**Что для виртуального мира закон?**

**А. П. Афонина,**

*студент Юридической школы ДВФУ,*

*научный руководитель –*

*Кандидат юридических наук, доцент*

*Д. В. Лобач*

Актуальность данной статьи обусловлена тем, что технологии современного мира заставляют человека переместить поле своей деятельности из реального пространства в виртуальное. Проблема заключается в том, что виртуальная реальность, как и любое глобальное событие в сфере социальной жизни, является большой проблемой для её регулирования.

Как и в реальном мире, с точки зрения правоохранительной деятельности, люди делятся на: тех, кто имеет права и несет юридические обязанности и на тех, кто нарушает эти права. С правонарушителями в реальном мире проще, ведь есть четкий алгоритм действий. Грубо говоря, выявить нарушения и наказать правонарушителя по реальным законам. Что же происходит в виртуальном мире? Как ловить нарушителя? Руководствуясь какими законам, вынести наказание? Которых нет?

И несмотря на то, что популярность различных виртуальных сообществ значительно возросла за последнее десятилетие, юридическое сообщество мало что предложило для решения вопроса о правилах, регулирующих эти цифровые миры. В то время, как главный мотив притягивающие к себе толпы поклонников многих из этих миров – представление или изображение образа жизни, который сильно отличается от происходящего в настоящем (например, фантастические или фантазийные вселенные, где как немаловажная часть сюжета, беспроблемно присутствуют все формы жестокости и насилия), это не является причиной для беспокойства. И конечно же мотив для совершения преступления. Ведь нет ни законодательной базы для разрешения таких отношений, ни управомоченного органа. Основной вопрос возникает тогда, когда человек способен «украсть» в виртуальном мире что-то, что можно обменять на настоящие деньги. Например, в некоторых виртуальных мирах пользователи проводят часы, создавая виртуальные вещи или улучшая характеристики персонажа, которые они затем намерены продать другим пользователям за фактическое, реальное денежное вознаграждение. Однако, если злоумышленник украдет каким-либо методом эти предметы, «взломав» учетную записи с помощью сторонних программ или даже с помощью способов явно незапрещенных в виртуальном сообществе, а затем кому-то перепродаст, можно ли это считать кражей, подсудной законам настоящего мира?

Вне зависимости от цели создания, любое сообщество, в котором люди взаимодействуют друг с другом, потенциально являться причиной противоречий и конфликтов интересов. Это дает повод задаться вопросом, возможно ли законы реального мира применить для решения проблем или преступлений в виртуальном.

Разберем понятия виртуальная реальность. Она представляет собой созданный техническими средствами мир, передаваемый человеку через его ощущения и имитацию физического воздействия [1]. Но упор будет вестись над киберпространством, а не само виртуальной реальности и дополненной реальности. Потому что, виртуальное пространство имеет боле общего с играми «от первого лица» и подобными вещами, где человека погружают в другую реальность, говоря о киберпространстве, я подразумеваю пространство, охватывающее отношения людей в цифровой системе Интернет.

1. *Гаврилов, А.А. Основные подходы к определению категории «виртуальная реальность» в современном философском дискурсе / А.А. Гаврилов // Молодой ученый – 2012, №9.– С.162*

И дополненную реальность реально регулировать и осуществлять контроль, потому что, не существует отдельно, а вместе с реальным миром. Примером может стать, тот же случай нарушения, который связан с игрой «Pokémon Go», где блогера Руслана Соколовского приговорили к условному сроку за ловлю покемонов в храме. «Pokémon Go» в течение 10 дней стала причиной 14 автокатастроф – это всё являет лишь подтверждением, что не нормативной базы для регулирования и органа для контроля. Под киберпространством следует понимать термин, иногда смешиваемый с виртуальной реальностью, которой обозначает пространство, которое симулируется и опосредуется электронными устройствами.

Именно в цифровой сети Интернет происходит те вещи, которые требует особого контроля и регулирования, именуемые киберпреступлениями.

Для того, чтобы понять реальную ситуацию на сегодняшний день, а также и актуальность, проанализируем статистику, предоставленную «Адвокатской газетой». Ведь без актуальной статистики тяжело понимать для чего рассматривается та или иная тема. Эксперты «АГ» выявили самые популярные составы киберпреступлений, дали рекомендации по их выявлению и рассказали о тонкостях квалификации. Специалисты обратили внимание на неутешительную статистику раскрываемости, единогласно назвав в качестве одной из ее причин неподготовленность кадров в правоохранительных органах. Эксперты сошлись во мнении, что число киберпреступлений в будущем будет лишь возрастать, поскольку злоумышленники быстро адаптируют современные технологии, чтобы повысить свою эффективность.

Согласно [отчету](https://genproc.gov.ru/smi/news/genproc/news-1431104/), опубликованному Генпрокуратурой, и расширенным данным, которые были предоставлены ведомством по просьбе «АГ», в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 37% (с 65 949 в 2016 г. до 90 587 в 2017 г.). При этом доля таких преступлений от числа всех зарегистрированных в России составляет 4,4%: это почти каждое 20-е преступление [2].

Коротко, про виды киберпреступлений:

- Фишинг. Заражение компьютеров ничего не подозревающих жертв.

- Кибервымогательство. Как правило, вначале у пользователя или компании, после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграждение (обычно в виде биткоинов или другой криптовалюты). Так как государственные денежные знаки можно отследить, а криптовалюту отследить сложно.

- Финансовое мошенничество. Взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией. Киберпреступления, связанные со вторжением в личную жизнь

- Кража персональных данных. Например, некто, желающий получить банковский заем, может украсть персональную информацию человека с хорошей кредитной историей.

- Шпионаж. Целью шпионажа, начиная от взломов индивидуальных компьютеров или устройств и заканчивая нелегальной массовой слежкой, является тайное отслеживание нашей личной жизни. Здесь может быть как физический шпионаж (например, при помощи веб- или CCTV-камер для наблюдения за отдельными персонами или группой людей), так и массовый

1. *«Адвокатская Газета» - Киберпреступлений становится все больше, однако их раскрываемость уменьшается. [Электронный источник]. -* [*https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/*](https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/)

мониторинг различного рода коммуникаций (чтение почты, текстовых сообщений мессенджеров, смс и так далее).

- Спам. Сюда входит массовая рассылка по электронной почте, смс,

мессенджерам и другим каналам коммуникации. Любую рассылку без согласия получателей можно отнести к спаму.

- Нарушение авторского права. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.

- Кибербуллинг. Некоторые формы кибербуллинга (например, вброс обнаженных фотографий) могут подпадать под незаконные действия (например, эксплуатация детей).

- Противозаконная порнография. В Российской Федерации она запрещена [3].

А теперь о реальных проблемах. Ведь теория — это конечно весело, но многие любят практику поэтому посмотрим на то, что студенты первого курса Юридической школы знают о киберпреступлениях.

Был проведен опрос, число участников составило 53 человека. По результатам исследования, 30 из 53 знают, то является киберпреступлением, но остальные сомневаются, что составляет почти 44%. 64% предположительно являлось жертвами фишига. 29 станиц взламывали, а значи, что они также предположительно являлись жертвами шпионажа или же похищения личной информации. Более 71% получали спам на почту. Страшно представить, но 9 человек подвергались кибербуллингу. Понятное дело, что в реальном мире эта проблема предположительно закончилась походом в полицию, но в случае с

1. *Статья «КИБЕРПРЕСТУПЛЕНИЯ: понятие, виды и методы защиты». – Центр обучения IT. – [Электронный ресурс]. - https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html*

киберпространством, некоторые даже не пытались сообщить. Но наши участники, возможно и не подозревают, что являлись или являются нарушителями.

Например, почти 82% слушают музыку без подписки, кто-то делится, что также нарушает авторское право. Больше половины смотрели фильмы на сайтах, не имеющих необходимую лицензию, и из низ есть люди, которые делились ссылкой источника с товарищами, что является нарушением авторских прав. Той же сериал «Игра Престолов» запрещена в Российской Федерации, но это никого не останавливает. Около 65% являлись/являются пользователями порносайтов, потому что система работает настолько плохо, что блокировки этих сайтов происходит не очень активно. Но при всём вышесказанном, 10 человек остерегаясь слежки с веб-камер, заклеивают её. Никто не хочет быть объектом шпионажа. Самый интересный вопрос, пожалуй, о том, знают ли участники о наказаниях за вышесказанные киберпреступления? 40% не имеют понятия, чем это пространство регулируется, большинство считает, что за это отвечает Уголовный Кодекс Российской Федерации, что в сегодняшних реалиях имеет суть.

Как с этим справляются другие страны? Многие, ссылаются на виртуальной договор о предоставлении услуг или Лицензионное соглашение пользователя (End User License Agreement, сокр. EULA). В некоторых странах начала действовать киберполиция и уже стала давать положительные результаты. Например, в Украине всего за 2018 год подразделение выявило около 6000 преступлений в сфере использования высоких информационных технологий. Среди успешных операций - задержание организатора бот-сети Avalanche, разоблачения участника международной хакерской группировки

1. *Лига. Tech. – «2018: Киберполиция выявила 1000 преступлений по кибербезопасности». – [Электронный ресурс]. - https://tech.liga.net/technology/novosti/2018-kiberpolitsiya-vyyavila-1000-prestupleniy-po-kiberbezopasnosti*

Cobalt, участие в прекращении деятельности международной хакерской группы FIN7.

Подводя итоги, стало понятно, что проблема киберпреступлений в виртуальном мире поставлена очень остро и страшно представить, что будет через пару десятков лет, если всё пустить на произвол судьбы. До этого времени, пользователям не следует полагаться на свои собственные суждения и стараться избегать потенциально опасных ситуаций или действий мошенников, и следовать правилам, изложенным в Лицензионном соглашении. Если что-то противоправное произойдет в виртуальном мире, лучшим способом попытаться решить проблему – это спрашивать с администрации, отвечающую за поведение пользователей в этом сообществе, а не обращаться с иском в суд.