

Короткова Ольга Валерьевна, канд. юрид. наук, старший преподаватель

Московская академия следственного комитета, Россия, г. Москва

О НЕОБХОДИМОСТИ УСИЛЕНИЯ МЕР ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В «КИБЕРПРОСТРАНСТВЕ» В УСЛОВИЯХ (COVID-19)

Аннотация: В статье анализируется появление новых видов противоправной деятельности в условиях пандемии в Российской Федерации и за рубежом. Подчеркивается увеличение масштабов преступлений в сфере онлайн. Делаются необходимые выводы о важности разработки новых и усиления, имеющихся мер противодействия преступлениям в «киберпространстве» в условиях самоизоляции.

Ключевые слова: «киберпространство»; сфера онлайн; пандемия; меры противодействия; безопасность.

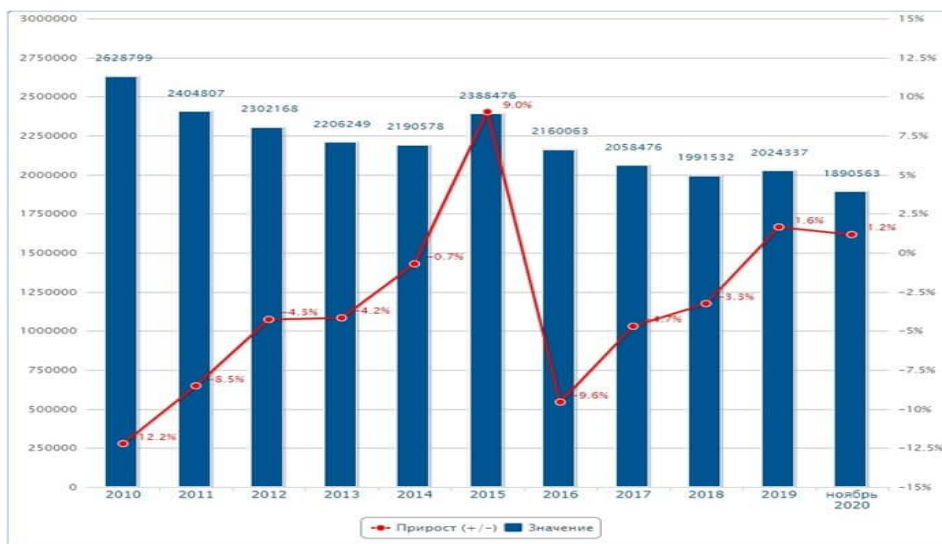
Abstract: The article analyzes the emergence of new types of illegal activities in the context of the pandemic in the Russian Federation and abroad. Highlights the increasing incidence of crimes in the sphere of online. The necessary conclusions are drawn about the importance of developing new and strengthening existing measures to counter crimes in «cyberspace» in conditions of self-isolation.

Keywords: «cyberspace»; online sphere; pandemic; countermeasures; security.

Распространение коронавирусной инфекции (COVID-19), охватившей весь мир, вызвало небывалый всплеск преступности, открыв ей новые возможности, способы и виды совершения противоправных действий. В Российской Федерации (РФ) в 2020 году, согласно данным Генпрокуратуры РФ, в 55 из 80 регионов был зафиксирован резкий всплеск преступности. И

хотя на сегодняшний день цифра прироста не велика-всего 1,3%, но в масштабах нашей страны она достаточно значительна (см. Таблицу 1).

Таблица 1. Рост преступности за период с 2010 по 2020 годы



Согласно материалам Генпрокуратуры РФ, более 60 тыс. человек пострадало в 2020 году от рук преступников, из них 22 тыс. было убито. В целом по нашей стране было совершено на 2,3 млн. преступлений подобного рода больше, чем в 2019 году. И это показательно, в силу того, что в условиях пандемии, в условиях резкого экономического спада, немалое количество россиян потеряло работу, произошло падение уровня жизни населения как в центре, так и в регионах РФ.

Важно тот факт, что в условиях самоизоляции, в связи с введенными в государстве ограничениями (карантином), впервые был выявлен резкий рост преступного использования онлайн пространства в целях совершения целого ряда мошеннических операций в ущерб экономической безопасности РФ. Так, увеличилось количество объектов преступных посягательств, а также возросла латентность совершаемых преступлений, которые можно отнести к такому виду преступлений как «киберпреступления».

Особо следует отметить, что в рамках данного явления следует рассматривать как известные виды так называемых «классических»

преступлений, которые совершаются в системе «киберпространства», так и относительно новые виды, затрагивающие преступное проникновение в работу чужих компьютерных систем, а также иные незаконные действия, совершаемые при помощи компьютеров, информационных сетей и компьютерных программ. Так, в своих работах правовед Т. Хусяинов, к подобному роду преступлений в «киберпространстве» относит такие виды как: незаконное вмешательство в компьютерные системы; противоправный доступ к конфиденциальной информации; незаконное вмешательство в данные как физических, так и юридических лиц [3].

Со своей стороны, М. Батухтин в своих работах к особым видам преступлений в «киберпространстве» относит любые виды незаконного вторжения в электронную сферу, совершаемого посредством компьютерных средств в виртуальной среде [1].

Правовед-международник Р. Дремлюга смело утверждает, что преступления в «киберпространстве» превратились в доходный бизнес, размеры доходов которого в несколько раз больше выручки от незаконной торговли наркотиками, оружием и другими иными видами криминальных доходов [2].

Проанализировав различные подходы к определению преступлений в «киберпространстве», можно смело утверждать, что под «киберпреступлением» можно понимать совершенное посредством информационных технологий любое противоправное действие в сетевом пространстве. Полагаем, что особенности специфики выбора места совершения преступления обусловлена необходимостью применения «онлайн инструментов» сегодняшнего дня, а именно новейших информационных технологий в условиях (COVID-19).

Безусловно, преступления в «киберпространстве» сегодня являются проблемой для населения всего земного шара. Подобного плана преступления развиваются одновременно с развитием сетевых коммуникационных технологий. Более того, внедрение и использование подобных видов противоправных действий развивается быстрее именно в латентной преступной

среде, а не в правоохранительной сфере государства, что затрудняет разработку профилактических средств противодействия данному явлению, осложняет процессы их своевременного выявления и пресечения.

Важно подчеркнуть, что по данным «*The Norton Cyber Security Insights Report*» за 2020 год 1285 млн человек в 22 государствах мира пострадали от киберпреступлений, а именно 42 % из опрошенных стали жертвами вброшенных вирусов в программу компьютера; у 20 % хакеры выкрали пароли от электронных кошельков и 19 % стали жертвой мошенничества с кредитными банковскими картами [3].

Что касается роста подобного вида преступлений в нашей стране, то согласно данным статистических отчетов Генеральной прокуратуры РФ, в 2020 году было выявлено 98 678 преступлений в «киберпространстве», что на 41 % выше 2019 года и составляет 5,4 % от общего количества выявленных преступлений в 2020 году (каждое 15-е).

Ряд отечественных исследователей выделяет основные факторы, определяющие возрастающую с каждым годом международную общественную опасность преступлений в «киберпространстве», а именно: галопирующую масштабность; возрастающую латентность; невозможность возмещения ущерба; проблему выявления преступников; широкий круг пользователей-распространителей информации [4]. Так, по итогам 2020 года глобальная численность пользователей интернета составила более 5,8 млрд. человек.

Сложившаяся обстановка в мире осложняется появлением и развитием новейших видов угроз в кибернетической сфере государств, а именно: масштабным распространением «спама»; преступным проникновением на сайты, содержащие, в том числе, личную информацию пользователей; полнейшую бесконтрольность обращаемой информации криминального характера и иное.

Более того, сама проблема уточнения границ киберпространства и его специфики требует сегодня отдельного рассмотрения и исследования.

Со своей стороны, исходя из сложившейся ситуации, полагаем, что при разработке мер пресечения подобного плана преступлений необходимо в кратчайшие сроки тщательно разработать меры профилактического характера по их раннему предупреждению; оптимизировать уголовно-правовые подходы; усилить уголовно-правовую политику; разработать комплекс специальных мер организационно-технического характера в условиях возможных новых всплесков пандемии; усилить процессы межведомственного взаимодействия правоохранительных структур на международном уровне.

Библиографический список:

1. Батухтин М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2019.

2. Дремлюга Р. И. Интернет–преступность: моногр. Владивосток, 2008.

3. Хусяинов Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования материалы всероссийского круглого стола. 2018.

4. Шидловский А. В., Цветков А.Н. Установление уголовной ответственности за киберпреступления – новый сегмент в правовой охране электронного государства // Сборник материалов VI Международной науч.-практ. конф. 2019.