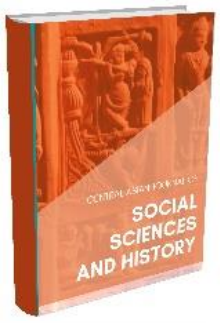
CENTRAL ASIAN JOURNAL OF SOCIAL SCIENCES AND HISTORY
VOLUME: 03 ISSUE: 12 | DEC 2022 (ISSN: 2660-6836)

CENTRAL ASIAN JOURNAL OF SOCIAL SCIENCES AND HISTORY

Journal homepage: https://cajssh.centralasianstudies.org



"Изучение Зарубежного Опыта В Сфере Конфиденциальности, Целостности И Доступности Компьютерных Данных Или Систем"

Рахмонкулов Абдурахим Худойберди ўғли
Студент Ташкентского государственного юридического университета, Факультет «Частного права»
abdurakhim142@gmail.com

Аннотация:
В данной статье рассматривается вопрос изучения зарубежного опыта в сфере конфиденциальности, целостности и доступности компьютерных данных и систем. В частности, будут сравнены уголовные кодексы Республики Узбекистан, Дании и Словении насчет киберпреступлений. Более того, будут рассмотрены Законы Республики Узбекистан “О защите персональных данных” по сравнению с Законом Дании “О защите данных” и с Законом Словении “О защите персональных данных”.

ARTICLEINFO

Article history:
Received 09-Sep-22
Received in revised form 08-Oct-22
Accepted 07-Nov-22
Available online 12-Dec-2022

Ключевые слова:
Несанкционированный доступ, компьютерные данные, компьютерные системы, персональные данные, неправомерный перехват, социальные сети.

Введение

Самой острой проблемой современного мира сейчас является обеспечение целостности, конфиденциальности и доступности компьютерных сетей или данных. Вследствие чего международное сообщество предпринимает меры по согласованию определенных уголовных норм разных стран мира.

Вице-президент Европейской комиссии Маргаритис Скинас на заседании комиссии 29 ноября 2020 г. подчеркнула, что борьба с киберпреступностью считается одним из главных целей

E-mail address: editor@centralasianstudies.org

Еврокомиссии и киберпреступность не знает границ. Разумеется, из её слов можно сказать, что киберпреступность становится все более актуальной проблемой во всём мире и наше государство не исключение.

Немаловажно отметить Указ Президента Республики Узбекистан «О Стратегии развития Нового Узбекистана на 2022-2026 годы» от 28 января 2022 года в главе VII цели 89 освещены такие вопросы как решение проблем связанных с публикацией в сети личных и конфиденциальных данных, создание и применение системы предупреждения киберпреступности, повышение уровня владения информационными устройствами населения и разработка единого НПА, которая будет регулировать сферу информации [1].

Принятии данной стратегии и конкретно вышесказанной цели означает, что с развитием информационных технологий возрастает уровень преступности в этой сфере. Следовательно, любое уважающее себя государство будет принимать соответствующие меры по предотвращению угроз, которые могут возникнуть в будущем или которые уже существуют.

Материалы и методы

Методологической основой данного исследования было выбрано несколько способов научного исследования, а именно сравнительно-правовой, структурный, логический анализ, системно-правовой и др. Сравнительно-правовой метод считается одним из распространенных и эффективных методов. Следовательно, проанализируем и сравним Уголовные Кодексы и законодательства Дании и Словении, входящие в Евросоюз и в Совет Европы, а также законодательство и Уголовный Кодекс Узбекистана насчет целостности, сохранности и доступности персональных данных. Более того, рассмотрим Конвенцию “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года).

Основой киберпреступлений считается несанкционированный доступ к компьютерным данным или системам. Так как его опасность возрастает с развитием компьютерных сетей или систем.

Итак, согласно статье 1 Главы I Будапештской Конвенции определяет следующие термины:

a) под термином "компьютерная система" можно понимать любое устройство или группу взаимосвязанных между собой, или смежных устройств, где одно или более из них, выполняет автоматизированную обработку информаций, работая в соответствии с определенной программой;

b) а термином "компьютерные данные" называются надлежащее для обработки в компьютерной системе любое представление информации, определенных фактов или понятий в форме. А также программы, которые в силе принудить компьютерную систему совершить ту или иную функцию [2].

Исходя из этой терминологии можно сказать, что компьютерная система представляет собой определенную группу взаимосвязанных между собой устройств, которые могут автоматически выполнять обработку данных. А также компьютерными данными считаются факты или информация, которые могут обрабатываться компьютерной системой. Следовательно, компьютерные данные тесно взаимосвязаны с компьютерной системой.

Раздел I части 1 главы II Конвенции “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года) описывает виды преступлений, связанные с конфиденциальностью, целостностью и доступностью компьютерных сетей и компьютерных

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836). Hosting by Central Asian Studies.

данных. И к таким преступлениям относятся воздействие на данные, неправомерный перехват данных, использование устройств в нарушении законодательства, воздействие на функционирование системы и противозаконный доступ.

Ученый А.Н.Караханьян под компьютерными преступлениями понимает “противозаконные действия, где орудием или объектом с помощью которого совершено преступление считается ЭВМ” современным языком можно толковать это все электронные устройства, которые имеют выход в сеть.

Далее мы подробно рассмотрим преступления указанные в Конвенции преступления и заодно сравним Уголовные Кодексы Республики Узбекистан, Дании и Словении.

Согласно статье 2 Конвенции “О преступности в сфере компьютерной информации” (EST N 185) сказано о противозаконном доступе следующие слова законодательные и иные меры должны быть приняты каждой стороной, которые необходимы для квалификации в качестве уголовного преступления доступ, где оно считается преднамеренным в отношении компьютерной системе в целом или любой ее части в соответствии ее национальному законодательству.

Любая сторона может требовать соответствующие меры чтобы такие действия определялись как противозаконные действия, если они содеяны с нарушениями мер безопасности и с целью завладеть компьютерными данными или иной целью. А также в отношении компьютерной системы, которая соединена с другой компьютерной системой [3].

Следовательно, страна, ратифицировавшее данный акт, принимает все необходимые меры для противодействия данного преступления.

В нашем Уголовном Кодексе есть целый раздел XX прим.1, который описывает преступления в сфере информационных технологий.

В частности, статья 278 прим. 2 описывает противозаконный доступ. И в этой статье сказано, что незаконный (противоправный) доступ к компьютерным данным означает доступ к информации или данным в информационно-вычислительных сетях, системах и их составных частях.

При этом, если эти действия стали причиной блокирования, копирования, модификации, уничтожения либо перехвата информации, а также повлекли за собой нарушение работы ЭВМ, системы электронно-вычислительных машин или их сети, то применяется санкции в виде штрафа до ста БРВ или лишением определенного права до трех лет либо исправительными работами до одного года [4].

По сравнению с нашим УК в статье 263а Уголовного Кодекса Дании сказано, что любое лицо, которое незаконным образом получает доступ к данным или программам других лиц, предназначенным для использования в системе обработки данных, подлежит наказанию в виде штрафа или тюремного заключения на срок до 1 года и 6 месяцев [5. стр. 66].

Тут мы видим, что за незаконный доступ к информации законодательством Дании предусмотрено более жесткое наказание как тюремное заключение до 1 года и 6 месяцев, а при отягчающих обстоятельствах до 6 лет. С другой стороны, у нас это деяние наказывается штрафом или исправительными работами до одного года, а при отягчающих случаях лишением

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836).. Hosting by Central Asian Studies. All rights reserved.

свободы от 1 года до 3 лет. Разумеется, это влияет на количество преступлений в Дании за несанкционированный доступ к информации.

В 1 и 2 части статьи 221 Уголовного Кодекса Словении сказано, что тот, кто взламывает информационную систему или незаконно перехватывает данные во время непубличной передачи в информационную систему или из нее, применяется санкции в виде лишения свободы на срок не более одного года.

Тот, кто незаконно использует данные в информационной системе или изменяет, копирует, передает, уничтожает или незаконно импортирует данные в информационную систему, или препятствует передаче данных или работе информационной системы, применяется наказание в виде лишения свободы на срок не более двух лет [6. стр. 91].

В отличии от Уголовных Кодексов Республики Узбекистан и Дании, Уголовный Кодекс Словении предусматривает только наказание в виде лишения свободы на определенный срок и в зависимости от тяжести преступления за незаконный перехват или доступ информации.

Итак, в статье 193 Уголовного Кодекса Дании сказано, что любое лицо, которое незаконным образом вызывает серьезные нарушения в работе общественных средств связи, государственной почтовой службы, общедоступных телеграфных или телефонных служб, радио- и телевизионных установок, информационных систем или установок для общественного водоснабжения, газоснабжения, электроснабжения или отопления, подлежит наказанию в виде лишения свободы на срок до 6 лет или штрафа [7, стр. 55].

Следовательно, за незаконный доступ к средствам связи, информационных систем т.е. к сетям телекоммуникации в Дании есть наказание в виде лишения свобода до 6 лет. А в нашем кодексе тоже есть такая аналогичная статья 278 прим.7, где описывается преступление в виде незаконного доступа к сети телекоммуникаций. За это деяния у нас предусмотрено наказание в виде штрафа, ограничением свободы от одного года до трех лет либо лишением свободы до трех лет. А в Уголовном Кодексе Словении аналогичная норма отсутствует.

Заключая сравнение Уголовного Законодательства Республики Узбекистан, Дании и Словении можно подчеркнуть, что в каждой из этих стран применяются меры для конфиденциальности, целостности и доступности компьютерных систем или компьютерных данных. В Уголовном Законодательстве каждой из приведенный стран есть нормы, которые описывают преступления, приведенные в раздел I части 1 главы II Конвенции “О преступности в сфере компьютерной информации” (EST N 185). Несмотря на то, что некоторые нормы отсутствуют в УК определенных стран как Словения. УК этой страны отличается более жесткими наказаниями в виде лишения свободы в отличии от Дании и Республики Узбекистан. Однако, В УК нашей страны более подробно описываются преступления в сфере информационных технологий более соответствуя указанным в разделе I части 1 главы II Конвенции “О преступности в сфере компьютерной информации” (EST N 185).

Перейдем к обсуждению законов Республики Узбекистан, Дании и Словении в сфере конфиденциальности, целостности и доступности компьютерных данных или компьютерных систем.

С развитием информационных технологий количество данных пользователей всемирной паутины, которые обрабатываются компьютерными сетями, резко увеличилось. Следовательно, это явление не предвещает какой-либо пользы для пользователей сети интернет. В силу этого

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836). Hosting by Central Asian Studies.

наше государство издаёт соответствующие законы.

Можно привести пример Закон Республики Узбекистан “О персональных данных”.

В статье 3 Закона Республики Узбекистан “О персональных данных” сказано, что юрисдикция данного закона покрывает такие отношения, которые появляются при обрабатывании и защите персональных данных вне зависимости от осуществляемых способов обработки, а также информационные технологии [8].

Исходя из вышесказанной статьи можно сказать, что этот закон регулируют отношения, которые возникают при обрабатывании или защите персональных данных граждан Республики Узбекистан. Мы можем отнести персональные данные к компьютерным данным, так как эти персональные данные обрабатываются компьютерными сетями. Например, различные социальные сети обрабатывают персональные данные своих пользователей. Это утверждение подтверждается статьей 1 Главы I Конвенцию “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года), где сказано о понятии компьютерных данных и сетей.

Перейдем к законодательству Словении и Дании. В основоном Закон Дании “О защите данных” и с Законом Словении “О защите персональных данных”. Эти два закона основываются Общим Регламентом защиты персональных данных (General Data Protection Regulation), который был принят 27 апреля 2016 года в Евросоюзе. Данный Общий Регламент защиты персональных данных вступил в законную силу 25 мая 2018 года.

В статье 21 Закона Словении “О защите персональных данных” сказано, что Персональные данные могут храниться только до того момента, пока это необходимо для достижения цели, для которой они были собраны или дополнительно обработаны.

По завершении обработки персональные данные удаляются, уничтожаются, блокируются или анонимизируются, если только в соответствии с законом, регулирующим архивные материалы и архивы, они не определены как архивные материалы, или если законом не предусмотрено иное для отдельного типа персональных данных [9. стр. 12].

Данная статья закона Словении соответствует статье 17 Общего Регламента защиты персональных данных (General Data Protection Regulation), где говориться об удалении персональных данных [10].

Схожая статья тоже есть в нашем законодательстве, а именно статья 17 ЗРУз “О персональных данных”, где тоже приводится уничтожение персональных данных.

Результаты исследования

Итак, обсудим результаты исследования и одно новшество в нашем законодательстве, а именно в Законе Республики Узбекистан “О персональных данных” добавили статью 27 прим.1, где описывается условия обработки персональных данных граждан Республики Узбекистан.

Согласно этой статьей 27 прим.1 вышесказанного закона, оператор или собственник при обработке персональных данных граждан нашей страны с применением информационных технологий, в том числе во всемирной паутине т.е. в Интернете, должен обеспечить их систематизацию, хранение и сбор в базах персональных данных на технических устройствах,

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836).. Hosting by Central Asian Studies. All rights reserved.

которые физически находятся на территории Республики Узбекистан. Более того, эти данные должны быть зарегистрированы в законодательном порядке в государственном реестре баз персональных данных [11].

Исходя из данной статьи можно сказать, что закон обязывает операторов т.е. различные социальные сети как Instagram, Facebook, Tik Tok, Vk и т.п. должны хранить персональные граждан Республики Узбекистан на территории нашего государства.

С одной стороны, можно подчеркнуть, что Республика Узбекистан хочет защитить персональные данные своих граждан путем хранения этих данных на серверах, которые находятся на территории Узбекистана. Тем самым минимизировав риски утечки персональных данных.

С другой стороны, на практике обязать крупные социальные сети хранить персональные данные граждан Узбекистана не простое дело. Так как, по правилам социальных сетей отдельно выделять данные пользователей конкретной страны будет похоже на дискриминацию.

Более того, эти социальные сети не уверены, что в Узбекистане есть соответствующие технологии для содержания таких серверов. Следовательно, эти социальные сети не размещают свои сервера на территории Узбекистана. В результате в работе некоторых из социальных поставили ограничения.

Из того можно сказать, что национальному закону проблематично применять санкции крупным международным компаниям.

А вот Общий Регламент защиты персональных данных (General Data Protection Regulation) имеет санкции за невыполнение норм данного нормативного акта. А под санкцией в этом случае понимается штрафы, которые зависят от конкретной статьи этого нормативного акта.

Например, применением штрафа за нарушение требований GDPR можно считать штраф в отношении компании Google на 50 млн евро в январе 2019 года. А суть нарушения заключалось в том, что политика конфиденциальности была написана на большее количество страниц и на сложным языке. В результате этого пользователи не могли понять каким же образом обрабатываются их персональные данные. Более того, согласие на обработку персональных данных также противоречило Регламенту, так как во всех полях уже были проставлены галочки [12].

Следовательно, такие международные акты как Общий Регламент защиты персональных данных (General Data Protection Regulation) имеет возможность оштрафовать такие крупные компании как Google за нарушение прав пользователей касательно персональных данных. Разумеется, если такое правонарушение произойдет в отношении персональных данных граждан Дании или Словении, то крупные компании будут оштрафованы согласно вышесказанному нормативному акту.

Заключая обсуждение данного абзаца можно сказать, что Закон Республики Узбекистан “О защите персональных данных”, Закон Дании “О защите данных” и Закон Словении “О защите персональных данных” имеют свои схожести и отличие. Схожесть данных законов проявляется в обязательности удаления персональных данных после использования их по назначению. А вот Закон Дании “О защите данных” и Закон Словении “О защите персональных данных” отличается от аналогичного закона нашего государства тем, что Дания и Словения разрабатывали эти законы в соответствии с Общим Регламентом защиты персональных данных

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836). Hosting by Central Asian Studies.

(General Data Protection Regulation).

Заключение

Делая вывод из всего вышесказанного можно подчеркнуть, что нормы Уголовного Законодательства Республики Узбекистан, Дании и Словении насчёт конфиденциальности, целостности и доступности компьютерных данных и систем составлены на основании Конвенции “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года). Более того, уголовный кодекс вышеупомянутых стран имеют различные санкции за преступления в информационной среде. Более того, исходя из примера намсчёт штрафа Google за нарушение норм Общего Регламента защиты персональных данных (General Data Protection Regulation). Следовательно, наш ЗРУз “О персональных данных” должен подвергнуться совершенствованию. А также наш ЗРУз “О персональных данных” должен был разрабатываться в соответствии Общим Регламентом защиты персональных данных (General Data Protection Regulation). Для этого, Республике Узбекистан должен ратифицировать данный нормативный акт.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Указ Президента Республики Узбекистан «О Стратегии развития Нового Узбекистана на 2022-2026 годы» от 28 января 2022
2. Конвенция “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года). https://www.alppp.ru/law/pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii---185-rus--angl-.html
3. Конвенция “О преступности в сфере компьютерной информации” (EST N 185) (Будапешт, 23 ноября 2001 года).
4. Уголовный Кодекс Республики Узбекистан https://lex.uz/docs/111457
5. Уголовный Кодекс Дании стр. 66 https://www.legislationline.org/download/id/6372/file/Denmark_Criminal_Code_am2005_en.pdf
6. Уголовный Кодекс Словении стр. 91 https://www.wipo.int/edocs/lexdocs/laws/en/si/si045en.pdf
7. Уголовный Кодекс Дании стр. 55 https://www.legislationline.org/download/id/6372/file/Denmark_Criminal_Code_am2005_en.pdf
8. Закон Республики Узбекистан “О персональных данных” ЗРУ-547-сон 02.07.2019 https://lex.uz/docs/4396428
9. Закона Словении “О защите персональных данных” стр.12 https://rm.coe.int/16806af30c
10. Общий Регламент защиты персональных данных (General Data Protection Regulation) https://gdpr-info.eu/
11. Закон Республики Узбекистан “О персональных данных” ЗРУ-547-сон 02.07.2019 https://lex.uz/docs/4396428 статья 27 прим. 1
12. https://data-privacy-office.com/what-is-gdpr/#Rights
13. Инамджанова, Э. Э. (2022). ЗАРУБЕЖНЫЙ ОПЫТ И КОЛЛИЗИИ В ПРАВОВОМ

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836).. Hosting by Central Asian Studies. All rights reserved.

РЕГУЛИРОВАНИИ ТОКЕНОВ (КРИПТОВАЛЮТ). Oriental renaissance: Innovative, educational, natural and social sciences, 2(7), 141-153.

14. Imamalieva , D. . (2022). Recent Challenges of Big Data Application in Healthcare System. International Conference on Multidimensional Research and Innovative Technological Analyses, 121–124. Retrieved from http://conferenceseries.info/index.php/ICMRITA/article/view/198

E-mail address: editor@centralasianstudies.org
(ISSN: 2660-6836). Hosting by Central Asian Studies.