УДК 341.1

О НЕКОТОРЫХ ВОПРОСАХ СОВЕРШЕНСТВОВАНИЯ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ СОВЕРШЕННЫЕ СРЕДСТВАМИ ИНТЕРНЕТ ТЕХНОЛОГИЙ В КИБЕРПРОСТРАНСТВЕ.

***Р. М. Данилов**, доцент кафедры информационного и технического обеспечения органов внутренних дел Дальневосточный юридический институт МВД России, кандидат технических наук*

В статье произведен анализ применения интернет технологий при раскрытии преступлений связанных с киберпространством. Так же уделено внимание описанию некоторых достоинств и недостатков методов расследование преступлений в интернет сетях.

Ключевые слова: Интернет; преступления; компьютерная сеть; уголовный кодекс; МВД.

ON SOME ISSUES OF IMPROVING THE DETECTION OF CRIMES COMMITTED BY MEANS OF INTERNET TECHNOLOGIES IN CYBERSPACE.

R. M. Danilov, associate professor of the Department of Information and Technical Support of the law enforcement agencies of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, kandidat nauk, degree in Technical Sciences

The article analyzes the use of Internet technologies in solving crimes related to cyberspace. Attention is also paid to the description of some advantages and disadvantages of methods of investigating crimes in Internet networks.

Keywords: Internet; crimes; computer network; criminal code; Ministry of Internal Affairs.

В век цифровых информационных технологий, одним из важных критериев национальной безопасности и безопасности каждого отдельного гражданина страны является информация, которая охватывает каждый аспект в жизни людей и взаимодействия отдельных структур государства.

Современные информационные технологии все больше приобретают популярность с ростом технологического процесса. Многие бюрократические процессы деятельности переходят в глобальную сеть. Уже в начале 2000-х годов с приобщением населения к сети интернет появился вопрос о правовой защите граждан, а также о защите информации и средств коммуникации от постороннего преступного вмешательства. Люди, овладевшие умением сбора, накопления информации, ее обработке и распространению, все чаще становились жертвами киберпреступников.

Данную проблему можно рассмотреть с несколько различных сторон. Первая – это вопросы связанные с понятийным аппаратам понятий информационных технологий. Вторая сторона – правовые основы отношений субъектов информационных правоотношений.

Рассматривая понятия современных информационных технологий можно предположить, что основная суть это прежде всего технологии и информация, которые обрабатываются, передаются и хранятся на различных источниках.

В современном мире уже не является редкостью преступление совершенный в сети интернет, посредством технологий и это доказывает статистика правонарушений в РФ [1]. Если погрузится в саму суть определения интернет-правонарушения, интернет-преступность, то можно сказать, что это противоправное общественное деяние, которое совершается в сети интернет. Согласно Уголовного кодекса РФ ст. 272, 273 неправомерный доступ к компьютерной информации, а также распространение компьютерных вирусов несет ответственность, кто распространяет данный вирус [2]. Очень часто бывает такое что пользователь и не знает, что его компьютер заражен вирусом и он участник правонарушения. Сейчас, когда целью преступников является не только приобретение данных большой компании, но и личная информация пользователей необходимость данного вопроса о защите информации всемирной сети возрастает во много раз, нежели раньше. Также хочется сказать, что вместе с этим без повсеместной информатизации невозможно развитие банков, государственных учреждений и общества в целом. Именно поэтому государство применила можно сказать практически все возможные меры для защиты от преступлений в виде посягательств в сфере компьютерной информации прав и свобод граждан Российской Федерации.

И таких примеров в судах Российской Федерации большое количество. Прежде чем говорить о статистике преступлений в сети интернет нужно дать определение этому словосочетанию. Так что же такое статистика преступления? Статистика преступлений – это одна из отраслей статистики, предметом исследования которой является анализ положения преступности: состава и динамики; ее уровня, активности правоохранительных органов по борьбе с правонарушениями; фоновых явлений, содействующих и сопутствующих преступности [3].

Если посмотреть на статистику преступлений с января по июнь 2021 года в России, то можно заметить, что информационных преступлений стало больше на 32 %, если сравнивать с прошлым годом. В сумме за весь 2020 год было зафиксировано примерно 37.2 тыс. информационно – технологических преступлений, информация предоставлена с официального сайта МВД РФ [4].

Из этого следует, что в отчетном периоде подобных информационных преступлений было выявлено и зарегистрировано больше на 32,2 % нежели год назад. В настоящее время люди все чаще используют сеть интернет в связи с этим – рост количества составил 51,3 %, а число преступлений при помощи сотовой связи выросло на 39 %

Исходя из документов, если в январе 2020 года доля преступлений составил в сфере высоких технологий от общего числа составляла 17,7 %, то в первом месяце 2021 года она увеличилась до 25 %. Проанализировав данную статистику Минкомсвязь отметили, что в рамках федерального проекта «Информационная безопасность» учтены мероприятия, которые направлены на борьбу с киберпреступлениями. Исходя из этого, можно прийти к выводу, что в России создаётся комплекс мер по предотвращению атак в сети и ликвидации последствий после сетевых атак. А также, ведется разработка киберполигона для обучения специальных людей в этой области, а также создание национального удостоверяющего центра, сообщил «Известиям пресс» – Министр цифрового развития, связи и массовых коммуникаций Российской Федерации Шадаев Максут Игоревич.

Исходя из статистики, можно предположить, что к концу 2021 года, если не предпримут какие-либо меры для решения проблемы информационных преступлений, то количество таких правонарушений станет больше примерно в 20 раз.

На сегодняшний день государство для решения проблемы преступности в интернет сети издало множество нормативных актов которое направлено на снижение преступлений в киберпространстве.

Рассматривая проблемы информационного права, которые делит информационные правоотношения на регулятивные и охранительные. Регулятивные – определяют дозволенность работы с информацией, например поиск или распространение. Охранительные правоотношения связаны с преступлениями, которые совершенны при работе с информацией. Помимо этих двух типов существует деление на материальные и процедурные правоотношения. Материальные информационные правоотношения складываются по поводу реализации прав и обязанностей субъектов данных отношений. Процедурные информационные правоотношения складываются по поводу процедуры их возникновения, изменения или прекращения. Рассмотрим примеры субъектов и объектов правоотношений.

Субъектами информационных отношений являются физические и юридические лица, а также прочие объединения, которые могут быть носителями предусмотренных информационным законодательством прав и обязанностей.

Объектами являются все виды информации, по которым у субъектов может возникать спор.

Изучая проблему безопасности необходимо выяснить, какие способы защиты за исключением правовой существуют.

Техническая защита информации: защита информации, заключающаяся в использовании методов обеспечения безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Физическая защита информации: способы защиты информации, при котором используются организационные мероприятия и совокупность средств, создающих препятствия для проникновения или доступа посторонних физических лиц к объекту защиты. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

Таким образом, рассмотрев все множество видов, признаков и особенностей, можно прийти к выводу, что данный сегмент жизни каждого человека, является одним из самых распространённых способов «вытянуть» из него информацию, а также предоставляет преступнику незаконно завладеть денежными средствами незащищённых от сетевых или технических атак граждан. А органам внутренних дел необходимо развивать правотворчество в этой сфере, и направлять силы для предотвращения возможности совершения таких преступлений.

Список источников

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ ред. от 04.02.2021 Доступ из справ.-правовой системы «КонсультантПлюс».
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ ред. от 24.02.2021. Доступ из справ.-правовой системы «КонсультантПлюс».
3. Постановление Правительства РФ от 15.04.2014 № 313 ред. от 16.12.2020 «Об утверждении государственной программы Российской Федерации» «Информационное общество» (с изм. и доп., вступ. в силу с 26.12.2020). Доступ из справ.-правовой системы «КонсультантПлюс».
4. Краткая характеристика состояния преступности в Российской Федерации за январь-июнь 2021 года [Электронный ресурс] https://мвд.рф/reports/item/25094008/ (дата обращения 21.07.2021)