УДК 34.09

Власенко О.Б.,
старший преподаватель кафедры
философии, политологии, социологии
им. Г.С.Арефьевой
ФГБОУ ВО «НИУ «Московский энергетический институт»
Россия, г.Москва

КИБЕРПРЕСТУПНОСТЬ КАК ВЫЗОВ СОВРЕМЕННОСТИ

Аннотация. В статье рассмотрена проблем решения задачи обеспечения безопасности от преступных деяний в сфере информационных технологий.

Раскрываются основные положения уголовного законодательства о киберпреступности, нормы уголовного законодательства о преступлениях в области компьютерной информации.

В статье вносится предложение о совершенствования уголовно-правовых норм в части дифференциации уголовной ответственности за совершение преступления с использованием информационных технологий.

Ключевые слова: киберпреступность, кибербезопасность, уголовная ответственность, компьютерная информация

Vlasenko Olga Borisovna
senior lecturer
National Research University "Moscow Power Engineering Institute",
Moscow, Russia

CYBERCRIME AS A MODERN CHALLENGE

Annotation. The article considers the problem of solving the problem of ensuring security from criminal acts in the field of information technology.

The main provisions of the criminal legislation on cybercrime, the norms of criminal legislation on crimes in the field of computer information are disclosed.

The article makes a proposal to improve criminal law norms in terms of differentiating criminal liability for committing a crime using information technology.

Keywords: cybercrime, cybersecurity, criminal liability, computer information

Одним из вызовов современности является киберпреступность. С развитием технологий население сталкиваемся с новыми угрозами, такими как киберпреступность и незащищенность личных данных россиян. Чтобы успешно противостоять этим угрозам, необходимо развивать нашу цифровую инфраструктуру и обеспечивать защиту персональных данных наших граждан.

Развитие общества в настоящий период связано с цифровизацией практически всех сфер жизнедеятельности. В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы отмечается, что информационные системы, социальные сети стали частью повседневной жизни россиян. Пользователями сети «Интернет» в России стали более 80 млн. человек [1].

Киберпреступность определяется как преступление, когда компьютер является объектом преступления или используется в качестве основного инструмента для совершения преступления [2].

Ущерб от киберпреступлений в России с начала текущего года превысил 116 миллиардов рублей, сообщил глава МВД РФ Владимир Колокольцев.

За последние пять лет число противоправных деяний в киберпространстве увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и составляет около 40%. А по тяжким и особо тяжким составам этот показатель уже приблизился к 60%", - сказал Колокольцев на заседании Общественного совета при МВД РФ.

В МВД есть специализированные подразделения по борьбе с преступлениями в сфере информационно-телекоммуникационных технологий.

По данным Генеральной прокуратуры РФ, киберпреступления, в том числе телефонные и онлайн-мошенничества, составили треть всех преступлений, которые были зарегистрированы в России. Главная проблема – это незащищенность персональных данных россиян [3].

Ежесуточно россиянам звонят по 6 млн. раз с целью кражи из средств, число кибер-преступлений все время растет. Причина этого — низкая цифровая грамотность россиян считают аналитики.

Полиция борется с киберпреступностью не только при расследовании уголовных дел, но и с помощью законодательных новелл и образовательных программ для следователей, сообщил Министр внутренних дел РФ на заседании Общественного совета при МВД России.

Одним из важных инструментов в борьбе с преступлениями в сфере компьютерной информации является их профилактика, повышение цифровой грамотности населения.

К преступным деяниям в сфере IT в настоящее время относятся:

- кража онлайн-личности, таковая возникает в тех случаях, когда преступник получает доступ к персональной информации пользователя, чтобы украсть его деньги, получить доступ к другой конфиденциальной информации или осуществить различные мошеннические аферы;

- социальная инженерия, которая предполагает вступление преступника в прямой контакт с гражданином, как правило, по телефону или электронной почте;

- незаконный контент, когда злоумышленники распространяют неприемлемый контент, который может считаться крайне неприятным и оскорбительным;

- онлайн-мошенничество, которое начинается с рекламы или спама, обещающих вознаграждение или предлагающих нереальные суммы денег.

В России правовая основа борьбы с киберпреступлениями впервые появилась с принятием Уголовного кодекса РФ, в котором появилась глава 28 «Преступления в сфере компьютерной информации»,

В российском законодательстве при характеристике виртуального пространства и высоких технологий используются такие прилагательные как «цифровое», «информационное». Наряду с термином «киберпреступления», используются такие категории как: «преступления в сфере информационных технологий» —«информационные преступления», сетевые компьютерные преступления, интернет-преступления. Глава 28 УК РФ «Преступления в сфере компьютерной информации», включает в себя пять статей с 272 по 274.2 УК РФ: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру РФ; нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования. Также к компьютерным преступлениям относят мошенничество в сфере компьютерной информации [4].

В заключение, можно сделать вывод, что на современном этапе развития информационного общества киберпреступления необходимо рассматривать как умышленные деяния, совершаемые с использованием IT-технологий. К киберпреступлениям относятся специальные кибер-преступления и общеуголовные киберпреступления. Специальные киберпреступления - это преступления в сфере компьютерной информации. Общеуголовные киберпреступления - это иные

преступления, совершаемые с использованием высоких технологий. К ним относятся преступления, в составе которых присутствует в качестве квалифицирующего признак совершения деяния с использованием информационно-телекоммуникационных сетей, а также преступления, составы которых в качестве предмета преступления называют, электронные носители информации. В целях дифференциации уголовной ответственности предлагается включить во все составы общеуголовных преступлений, которые могут быть совершены посредством высоких технологий, квалифицирующий признак: совершение преступного деяния с использованием электронных или информационно-телекоммуникационных сетей.

Использованные источники:

1. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.05.2017.
2. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 06.12.2016.
3. Приказ Генпрокуратуры России от 14 сентября 2017 г. N 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // Законность. 2017. № 12.
4. Виды киберпреступлений по российскому уголовному законодательству. Иванова Лилия Викторовна, статья из рубрики "Уголовный закон и правопорядок ", cyberleninka.ru