF UZBEKISTAN

ABSTRACT

This article discusses the importance of establishing effective organizational and legal foundations for ensuring cybersecurity in the Republic of Uzbekistan. The author assert that the rapid growth of digital technologies and the increasing dependence on information systems have made cybersecurity a vital concern for governments, businesses, and individuals. The article examines the current state of cybersecurity in Uzbekistan and identifies some of the major challenges facing the country in this field. The article concludes by highlighting some of the key strategies that Uzbekistan can

take to strengthen its cybersecurity posture and protect its citizens and critical infrastructure from cyber threats.

Keywords: cybersecurity, cyber threats, digital technologies, organizational and legal bases.

Анализ имеющихся сведений показывает возрастающую степень актуальности обеспечения безопасностью киберпространства нашей страны. Этому свидетельствуют увеличение случаев кибератак, низкие позиции страны в различных авторитетных рейтингах кибербезопасности, а также отсутствие организационно-правовых основ обеспечения кибербезопасности.

По мнению специалистов, на сегодняшний день по всему миру кибератаками наносится экономический ущерб в размере 26 млрд. долларов США.

В рейтинге подверженности киберугрозам *(CEI – Cybersecurity Exposure Index)* из 108 государств наша страна набрала индекс равный 0,7121 пункту, заняв 70 место.

Проведенный в 2020 году государственным унитарным предприятием «Центр кибербезопасности» мониторинг национального сегмента интернета выявил в нем более 27 млн. вредоносных и подозрительных действий.

Также на протяжении данного периода количество инцидентов информационной безопасности на веб-сайты органов государственного и хозяйственного управления выросло на 144%, проведенные 243 экспертизы веб-сайтов, выявили 337 нежелательных событий в национальном домене «.uz», 79 из которых веб-сайты госорганов.

В соответствии с мировым рейтингом уровня кибербезопасности, составленным аналитиками британской исследовательской компанией Comparitech, среди 60 стран, подверженных атакам криптомайнеров, Узбекистан занял 56 место.

В частности, с точки зрения обеспечения кибербезопасности одной из стран с самым высоким рейтингом является Япония, где законодательная база в данной сфере получила оценку 6 баллов, а готовность к предотвращению кибератак – 0,7 баллов, тогда как в Узбекистане данные показатели составили 3 и 0,2 балла соответственно.

Исследование данных МВД Республики Узбекистан свидетельствует, что количество противоправных деяний, совершаемых в киберпростанстве, сохраняется на значительном уровне, особенно высока доля подобных преступлений в сфере использования банковских пластиковых карточек.

Так, за 7 месяцев текущего года подразделениями МВД Республики Узбекистан в отношении 323 лиц расследовано 376 уголовных дел в киберпространстве, из которых 121 дело по ст.168 ч.2 п.«в» УК РУз *(мошенничество с использованием средств компьютерной техники)* и 83 – по ст.169 ч.3 п.«б» *(кража с несанкционированным проникновением в компьютерную систему)* УК РУз.

Среди противоправных деяний, совершенных в сфере информационных технологий, 135 преступлений связаны с использованием банковских пластиковых карточек, из которых 77 мошенничеств, 56 краж, по 1 хищение путем присвоения или растраты, а также незаконной деятельности с привлечением денежных средств и (или) другого имущества. В рамках указанных уголовных дел Экспертно-криминологическим центром МВД проведено более 300 судебных экспертиз компьютерной техники.

В то же время, требует совершенствования механизм информационного обмена между органами внутренних дел, органом финансовой разведки и банками в рамках расследования уголовных дел, связанных с мошенническими действиями с банковскими картами. В данном направлении, отсутствие методических рекомендаций, совместных решений заинтересованных структур, четкого механизма предоставления доступа к базам данных финансовых транзакций существенно затрудняют раскрытие преступлений, не позволяют своевременно пресекать преступные действия.

Справочно: *Под влиянием вышеперечисленных факторов раскрытие преступлений по данной направлении остается низким. Например, за 4 месяца 2021 года в городе Ташкенте совершено 56 преступлений, связанных с использованием банковских пластик карт, которых нераскрыто 48 или 85,7%***.**

В этой связи необходимо отметить актуальность формирования организационно-правовых основ обеспечения кибербезопасности в Республике Узбекистан, т.к. в нашей стране понятие «кибербезопасность» не закреплено ни в одном нормативно-правовом акте и сформулировано лишь выводами отдельных специалистов, исходя из личного видения той или иной проблемы.

Так, по мнению главного специалиста информационных технологий и безопасности главного управления экономического развития и сокращения бедности Ж.Абдукадирова «Кибербезопасность – это защита от случайно и умышленно совершенной информационной атаки. Будучи многогранной сферой деятельности для нее характерен только системный и комплексный подход».

По утверждению ответственного работника Национального правового центра «Адолат» Р.Жабборова «Кибербезопасность – это деятельность, направленная на цифровую защиту информационных систем, сетей и программ».

В соответствии с Законом Украины «Об основных принципах обеспечения кибербезопасности» принятым 5 октября 2017 года, «Кибербезопасность – это защищенность жизненно важных интересов личности и гражданина, общества и государства в киберпространстве».
В данном аспекте это обеспечивает устойчивое развитие цифровой коммуникационной атмосферы и информационного общества через своевременное выявление, блокирование и ликвидацию реальных и возможных угроз национальной безопасности в киберпространстве Украины.

***Справочно**: Закон о кибербезопасности имеется в странах ЕС, США, Китае, Эстонии, Украине, Туркменистане и др.государствах.*

Исходя из вышеизложенного, целесообразно принять меры к изданию в нашей стране Закона «О кибербезопасности», в котором должны найти своё отражение такие понятия как «кибербезопасность», «киберпространство», «объект кибербезопасности», «киберзащищенность объекта», «кибератака», «субъект кибербезопасности» и др.

Вместе с тем, термином «кибербезопасность» необходимо охватить такие направления как защита интернета, защита компьютеров, защита цифровых данных, защита телекоммуникационной структуры, защита канала передачи цифровых данных, защита приложения и др.

На основании этого также необходимо определить круг общественно опасных деяний, которые будут квалифицироваться как киберпреступления.

Опираясь на международный опыт рационально рассмотреть Конвенцию Совета Европы «О киберпреступности», принятую 23 ноября 2001 г. в г. Будапешт, где рассматривается понятие киберпреступления, которое охватывает следующие виды противоправных деяний: действия против компьютерной информации (в качестве предмета преступного посягательства), использование компьютера как орудия преступления и другие действия. В данном случае информация и компьютер являются объективной стороной преступления (орудие преступления, составная часть совершения или сокрытия преступления).

Также согласно Конвенции объектом киберпреступлений являются общественные отношения в сфере сбора, воспроизводства, хранения, использования компьютерных сведений, а также компьютерных систем и сетей в процессе осуществления информационной деятельности.

Объективная сторона киберпреступлений отражается в четырёх группах общественно опасных деяний:

- действия, направленные против целостности конфенденциальности компьютерных сведений и систем;
- действия, связанные с использованием компьютеров;
- действия, связанные с хранением информации;
- действия, связанные с нарушением авторских и других смежных прав.

Субъектом киберпреступления является лицо, осуществляющее вышеуказанные действия.

Субъективная сторона киберпреступления выражается в умышленном их совершении.

В соответствии с Конвенцией ответственность за киберпреступления наступает не только при оконченных действиях, но и при покушении, соучастии и пособничестве в их совершении.

В заключении к вышесказанному, необходимо подчеркнуть важность пересмотра политики в сфере обеспечении кибербезопасности и обеспечить принятие нижеследующих адресных мер по дальнейшему повышению уровня киберзащищенности Республики Узбекистан:

– разработка и принятие «Стратегии кибербезопасности Республики Узбекистан», Закона «О кибербезопасности» и дорожных карт к ним;

– в рамках принятых нормативно-правовых актов рассмотреть возможность по своевременному раскрытию и пресечению преступлений, совершаемых с использованием банковских карт путём принятия совместного решения Генеральной прокуратуры, Министерства внутренних дел с Центральным банком Республики Узбекистан, установив алгоритм и механизм дистанционного межведомственного обмена необходимыми сведениями, а также разработать методические рекомендации для сотрудников правоохранительных подразделений по данному вопросу;

– рассмотреть вопрос ратификации Конвенции ЕС «О киберпреступности»;

– проведение международных и региональных собраний, конференций и круглых столов с ведущими иностранных организациями, занимающимися вопросами кибербезопасности, а также активное принятие участия в подобных зарубежных проектах;

– рассмотрение вопроса создания национального органа (комитет, совет, рабочая группа) по совершенствованию политики кибербезопасности;

– разработка правовых основ, которые позволят обязать юридические лица, оказывающих цифровые услуги, управлять киберугрозами;

– совершенствование отчетности эффективной реализации политики в сфере кибербезопасности для компаний и организаций, оказывающих информационные услуги;

– усиление ответственности за качество выполнения требований кибербезопасности лиц, предоставляющих цифровые услуги в государственном секторе;

– включение в учебные программы общеобразовательных школ уроков по компьютерной и кибербезопасности;

– подготовка отечественных кадров в сфере кибербезопасности, их привлечение в военизированных образовательных учреждениях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ: (REFERENCES)

1. Наркулов А. К. У. Роль правоохранительных органов и общественных организаций в сфере обеспечения общественного порядка (на примере США) //Science and Education. – 2023. – Т. 4. – №. 2. – С. 1615-1620.
2. Наркулов А. К. У. НОРМАТИВНО-ПРАВОВАЯ БАЗА ЗАРУБЕЖНЫХ СТРАН И МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ //Academic research in educational sciences. – 2022. – Т. 3. – №. 3. – С. 217-224.
3. АМАНБАЕВ Ж. А., НАРКУЛОВА И. Р. К. Технология организации самостоятельной работы в высших военных образовательных заведениях Республики Узбекистан //МОЛОДОЙ УЧЕНЫЙ Учредители: ООО" Издательство Молодой ученый". – 2022. – №. 23. – С. 136-139.
4. Абдухафизов, Сардор Неъматович, Наркулова, Индира Рустам Кизи СПЕЦИФИКА ОБУЧЕНИЯ ГЛАГОЛАМ ВОСПРИЯТИЯ В ВЫСШИХ ВОЕННЫХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ // ORIENSS. 2023. №3. URL: https://cyberleninka.ru/article/n/spetsifika-obucheniya-glagolam-vospriyatiya-v-vysshih-voennyh-obrazovatelnyh-uchrezhdeniyah (дата обращения: 22.05.2023).
5. Наркулов А. МЕТОДИКА ПОДГОТОВКИ СОТРУДНИКОВ НАЦИОНАЛЬНОЙ ГВАРДИИ К ПРИМЕНЕНИЮ СИЛОВЫХ СПОСОБОВ ЗАДЕРЖАНИЯ ПРАВОНАРУШИТЕЛЕЙ //Educational Research in Universal Sciences. – 2022. – Т. 1. – №. 4. – С. 117-122.
6. Наркулов А. К. Алгоритмизация как эффективный метод оптимизации патрулирования //Science and Education. – 2023. – Т. 4. – №. 1. – С. 1165-1168.
7. Наркулов А. К. Патрулирование-основа обеспечения общественного порядка //Science and Education. – 2022. – Т. 3. – №. 11. – С. 1334-1339.

8. Abdurashidovich M. K., Kizi Y. I. R. Developing self-study competence of pedagogies in English languages by computer technologies //Наука и образование сегодня. – 2019. – №. 11 (46). – С. 45-48.
9. кизи Наркулова И. Р. ОСОБЕННОСТИ ОБУЧЕНИЯ РУССКОМУ ЯЗЫКУ КУРСАНТОВ-БИЛНГВОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ //Educational Research in Universal Sciences. – 2022. – Т. 1. – №. 3. – С. 185-193.
10. НАРКУЛОВА И. THE USE OF COMPUTER LINGUODIDACTICS IN THE PROCESS OF TEACHING THE RUSSIAN LANGUAGE //Social sciences.
11. Narkulova I. R. PROJECT TECHNOLOGY AS A MEANS OF DEVELOPING THE INDIVIDUALITY OF CADETS //International journal of conference series on education and social sciences (Online). – 2023. – Т. 3. – №. 1.
12. Хурсандов А. С., Наркулова И. Р. К. Способы выражения правой валентности глаголов восприятия в современном русском языке //Science and Education. – 2023. – Т. 4. – №. 4. – С. 1337-1341.
13. Najmutdinova M., Narkulova I. R. Q. O‘zbekiston Respublikasi suverenligining huquqiy asosi //Science and Education. – 2023. – Т. 4. – №. 3. – С. 895-899.
14. Закирова А. О., Наркулова И. Р. Қ. Роль русского языка в работе сотрудников органов внутренних дел //Science and Education. – 2023. – Т. 4. – №. 1. – С. 737-740.
15. Ашуров Р. Р. ОСОБЕННОСТИ ПРОФЕССИОНАЛЬНОЙ РЕЧИ ВОЕННОГО ЮРИСТА Ёриев Озодбек Ойбек ўғли //ЎЗБЕКИСТОНДА ИЛМИЙ ТАДҚИҚОТЛАР: ДАВРИЙ АНЖУМАНЛАР: 10-ҚИСМ. – С. 34.