

Секция «Юриспруденция»

Криминалистические и превентивные меры борьбы с преступлениями в сфере компьютерной информации

Васильева Ольга Ильинична

Студент

*Северо-Восточный федеральный университет им. М.К. Аммосова, юридический,
Якутск, Россия*

E-mail: joakuin1@yandex.ru

В связи с переходом общества к информационному, законодатель успешно не может вести борьбу с преступлениями в сфере компьютерной информации. Данная проблема в РФ не только не выдвигалась на первый план научных исследований, но фактически игнорировалась. Подход исследователей и позиция игнорирования законодателя неоправданна в условиях совершенствующихся инфоркоммуникационных технологий.

В результате научного исследования мы разработали криминалистические и превентивные меры борьбы с преступлениями в сфере компьютерной информации: 1) правовые; 2) общепрофилактические. I. Рекомендуем правовые меры: 1) Действующий УК РФ нуждается во внесении тотальных изменений касаясь преступлений в сфере компьютерной информации в целом, так и в частности криминализации нового состава преступления в УК РФ как «кибертерроризм», что представляет новизну сферы правового регулирования и сможет совершенствовать теоретические основы. Рассматривая кибертерроризм как составляющую часть компьютерной преступности с помощью которого совершается террористическая деятельность, представляется целесообразным закрепить приведенное определение «кибертерроризм» на уровне ФЗ, а именно в ст. 3 ФЗ «О противодействии терроризму» от 06.03.2006 г. 35-ФЗ. 2) В целях единообразия правоприменительной практики и точности понятийного аппарата представляются разумными предложения о внесении дополнений в ст. 205, ст. 207, 208, 210, 215, 2151, 2152, 2153 и 217 УК РФ. 3) Необходимо квалифицировать кибертерроризм как и преступление против общественной безопасности и общественного порядка. Так ч. 2 ст. 205 УК РФ целесообразно дополнить пунктом «г» следующего содержания: «Те же деяния, совершенные с использованием ЭВМ, информационных систем и телекоммуникационных сетей, связанных с критическими элементами инфраструктуры». 4) Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран, например, сближение уголовного законодательства стран ЕС в части экстрадиции хакеров. 5) Отсутствие Постановлений Верховного Суда РФ по уголовным делам о данных преступлениях создает коллапс при применении уголовного закона органами предварительного следствия и судами. 6) Рекомендуем законодателю широко толковать состав ч. 1 ст. 272 УК РФ: «неправомерный доступ к компьютерной информации - это несанкционированное незаконным пользователем информации проникновение к ней, в том числе с возможностью ознакомления, которое позволяет распоряжаться этой информацией, создающее опасность разглашения в корыстных целях незаконного пользователя, как для самой информации, так и для интересов собственника, иного законного пользователя». Тем самым материальную конструкцию состава ст. 272 УК РФ предлагается сделать формально-материальной, т.е. просмотр информации, предназначенной для личного пользования, должен тщательно охраняться законом, не до-

пускакая нарушения конституционных прав граждан о защите от вторжения в частную жизнь и сбора данной информации.7)В связи с злободневной проблемой взлома электронной почты мы рекомендуем законодателю дополнить ст. 138 УК РФ о нарушении тайны переписки граждан квалифицирующим признаком «нарушение тайны переписки через несанкционированный доступ с помощью ЭВМ к личным электронным ресурсам граждан, осуществляющих личную электронную переписку через Интернет».8) 9)Рекомендуем ввести новую санкцию в ст.ст. 272-273 УК РФ – конфискацию имущества.10)Санкции ч. 1 ст. 272 УК РФ рекомендуем ужесточить и применять меру наказания с отменой назначения условного осуждения, назначив основным наказанием - лишение свободы с выплатой денежного штрафа в размере причиненного ущерба, что полностью исключит проблему ссылки компьютерного преступника на свою материальную несостоятельность выплатить штраф.11)Ввести дополнительное наказание - ограничение к доступу пользования персональным компьютером или другими ЭВМ после отбывания основного срока. 12) Рекомендуем дополнить содержание п. «б» ч. 2 ст. 158 и статей 159, 160, 163 УК РФ, квалифицирующим признаком «с использованием ЭВМ, системы ЭВМ или их сетей». Это особо актуально в эпоху информатизации при электронном оформлении кредитов.13)Для отбывания срока лишения свободы хакеров, рекомендуем выделить финансирование из бюджета РФ на строительство специализированной тюрьмы, где они будут разрабатывать программы и меры защиты по борьбе с вредоносными программами для ЭВМ. Тем самым хакеры могут заработать себе досрочное освобождение как за примерное поведение и исправление.14)Важным направлением в борьбе с данными преступлениями станет развитие правового фундамента в сфере Интернета путем принятия ФЗ «О правовом регулировании использования сети Интернет».II.Рекомендуем общепрофилактические меры:1)В целях профилактики проводить мероприятия по предупреждению данных преступлений на федеральном, региональном уровне и МСУ в целях преодоления правового нигилизма руководителей организаций, отдельных граждан и угрозы роста латентной преступности в сфере высоких технологий.2)Повысить уровень доверия населения к уголовной юстиции в целях обеспечения законности функционирования ее системы.3)Создание абсолютной защиты компьютерной информации, разработанной сотрудниками управления «К» МВД РФ по типу антивирусной программы, содержащей в себе механизм самопрогрессирования и распознавания, уничтожения компьютерных вирусов и червей поднимет на новый уровень борьбу с компьютерной преступностью.4)Рекомендуем разработать сайт доверия МВД РФ, концентрирующий информацию о готовящихся или проведенных хакерских нападениях, информации о несанкционированных доступах в информационные сети ЭВМ.6)Необходимо создать этический кодекс компьютерного сообщества, закрепивший нормы обращения с компьютерной информацией, сформировал основы корпоративной морали и информационной ответственности организаций, отдельных граждан.

Литература:

- 1.Вехов В.Б.,Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации. - М.: ИМЦ ГУК МВД РФ, 2002.
- 2.Генпрокуратура РФ и Управление «К» МВД РФ. «Раскрытие преступлений информации с использование информационных технологий». - М., 2005. - 1-20 с.
- 3.Яблоков Н.П. Криминалистика: Учебник / М.: МГУ, Юристь, 2001.