Юсько Алина

Магистрант

Направление: Юриспруденция

Магистерская программа: Уголовное право, криминология, уголовно-исполнительное право

Уголовное законодательство зарубежных государств и стран СНГ об ответственности за неправомерный доступ к компьютерной информации

Аннотация. В статье проведен краткий сравнительно-правовой анализ уголовного законодательства ряда зарубежных стран, а также стран-участников СНГ с целью выявления общих и отличительных особенностей установления уголовной ответственности за несанкционированный доступ к компьютерной информации. В процессе исследования выявлена несогласованность уголовного законодательства европейских стран и отмечается необходимость унификации подходов к криминализации несанкционированного доступа к компьютерной информации.

Ключевые слова: преступление, компьютер, информация, доступ.

С момента появления новых информационных технологий и процессов возникла необходимость их правового регулирования. Как всем известно, право – это универсальный регулятор общественных отношений, однако в сфере компьютерной информации оно оказалось не способным к ее регулированию.

Для того, чтобы борьба с компьютерными преступлениями, а именно неправомерным или в некоторых законодательных актах зарубежных стран называемым несанкционированным доступом к компьютерной информации, была эффективной необходимо принимать во внимание практический опыт других стран, так как этот вид преступлений в отечественном уголовном законодательстве является новым.

Наряду с этим перед большинством зарубежных стран в настоящий момент также стоит проблема борьбы с одним из наиболее «популярных» преступлений – неправомерный доступ к компьютерной информации. Многие зарубежные государства стараются усовершенствовать законодательство, которое регулирует борьбу с компьютерными преступлениями. Унификация законодательства в данной области необходима в связи с ростом компьютерных преступлений международного характера и с этой целью целесообразно провести сравнительно-правовой анализ уголовного законодательства некоторых зарубежных государств и стран СНГ для выявления общих и отличительных особенностей установления уголовной ответственности за неправомерный доступ к компьютерной информации.

В современном мире одной из первых цивилизованных стран, которая приняла меры по установлению уголовной ответственности за совершение преступлений в компьютерной сфере были Соединенные Штаты Америки, где компьютерные преступления обозначились раньше других государств.

В США еще в 1977 году был разработан первый законопроект, который устанавливал уголовную ответственность за преступления в сфере информационных технологий. В октябре 1984 года на базе вышеуказанного законопроекта был принят закон о мошенничестве и злоупотреблении с использованием компьютеров (CFAA – Computer Fraud and Abuse Act), который стал основным нормативно-правовым актом, констатирующим уголовную ответственность за преступления в сфере компьютерной информации. В дальнейшем данный документ преобразовывался [7].

Закон о мошенничестве и злоупотреблении с использованием компьютеров определяет ответственность за следующие основные составы преступлений:

- компьютерный шпионаж;
- несанкционированный доступ к информации;
- компьютерное мошенничество;

– умышленное или по неосторожности повреждение защищенных компьютеров;

– угрозы, вымогательство, шантаж, совершаемые с использованием компьютерных технологий и другие.

Санкциями за киберпреступления являются денежные штрафы, а также тюремное заключение и зависит наказание от таких факторов как: тяжесть совершенного преступления, размер экономического ущерба, причинность деяния, криминальность прошлого подсудимого и многие другие.

Одним из разделов закона о мошенничестве и злоупотреблении с использованием компьютеров регламентируется экономический шпионаж и им предусматривается повышение штрафов за хищение интеллектуальной собственности американских компаний. В данном разделе урегулированы также и сроки заключения для приговоренных судом по этим обвинениям – до 20 лет. В случае, если злоумышленник совершил проникновение в компьютерные сети инфраструктуры США, такие как телесети, энергосети, транспортные каналы связи, системы управления водоснабжением, то он может быть приговорен к 30-ти годам заключения без права досрочного освобождения.

В Великобритании в августе 1990 года вступил в силу Закон о компьютерных злоупотреблениях [4, с. 63]. В данном документе первый параграф регламентирует «неуполномоченный доступ к компьютерным данным» и устанавливает, что лицо совершает преступление, при использовании компьютера для выполнения любой функции с преднамерением обеспечить доступ к любой программе либо данным, которые содержатся в любом компьютере, если этот доступ заведомо неправомочен. Согласно законодательному акту преступлением в компьютерной сфере является доступ к компьютеру, с помощью которого модифицируются либо совсем уничтожаются программы или данные; информация копируется либо перемещается в иное от первоначального нахождения место; данные каким-либо способом используются. Наказание за совершение указанного

преступления предусмотрено в виде штрафа либо тюремного заключения на срок не более 6 месяцев [6].

В Уголовном кодексе Германии используется термин – «Daten», определение которому указано в ст. 202 УК Германии и обозначает информацию, которая сохранена либо передается электронным, магнитным или другим способом, который визуально не воспринимается, т.е. компьютерные данные. Наказание в виде лишения свободы сроком до трех лет предусмотрено за то, что лицо, с целью извлечения выгоды для себя либо для третьего лица незаконно получило компьютерную информацию, предназначенную не ему, и которая находится под специальной защитой от неправомочного доступа. Также наказание в виде штрафа либо заключения сроком до двух лет предусмотрено за такие деяния как стирание, уничтожение, приведение в негодность, изменение информации или попытки произвести такие действия [2].

В соответствии с Уголовным кодексом Испании ст. 197 предусмотрено наказание в виде штрафа либо тюремное заключение на срок от одного до четырех лет за преступные деяния, такие как раскрытие и распространение тайных сведений без согласия их владельца, включая сведения из электронной почты, сведения, которые хранятся в базах данных, а также перехват телекоммуникаций или применение записывающих и подслушивающих устройств [3, с. 821].

Согласно ст. 615 УК Италии санкционирует наказание в виде лишение свободы сроком до трех лет за неправомерные деяния как неправомочный доступ к компьютеру либо телекоммуникационной системе, а именно доступ к компьютерам либо системам, которые защищены мерами безопасности, или доступ вопреки выраженного либо подразумеваемого желания владельца подобный доступ исключить [5].

Компьютерные преступления предусмотрены также Модельным Уголовным кодексом для государств СНГ от 17.02.1996. Разделом XII главой

30 регламентируются «Преступления против информационной безопасности». К данной группе преступлений относятся:

– несанкционированный доступ;

– модификация компьютерной информации;

– компьютерный саботаж;

– неправомерное завладение компьютерной информацией;

– изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе либо сети;

– разработка, использование и распространение вредоносных программ;

– нарушение правил эксплуатации компьютерной системы либо сети.

В свою очередь уголовное законодательство различных государств участников СНГ имеет свои особенности в части установления вида уголовно-правовых деяний в данной сфере, а также особенности имеют и наименование глав, где расположены данные составы преступлений.

К примеру, уголовные кодексы Беларуси, Таджикистана и Армении содержат главы, регламентирующие данные преступления. Они имеют общее название «Преступления против информационной безопасности». В УК Украины данные составы преступлений находятся в главе под названием «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей». А в УК Молдовы глава именуется «Информационные преступления и преступления в области электросвязи» [1, с. 89].

Проведенный анализ уголовного законодательства зарубежных государств выявил, что, несмотря на то, что несанкционированный доступ к компьютерной информации во многих европейских государствах законодательно закреплен, однако отсутствует унифицированный подход к описанию признаков состава данного преступления, что снижает эффективность противодействия рассматриваемому преступлению.

Анализ же уголовного законодательства стран СНГ позволяет заключить, что единого подхода на понятие данной группы преступлений нет, но, несмотря

на это в целом в уголовном законодательстве стран СНГ содержатся практически идентичные составы преступлений и только их количество может варьироваться в зависимости от законодательного акта [1, с. 91].

Также можно сделать вывод о том, что большинство стран СНГ придают особое значение противодействию таким деяниями как несанкционированный (неправомерный) доступ, создание, использование и распространение вредоносных компьютерных программ, компьютерный саботаж, модификация компьютерной информации, ее перехват, нарушение правил эксплуатации компьютерной системы или сети.

Тем не менее, исследование накопленного в других странах законодательного опыта может быть использовано для выработки предложений по совершенствованию уголовного законодательства в части обеспечения безопасности компьютерной информации.

Литература

1. Волосова Н.Ю., Журкина О.В. Уголовное право стран СНГ: Учебное пособие. Оренбург: ОГУ, 2020.

2. Головненков П.В. Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB) – Научно-практический комментарий и перевод текста закона, 2021 [Электронный ресурс] // Режим доступа: https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann (дата обращения: 17.12.2021).

3. Козочкин И.Д. и др. Уголовное право зарубежных стран. Общая и особенная части: Учебник / Отв. ред. Н.Е. Крылова. 4-е изд., перераб. и доп. М.: Юрайт, 2020.

4. Аистова Л.С., Краев Д.Ю. Уголовное право зарубежных стран: Учебное пособие. СПб.: Санкт Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2020.

5. Codice penale. Libro I-III / con le modifiche apportate dalle leggi 205/1999; 479/99, 507/1999; 7.12.2000 n. 397 (indagini difensive G.U. 3 gennaio 2001 e legge

1.03.2001 n. 63. legge 27 marzo 2001 n. 97. Artt. 1-734 [Электронный ресурс] // Режим доступа: https://www.polpenuil.it/attachments/047_CodicePenale.pdf (дата обращения: 17.12.2021).

6. Computer Misuse Act 1990. First Published 1990, Reprinted in the United Kingdom by The Stationery Office Limited. London, 1997 [Электронный ресурс] // Режим доступа: https://www.legislation.gov.uk/ukpga/1990/18 (дата обращения: 17.12.2021).

7. Federal Criminal Code and Rules / Title 18 – Crime and Criminal Procedure – § 1030 Fraud and related activity in connection with computers – (amendment received to February 15, 1999), West Group, St. Paul, Minn, 1999 [Электронный ресурс] // Режим доступа: https://www.law.cornell.edu/rules/frcrmp (дата обращения: 17.12.2021).