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

ANALYSIS OF THE EXPERIENCE OF FOREIGN COUNTRIES IN ENSURING THE PROTECTION OF PERSONAL INFORMATION SECURITY

Sadullaev Gayrat Abdujabbor ugli
Doctoral student at the Faculty of Postgraduate Education
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Sobirov Zhakhongir Kurbonboy ugli
independent applicant
https://doi.org/10.5281/zenodo.11395151

ARTICLE INFO

Received: 22th May 2024
Accepted: 29th May 2024
Online: 30th May 2024

KEYWORDS

Crime, cybercrime, personal data protection, personal information.

ABSTRACT

This paper analyzes the experience of foreign countries in the field of personal information security. Information security has become one of the key problems of modern society in the context of global digitalization and the growing number of cyber threats. The main focus is on the consideration of legal, organizational and technological measures taken by various countries to protect personal data and prevent unauthorized access to personal information of citizens.

АНАЛИЗ ОПЫТА ЗАРУБЕЖНЫХ СТРАН ПО ОБЕСПЕЧЕНИЮ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Саъдуллаев Гайрат Абдужаббор угли
докторант факультета послувузовского образования
Академии МВД Республики Узбекистан
Собиров Жахонгир Курбонбой угли
самостоятельный соисакатель
https://doi.org/10.5281/zenodo.11395151

ARTICLE INFO

Received: 22th May 2024
Accepted: 29th May 2024
Online: 30th May 2024

KEYWORDS

Преступление, киберпреступность, защиты персональных данных, личная информация.

ABSTRACT

В данной работе проводится анализ опыта зарубежных стран в области обеспечения информационной безопасности личности. Информационная безопасность стала одной из ключевых проблем современного общества в условиях глобальной цифровизации и роста количества киберугроз. Основное внимание уделяется рассмотрению правовых, организационных и технологических мер, предпринимаемых различными странами для защиты персональных данных и предотвращения несанкционированного доступа к личной информации граждан.

Сегодня в нашей стране, которая интегрируется в мировое сообщество, проводится последовательная государственная политика по эффективному

использованию информационных коммуникационных технологий и современных информационных систем.

Помимо современных цифровых технологий, внедряемых во все сферы, создающих ряд удобств и возможностей для граждан, актуальной остается проблема обеспечения информационной безопасности личности.

Согласно данным Международного Статистического портала на начало 2024 года 5,35 миллиардов людей или 66,2 % населения Земли составляют пользователи Интернета, прирост по сравнению с предыдущим годом составил 1,8 %, что и подтверждает тезис о том, что мы практически не можем представить свою жизнь без виртуального пространства[1].

Рекордный темп роста числа пользователей сети в Узбекистане наблюдался в последние десять лет. Их количество увеличилось с 16 % до 86 % населения. Согласно данным Министерства цифровых технологий Республики Узбекистан количество пользователей всемирной сети превысило **31 миллион** человек.

По данным МВД Республики Узбекистан, в 2022 году в республике было совершено 4310 киберпреступлений. Президент Узбекистана Шавкат Мирзиёев заявил, что за 11 месяцев 2023 года в стране зафиксировали 5,5 тыс. киберпреступлений. Из них 70% — мошенничество и кражи, связанные с банковскими картами[2].

В своем выступлении на расширенном заседании Совета безопасности от 13.01.2023 года Ш.М. Мирзиёев отметил, что **«в условиях нынешних напряженных геополитических противостояний обостряются проблемы в экономической, социальной, политической сферах, информационной безопасности и других областях»[3].** Действительно, обеспечение информационной безопасности является одним из способов противодействия киберпреступности.

В структуре подобных преступлений рост числа преступлений, направленных на информационную безопасность личности, показывает отрицательную тенденцию.

При изучении современного состояния борьбы с преступлениями, направленными на личную информационную безопасность, остановимся на организационно-правовых аспектах борьбы с этим видом преступлений, которые являются предметом нашего исследования.

Организационно-правовые аспекты борьбы с преступлениями, направленными на информационную безопасность личности, включают в свой состав следующие вопросы: правовые акты, относящиеся к сфере, определяющей деятельность уполномоченных органов по борьбе с данным видом преступлений; осуществляемые ими организационно-правовые меры; вопросы, связанные с организационно-правовым механизмом борьбы с данным видом преступлений.

Итак, организационно-правовые аспекты борьбы с преступлениями, направленными на информационную безопасность личности, представлены процессом борьбы с этим видом преступлений, организационной структурой подразделений

[1] https://www.byyd.me/ru/blog/2024/02/digital-2024-datareportal
[2] https://uz.kursiv.media/2023-12-20/v-2023-m-v-uzbekistane-bylo-soversheno-55-tys-kiberprestuplenij
[3] https://www.gazeta.uz/ru/2023/01/13/sovbez/

государственных органов, относящихся к отрасли, мерами, осуществляемыми ими в борьбе с этими преступлениями, совершенствованием правовых актов, регламентирующих их деятельность, относящихся к отрасли.

Отсюда следует, что организационно-правовой механизм борьбы с преступлениями, направленными на информационную безопасность личности, представляет собой систему организационно-правовых мер, регулируемых соответствующими нормативными правовыми актами, осуществляемых структурными подразделениями компетентных органов в борьбе с этим видом преступлений.

В нормативных правовых актах в качестве субъектов противодействия преступлениям, направленным на обеспечение информационной безопасности личности, приводятся следующие государственные органы[4]:

– органы, осуществляющие оперативно-розыскную деятельность и расследование уголовных дел;

– органы, осуществляющие экспертную оценку угроз персональной информации.

Субъектами, обеспечивающими информационную безопасность личности, являются: - Президент Республики Узбекистан, Олий Мажлис, Кабинет Министров, Администрация Президента и Совет безопасности при Президенте Республики Узбекистан, Верховный суд, министерства и ведомства, в том числе гражданы.

Персональные данные должностных лиц и служащих государственных органов являются объектом повышенного интереса как внутри страны, так и за рубежом.

Деятельность по борьбе с преступлениями, направленными на информационную безопасность личности, в Узбекистане в основном осуществляется Центром кибербезопасности МВД и его территориальными подразделениями.

В большинстве стран мира мы видим, что структуры(подразделения) по борьбе с преступностью, ориентированные на личную информационную безопасность, организованы в полиции государств (МВД, министерство общественной безопасности) под следующими названиями: Киберполиция – (Украина, Греция); Управление “К” (департамент) – (РФ); отдел компьютерной преступности – (Бельгия); отдел киберпреступности – (Австрия, Румыния, Франция); отдел расследования киберпреступлений – (Финляндия); отдел расследования компьютерных преступлений – (Ирландия); отдел преступлений в области информационных технологий – (Чехия).

Также в этих государствах созданы отдельные направления и подразделения, состоящие из соответствующих специалистов в структурах по борьбе с преступностью, ориентированные на информационную безопасность личности.

Исторически первый законопроект, устанавливающий уголовную ответственность за преступления в сфере информационных технологий, был разработан в США в 1977 году[5]. На основе этого законопроекта в октябре 1984 года

[4] https://lex.uz/ru/docs/5960609

[5] Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. №11. URL:

был принят Закон о компьютерном мошенничестве и злоупотреблениях, основной правовой документ, устанавливающий уголовную ответственность за преступления в области компьютерной информации, и до сих пор в него вносятся дополнения. Закон о компьютерном мошенничестве и злоупотреблениях устанавливает ответственность за несколько основных правонарушений: компьютерный шпионаж; несанкционированный доступ к информации; компьютерное мошенничество; умышленное или неосторожное повреждение защищенных компьютеров; угрозы, вымогательство, шантаж и т.д., совершенные с использованием компьютерной техники.

В США санкции за преступления, направленные на информационную безопасность личности (кибербезопасность), включают денежные штрафы и тюремное заключение[6]. Наказание зависит от многих факторов: тяжести совершенного преступления, размера экономического ущерба, причиненного преступлением, криминального прошлого обвиняемого и т.д.

В Великобритании Закон о злоупотреблении компьютерами (незаконном использовании) действует с августа 1990 года[7]. Первый пункт этого Закона касается «Несанкционированного доступа к компьютерной информации". Если при использовании компьютера для выполнения какой-либо задачи с целью предоставления доступа к любому программному обеспечению или информации, доступной на любом компьютере, лицо считается совершившим преступление, если известно, что этот доступ является несанкционированным.

Статья 202 Уголовного кодекса Германии содержит специальный термин

“датен", который означает, что информация, хранящаяся или передаваемая электронным, магнитным или иным образом, а также компьютерные данные не могут быть просмотрены напрямую.

Согласно данной статье незаконное получение физическим лицом компьютерных данных, не предназначенных для него, особо защищенных от несанкционированного доступа, в целях преследования его собственных или третьих лиц наказывается лишением свободы на срок до трех лет.

Удаление, использование, изменение или попытка сделать данные непригодными для использования наказывается штрафом или тюремным заключением на срок до двух лет.

Из анализа зарубежного опыта можно сделать вывод, что: существует ответственность за нарушение авторских и смежных прав в нашем национальном законодательстве однако нет ответственности за присвоение продукта мышления с

https://cyberleninka.ru/article/n/razvitie-ugolovnogo-zakonodatelstva-o-prestupleniyah-v-sfere-kompyuternoy-informatsii-v-zarubezhnyh-stranah-ssha-velikobritanii-frg (дата обращения: 30.05.2024).

[6] Смекалова Мария Владимировна Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. №1. URL: https://cyberleninka.ru/article/n/evolyutsiya-doktrinalnyh-podhodov-ssha-k-obespecheniyu-kiberbezopasnosti-i-zaschite-kriticheskoy-infrastruktury (дата обращения: 30.05.2024).

[7] https://ria.ru/20130809/955198703.html

использованием всемирной паутины; в отличие от традиционных компьютерных технологий мобильные устройства, подключенные к интернету, в нашем уголовно-административном законодательстве за киберпреступления, которые могут быть совершены с помощью смарт-технологий необходимо внести изменения и дополнения; законодательством, определяющим уголовно-административную ответственность, должна быть четко определена классификация видов преступлений и правонарушений, совершаемых с использованием информационно-коммуникационных технологий; принятие директивы об использовании единой идентификационной информации для каждого пользователя с пересмотром возможностей анонимного доступа к сети Интернет, усиление контроля и контроля государства над сетью Интернет.

Из приведенного анализа можно сделать вывод, что принятие в национальном законодательстве законодательных актов по борьбе с преступлениями, направленными на информационную безопасность личности, а также развитие международно-правового сотрудничества не только восполняет правовые пробелы в этой сфере, но и способствует профилактике преступлений путем повышения культуры использования гражданами виртуального пространства и информации, а также обеспечению защиты интересов личности, общества и государства от киберпреступности. гарантийное обслуживание делает.

References:

1. https://www.byyd.me/ru/blog/2024/02/digital-2024-datareportal
2. https://uz.kursiv.media/2023-12-20/v-2023-m-v-uzbekistane-bylo-soversheno-55-tys-kiberprestuplenij
3. https://www.gazeta.uz/ru/2023/01/13/sovbez/
4. https://lex.uz/ru/docs/5960609
5. Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. №11. URL: https://cyberleninka.ru/article/n/razvitie-ugolovnogo-zakonodatelstva-o-prestupleniyah-v-sfere-kompyuternoy-informatsii-v-zarubezhnyh-stranah-ssha-velikobritanii-frg (дата обращения: 30.05.2024).
6. Смекалова Мария Владимировна Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. №1. URL: https://cyberleninka.ru/article/n/evolyutsiya-doktrinalnyh-podhodov-ssha-k-obespecheniyu-kiberbezopasnosti-i-zaschite-kriticheskoy-infrastruktury (дата обращения: 30.05.2024).
7. https://ria.ru/20130809/955198703.html
8. Расулев А., Садуллаев Г. Training of Personnel in the Field of Countering Cybercrime: the Need and the Requirement of Time //in Library. – 2021. – Т. 21. – №. 1. – С. 123-130.

9. SADULLAEV G., ABDUGOFAROV A. Ensuring personal information security: prevention and prevention //Евразийский журнал права, финансов и прикладных наук. – 2023. – Т. 3. – №. 8. – С. 43-46.
10. Расулев А., Собиров Ш., Саъдуллаев Г. Legal provision of information security as an integral factor in the context of a pandemic //in Library. – 2020. – Т. 20. – №. 2. – С. 53-58.