СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА СТРАН СНГ В СФЕРЕ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Закатнова Анна Александровна

студент, Саратовская государственная юридическая академия, РФ, г. Саратов

Шевченко София Васильевна

студент, Саратовская государственная юридическая академия, РФ, г. Саратов

Желоков Николай Вячеславович

научный руководитель, канд. юрид. наук, доцент кафедры уголовного и уголовно-исполнительного права, студент, Саратовская государственная юридическая академия, РФ, г. Саратов

Аннотация. Современное информационное общество и условия жизни людей во многом обусловливаются уровнем доступности использования информации. Главным фактором здесь выступает право граждан на доступ к информации, соблюдение законности при ее сборе и использовании. Сегодня в мире информационных технологий основная часть информации приходится на компьютерных носителях, флеш-устройствах. Такой этап развития жизни общества можно отметить как переход на качественно новый научно-технологический уровень. В условиях реальности совершение преступлений против безопасности компьютерной информации способно оказывать весьма негативные воздействия на национальную безопасность в целом, развитие науки и техники, а также цифровой экономики в Российской Федерации.

Ключевые слова: уголовный закон, компьютерная безопасность, квалификация.

Законодатель предусматривает строгие меры уголовно-правовой ответственности за совершение различных видов преступлений против безопасности компьютерной информации (ст.ст. 272-274.1 УК РФ). [7] Обратившись к анализу экспертных данных, можно сделать вывод о ежегодном росте криминальной активности компьютерной преступности и производного от них размера ущерба [1].

Преступления против безопасности компьютерной информации – это запрещенные уголовным законом Российской Федерации виновно совершенные общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности обращения компьютерной информации или вреда критической информационной инфраструктуре Российской Федерации.

С 1 января 2018 года вступил в силу Федеральный закон №194-ФЗ о дополнении главы 28 УК РФ статьей 274.1, который в полной мере согласуется с положениями Доктрины (п. 22) о защите информационной инфраструктуры как одной из стратегических целей обеспечения информационной безопасности [2]. Данный Федеральный закон предусматривает более серьезные меры ответственности за неправомерное воздействие на критическую

информационную инфраструктуру Российской Федерации [3].

Перечисленные выше внесённые законодателем изменения подтверждают актуальность развития направления политики в сфере обеспечения национальной безопасности.

Российская Федерация является участницей различных международных форумов, одним из которых является Конференция, проходившая в Сингапуре 28-30 сентября 2016 года [9]. Итогом проведения таких мероприятий возникает необходимость создания на межгосударственном и государственном уровне специализированных органов по борьбе с компьютерными преступлениями [4].

Так, например, в Уголовном Кодексе Грузии предусмотрена ответственность за киберпреступления [5]. По своему смыслу деяния, ответственность за которые предусмотрена ст. 284 и ст.286, могут квалифицироваться в отечественной практике по ст. 272 УК РФ. Вместе с тем возможность квалификации такого деяния по совокупности с иными составами преступлениями УК Грузии не исключает.

Научный интерес представляет Уголовный Кодекс Армении, в котором составы рассматриваемых преступлений содержатся в Главе 24 «Преступления против безопасности компьютерной информации» [6]. В данном уголовном кодексе предусмотрен состав преступления за компьютерный саботаж (ст. 253 УК РА), который остается неизвестным отечественному законодателю по настоящее время.

Уголовный Кодекс Узбекистана по своему содержанию относительно преступлений против безопасности компьютерной информации близок к нормам Российского уголовного закона [8].

По сравнению с российским уголовным правом в законодательстве нашей страны отсутствуют такие составы преступления как «изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе» (ст. 278-3 УК РУ).

Проведя сравнительно-правовой анализ уголовного законодательства стран СНГ, можно сделать вывод о том, что предусмотренные в них составы преступлений, во многом схожи с составами преступлений, предусмотренными в отечественном уголовном законодательстве. Некоторые страны-участники СНГ за постсоветский период развития уголовного законодательства внесли существенные изменения в сфере регламентации уголовной ответственности рассматриваемых деяний и шагнули вперед попутно с развитием информационных технологий.

Следует отметить, что исходя из санкций, предусмотренных уголовно-правовыми нормами УК РФ стран-участников СНГ за преступления против безопасности компьютерной информации, существенной разницы между ними нет. Разница лишь в том, что в каких-то странах ответственность мягче (например, в Грузии, Армении, Узбекистане), а в других, хоть и несущественно, но выше (например, Казахстан).

Необходимо отметить, что правовая база в сфере преступлений против компьютерной безопасности имеет ряд сходств и различий, на которые необходимо обратить внимание в настоящее время.

В заключение хотелось бы отметить, что учет опыта стран ближнего зарубежья необходим для дальнейшего развития и выработки единого подхода к квалификации данной категории преступлений.

Список литературы:

1. Лацинская М. Group-IB представила отчет о хакерских атаках // Газета.Ру. 2016 г. 13 окт. URL: https://www.gazeta.ru/ (дата обращения: 09.01.2023).

2. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 дек. 2016 г. № 646 // Собрание законодательства РФ. 2016. №50. Ст. 7074.

3. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О государственной поддержке предпринимательской деятельности в Арктической зоне Российской Федерации» от 13.07.2020 №194-ФЗ (ред. 21.12.2021) // Собрание законодательства РФ. 2020. №29. Ст. 4504.

4. Конвенция Совета Европы о преступности в сфере компьютерной информации: ETS № 185, 23.11.2001, Будапешт; п. «h» ч. 1 Конвенции ООН против транснациональной организованной преступности: принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года; Создание глобальной культуры кибербезопасности: Резолюция, принята Генеральной Ассамблеей 31.01.2003.

5. Уголовный кодекс Грузии от 13.08.1999 г. № 41 (48) // URL: https://matsne.gov.ge/ka/(дата обращения: 10.01.2023).

6. Уголовный кодекс Республики Армения от 18.04.2003 г. // URL: http://www.parliament.am/legislation./ (дата обращения: 10.01.23).

7. Уголовный кодекс Российской Федерации от 13 июля 1996 г. №63-ФЗ (ред. от 29.12.2022) // Собрание законодательства РФ. 1996. №25. Ст.2954.

8. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 г. // URL: http://lex.uz/pages/getpage.aspx/(дата обращения: 10.01.2023).

9. INTERPOL-EuropolCybercrimeConference (28-30 Сентября 2016, Сингапур).