УДК 343.2.7

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Саттаров Р.Р.

магистр 2 курс,

Набережночелнинский институт (филиал) ФГАОУВО «Казанский (Приволжский) федеральный университет»

г. Набережные Челны, Россия

Аннотация

В данной статье автор описывает криминологические особенности преступлений, совершаемых в области информационных технологий. В настоящей статье проанализированы теоретические аспекты и рассмотрены криминальные характеристики данного преступления. Делается вывод о том, что все преступления совершены в области информационно-коммуникационных технологий.

Ключевые слова: информационно-коммуникационные технологии, киберпреступность, информация, преступления в сфере информационно-коммуникационных технологий, компьютерные преступления.

CRIMINOLOGICAL CHARACTERISTIC OF CRIMES COMMITTED IN THE FIELD OF INFORMATION TECHNOLOGIES

Sattarov R.R.

Master 2 course,

Naberezhnye Chelny Institute (branch) of FSAEI of Kazan (Volga Federal University)

Naberezhnye Chelny, Russia

Annotation
In this article, the author describes the criminological features of crimes committed in the field of information technology. In this article, we analyzed theoretical aspects and examined the criminal characteristics of this crime. The conclusion is made about all crimes committed in the field of information and communication technologies.
Key words: information and communication technologies, cybercrime, information, crimes in the field of information and communication technologies, computer crimes.

Цифровые технологии, появившиеся в конце XX века, выявили новые социальные связи, и знакомство с сообществом начало меняться, после чего появились новые формы преступности и, следовательно, новые нормы уголовного права.

Глава 28 "Преступления в сфере компьютерной информации" была добавлена в УК РФ 1996 г. и включала в себя четыре состава преступления (ст. 272-274.1 УК РФ). Глава 21 УК РФ была дополнена статьей 159.6 " мошенничество в сфере компьютерной информации" [2].

Информационная и коммуникационная информация, преступность в области техники и степень ее разнообразия требуют интенсивного изучения термина «компьютерная информация». В настоящее время преступные действия совершаются не только в сфере информации, но и в других сферах связей с общественностью.

Важной частью национальной безопасности Российской Федерации было обеспечение безопасности критически важных инфраструктурных и информационно-коммуникационных систем, а также повышение уровня безопасности корпоративных и персональных информационных систем [3].

Судебная практика и научная литература не позволяют прийти к

единодушному мнению о классификации таких преступлений, даже теоретические инструменты и терминология не имеют единого представления. Таким образом, наука уголовного права не устраняет вышеуказанные пробелы и должна быть дополнена.

Сегодня существует много видов компьютерных преступлений (киберпреступность): разглашение конфиденциальной информации, коммерческой тайны, личной информации, производство и распространение компьютерных вирусов, взлом чужого доменного имени, административные и преступные действия, в том числе детей, а также производство детской порнографии. Создание криптовалют позволяет обналичивать деньги. Интернет позволяет оставаться незамеченным в преступлении. Кроме того, благодаря своей способности действовать удаленно, преступники используют различия в правовых системах разных стран, чтобы избежать ответственности. Кибертерроризм процветает. Вышеперечисленное можно сделать, используя компьютер жертвы и Интернет.

Отправной точкой для раскрытия преступлений в области информационно-коммуникационных технологий считается специализация преступлений в области компьютерной информации.

Для примера возьмем норму ст. 272 УК РФ "Неправомерный доступ к компьютерной информации". Данная статья содержится в Главе 28 "Преступления в сфере компьютерной информации", последняя, в свою очередь, содержится в разделе 19 УК РФ "Преступления против общественной безопасности и общественного порядка". Эта позиция обусловлена тем фактом, что любое незаконное вмешательство в банковские, военные и другие компьютерные системы назначения может нанести вред любому человеку, включая смерть людей.

Статья 272 УК РФ следует тенденции, в соответствии с которой нормы права имеют многоотраслевой характер. В связи с тем, что

большинство понятий, содержащихся в статье 272 УК РФ, подробно раскрываются в других нормативно-правовых актах, в частности Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", данная статья является бланкетной. Итак, слово «информация» раскрывается как материал (сообщение, данные) независимо от формы их предоставления.

Объектом преступления считаются отношения защищающие права лиц, которые в соответствии с законом могут осуществлять свои полномочия в отношении информации. Кроме того, выделяется также дополнительные объекты преступления, которыми выступают различные виды тайн (государственная, адвокатская, коммерческая и т.д.).

Объективная сторона: создает несанкционированный доступ к защищенной законом информации о компьютере. Субъективная сторона: характеризуется преднамеренной формой вины в отношении предпринятых действий. Субъект: любой человек, достигший возраста 16 лет.

Многие авторы придерживаются мнения, что компьютерные преступления определяются как виртуальные преступления или действия, которые только нарушают безопасность компьютерных данных и систем [4]. Практика показала, что такая концепция тесно связана с реальными общественными отношениями.

Другие авторы считают, что при совершении компьютерных преступлений первой предпосылкой считается наличие сети. Сегодня с помощью Интернета сообщества обмениваются информацией, передавая некоторую информацию. В то же время Интернет, несмотря на новые возможности для человечества, несет новые риски и используется преступниками для активного совершения социально опасных действий [5].

Также следует обратиться к международным нормам. Главным

правовым актом, посвященной описываемой проблемы является Конвенция Совета Европы от 23 ноября 2001 г. "О преступности в сфере компьютерной информации", г. Будапешт (далее - Будапештская конвенция).

В Конвенции описываются такие понятия, как «компьютерные данные», «компьютерная система», «данные потока сведений» и «поставщик услуг». Вот четыре распространенных типа киберпреступности:

- преступления против конфиденциальности, целостности и доступа к данным и компьютерным системам (незаконный доступ к компьютерным системам, незаконный перехват, вмешательство в данные, вмешательство в системы и неправильное использование оборудования);

- компьютерные преступления;

- содержание данных / материалы, связанные с правонарушениями;

- преступления, связанные с нарушением авторских прав и смежных прав.

Кроме того, только первый тип преступления может быть отнесен к фактическому компьютеру, остальные три связаны с любым компьютером (computer-related), либо совершаются с помощью компьютера (computer-facilitated).

Однако, вышеуказанная Конвенция не была ратифицирована Российской Федерацией в связи с тем, что в ней содержалась норма, которая позволяла бы иностранным спецслужбам в любое время и без предупреждения осуществлять свои операции в сетях стран участниц Будапештской конвенции.

Россией ратифицированы другие международные акты общего характера, в частности Конвенция от 15.11.2000 "Против транснациональной организованной преступности".

В качестве альтернативы Будапештской конвенции Россия с

помощью ряда других соответствующих департаментов разработала Конвенцию ООН о сотрудничестве в области противодействия информационной преступности, подготовленную российским министерством иностранных дел. Основной целью Конвенции считается принятие и усиление мер, направленных на эффективное предупреждение преступности и других незаконных действий в области информационно-коммуникационных технологий (ИКТ).

Проект закрепил в себе 12 видов преступлений: незаконный доступ к информации в электронном виде, незаконный перехват, незаконное воздействие на информацию; нарушение функционирования ИКТ, создание, использование и распространение вредоносных программ, распространение спама; контрабанда устройства; кража ИКТ; детская порнография; сбор информации в электронном виде путем введения пользователя в заблуждение; информация, связанная с преступлениями, защищенными национальным законодательством; нарушение авторских прав на ИКТ. Статья 18 предусматривает акты ИКТ, которые признаны в качестве преступлений по международному праву.

Из вышеизложенного можно сделать вывод о том, что Российское уголовное право имеет узкую направленность в сфере преступлений, совершаемых в области информационных и коммуникационных информаций, технологий, и распространяется только на преступления в области компьютерной информации. Концептуальный механизм должен быть разработан в отношении терминологии в области информационных и коммуникационных технологий.

Библиографический список:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-

ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // "Собрание законодательства РФ", 04.08.2014, № 31, ст. 4398.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // "Собрание законодательства РФ", 17.06.1996, № 25, ст. 2954,

3. Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации" // "Собрание законодательства РФ", 04.01.2016, № 1 (часть II), ст. 212

4. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: Монография. - М.: Юрлитинформ, 2018. 306 с.

5. Летелкин Н.В. К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право: стратегия развития в XXI веке: Материалы XV Международной научно-практической конференции (Москва, 25 - 26.01.2018): Сб. науч. ст. М.: Проспект, 2018. С. 617 - 619.

6. Саркисян А.Ж. Состояние преступности в сфере высоких технологий / А.Ж. Саркисян // Расследование преступлений: проблемы и пути их решения. - 2015. - N 4(10). - С. 80 - 84.

7. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. канд. юрид. наук. - Владивосток, 2005. 235 с.

Оригинальность 75%