***А. А. Синельникова,***
***А. А. Ульянов***
*Научный руководитель*
***В. А. Одинцов***
*Белорусский торгово-экономический*
*университет потребительской кооперации*
*г. Гомель, Республика Беларусь*

## ПРАВОНАРУШЕНИЯ В ИНТЕРНЕТЕ

Интернет (англ. Internet (Interconnected Networks) – объединенные сети) – всемирная система объединенных компьютерных сетей для хранения и передачи информации.

По заказу Министерства обороны США Агентство по перспективным оборонным научно-исследовательским разработкам США (DARPA) предложило разработать компьютерную сеть, состоящую из взаимозаменяемых сегментов без ярко выраженного центра, который не возможно было бы вывести из строя в случае ядерной войны. В 22 ч 30 мин 29 октября 1969 г. между двумя первыми узлами сети ARPANET, находящимися на расстоянии в 640 км (в Калифорнийском университете Лос-Анджелеса (UCLA) и Стэндфордском исследовательском институте (SRI)), удалось провести успешный сеанс связи. Этот день можно считать днем рождения Интернета. По оценкам Международного союза электросвязи, к концу 2013 г. количество пользователей Интернета должно было достичь 2,7 млрд чел., или 39% населения планеты.

С появлением Интернета зарождается и новый вид преступности – интернет-преступность, т. е. совершение преступлений посредством или при помощи Интернета.

В 70-х гг. XX в. появляется термин «хакер» – компьютерный преступник, в том числе и интернет-преступник. Именно тогда первый профессиональный взломщик удаленных телефонных коммуникаций Джон Дрэйпер создал первую специализацию хакеров – фрикеры (телефонный хакер). Он не только разработал устройство, позволяющее делать бесплатные звонки, в том числе международные и междугородние, но и опубликовал статью в журнале с описанием алгоритма его изготовления.

В 1983 г. в США в штате Милуоки произошел первый арест интернет-преступников, когда группа из шести подростков в течение девяти дней взломала 60 компьютеров, в том числе Лос-Аламосской государственной лаборатории (место исследования ядерного оружия), получив за это условный срок.

В 1984 г. Фред Коэн опубликовал сведения о разработке первых вредоносных саморазмножающихся компьютерных программ и применил к ним термин «компьютерный вирус».

В 1986 г. в Пакистане двумя программистами с целью защиты от несанкционированного копирования их продуктов создается первый свободно распространяющийся вирус для персональных компьютеров «Мозг», заражающий посредством дискет, и только через два года появляется первая антивирусная программа.

В 1994 г. интернет-преступность выходит на мировую арену, когда возникает дело Владимира Левина, отнесенное к категории транснациональных сетевых компьютерных преступлений. Международная организованная преступная группа из 12 чел., используя Интернет и сеть передачи данных «Спринт/Теленет», преодолев защиту от несанкционированного доступа, попыталась осуществить 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 долл. США со счетов клиентов банка, находящихся в 9 странах мира, на счета, расположенные в США, Финляндии, Израиле, Швейцарии, Германии, России, Нидерландах. Но после похищения только 400 тыс. долл. США их преступная деятельность была пресечена.

Последующее развитие информационных технологий приводит к появлению таких понятий, как интернет-терроризм, интернет-забастовка и интернет-война.

В 1998 г. 12-летний хакер проник в компьютерную систему, которая контролировала водоспуск плотины Теодора Рузвельта в Аризоне. В случае открытия сливных ворот вода могла затопить города Темп и Месэ с общей численностью населения в 1 млн чел. Находись на его месте член террористической группировки, последствия были бы ужасны.

Первую интернет-забастовку провела группа «Страно Нетворк», протестовавшая против политики французского правительства в вопросах ядерных программ и социальной сферы. В течение часа 21 декабря 1995 г. эта группа с разных континентов атаковала различные сайты правительственных агентств путем одновременного входа на правительственные сайты с целью их перегрузки.

Первой интернет-войной считается конфликт в Косово, когда Интернет использовали для осуждения военных действий противника и формирования собственного положительного облика как Югославия, так и страны НАТО при помощи умышленного нарушения работы правительственных компьютеров и получения контроля над сайтами с последующим изменением содержимого – «дефейса». В настоящее время ни один военный или политический конфликт не обходится без организованного противоборства в Интернете.

Можно уверенно утверждать, что к настоящему времени преступность в Интернете приобрела транснациональный характер, не знает государственных границ, имеет тенденции к преобладанию над другими видами преступности и в будущем будет существенно влиять на экономические и политические процессы.

Официально зафиксирован даже факт убийства, которое было совершено посредством Интернета в феврале 1998 г. в США. Тяжелораненый свидетель преступления был спрятан в закрытом госпитале на территории военной базы, и преступники через Интернет изменили режим работы кардиостимулятора и аппарата вентиляции легких, что привело к его смерти.

В настоящее время можно выделить несколько основных групп интернет-преступлений: распространение вредоносных вирусов, взлом паролей, кража номеров кредитных карточек и других банковских реквизитов (фишинг), мошенничество и др. Жертвами этих преступлений одновременно становятся сотни тысяч людей, а ущерб составляет миллионы долларов США.

В Республике Беларусь широко распространены в Интернете мошенничества с предложением перечислить небольшие суммы (200–500 долл. США) в качестве регистрации, налога, необходимые для получения выигрыша по различным лотереям на крупную сумму денег и т. п. Во многом способствует этому и сама личность жертвы, легко заглатывающая «наживку» в виде обещаний скорого обогащения.

Большое количество правонарушений в Интернете происходит в сфере авторских прав, в связи с чем правообладатели терпят убытки на сотни миллионов долларов США.

В отдельную главу Уголовного кодекса Республики Беларусь (далее – УК) выделены преступления против информационной безопасности, т. е. преступления, прямо связанные с использованием информационных технологий, сетей и систем. При наступлении определенных законом последствий предусмотрена уголовная ответственность за несанкционированный доступ к информации (ст. 349 УК), ее модификацию (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработку, использование либо распространение вредоносных программ (ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК). Следует знать, что на первый взгляд невинная шутка (к примеру, подбор пароля к электронному ящику или аккаунту в социальной сети) уже влечет административную ответственность в виде штрафа в размере от 20 до 50 базовых величин.

Особое место в интернет-преступности занимают преступления, направленные против чести и достоинства, конституционных прав и свобод человека и гражданина, общественной нравственности. В Республике Беларусь довольно совершенная правовая база в данной области и ведется соответствующая работа в данном направлении. Так, был возбужден ряд уголовных дел по ст. 343 УК (изготовление и распространение порнографических материалов или предметов порнографического характера) за размещение материалов видеозаписей порнографического характера, а также по ст. 188 УК (клевета) за распространение в Интернете клеветнической информации.

В Интернете активно предлагают скачать и воспользоваться программами для негласного контроля телефонных переговоров, содержания СМС, в результате использования которых после установки на корпоративные телефоны руководитель будет знать, о чем говорят сотрудники в рабочее время. Те, кто воспользовался подобным предложением, не учитывают, что за нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений предусмотрена уголовная ответственность.

Подводя итоги, можно отметить, что интернет-преступность – это разновидность современной преступности, имеющая такие отличительные особенности, как глобальность, неперсонифицированность, интеллектуальная природа, общедоступность, высокая латентность, быстрый рост, широкая распространенность и транснациональность.