Студент магистратуры Ивановского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

Научный руководитель: С. К. Редков, доцент кафедры конституционного и муниципального права Ивановского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

К вопросу о понятии и причинах возникновения киберпреступлений в Российской Федерации

Е. В. Михайленкова

В данной статье рассматривается актуальная проблема современного мира – киберпреступность. Автор анализирует отечественные и зарубежные подходы к определению понятия «киберпреступность», и на основе проведенного анализа предлагает авторское определение. Далее автор приводит перечень причин развития киберпреступлений, а также предлагает пути решения для устранения условий развития киберпреступлений.

Ключевые слова: личность, киберпреступность, информационные технологии, цифровизация, прогресс.

С появлением новых технологий и развитием поставщиков интрасетей все чаще граждане погружаются в виртуальные среды. Это означает: чем больше появляется новых возможностей, тем больше вероятность того, что каждый из нас столкнется с новыми проблемами, особенно с мошенничеством в сети Интернет.

«В отечественной и зарубежной литературе подходы к определению понятия киберпреступления разнятся, ввиду отличительной черты данного вида правонарушений, а именно в том, является ли компьютер целью правонарушения или же средством для совершения преступных деяний» [5, с. 18].

«Энциклопедия «Britannica» киберпреступлением, которое, так же может быть названо компьютерным преступлением определяет использование компьютера, как инструмент для совершения противоправных действий, как кража, распространение порнографии или нарушение прав интеллектуальной собственности» [6].

В отечественной литературе Т.Л. Тропина дает следующее определение киберпреступности – «это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных» [3, с. 219].

Стоит отметить, что в законодательстве Российской Федерации отсутствует понятие «киберпреступность», однако, упоминается понятие «информационная безопасность». Под информационной безопасностью законодатель предлагает понимать «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека, и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [4].

По нашему мнению, определение «информационная безопасность» намного

шире, чем понятие «киберпреступность» и соответственно, представляется необходимым дать авторское определение «киберпреступности – это совокупность преступных деяний, осуществляемых в виртуальной среде с использованием компьютерных систем или сетей, а также других средств доступа к интернету, направленных против компьютерных систем и любых данных, которые на нем хранятся».

На данный момент, в условиях постоянного прогресса и цифровизации, государство обязано защищать граждан и их личную информацию, персональные данные от мошенничества и других преступлений в сети Интернет, однако, так как киберпреступления имеют латентных характер, государству не удается защитить граждан от киберпреступлений. Например, в 2020 году «возросло число преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составило - 14 063 182» [1, с. 55].

Учитывая тот факт, что у части граждан, вся личная информация хранится на компьютерах, телефонах, а доступ к персональным данным можно получить через придуманные пароли самим пользователем, которые зачастую состоят из примитивной комбинации даты рождения или номера телефона, то государство в первую очередь должно позаботиться о сохранности данных, а также недопущении и пресечении киберпреступлений.

Также заметим, что носителем важной и ценной информации может быть не только гражданин, но и юридическое лицо, в том числе и государство. Если еще кража денежных средств с электронного кошелька гражданина, относительно небольшое преступление, по степени тяжести, то, например, кража личной информации президента страны, с целью компрометирования, очернения репутации – более серьезнее деяние.

Причинами развития киберпреступлений, на наш взгляд, являются:

1. В Российской Федерации, в связи с набравшей популярностью в 2020 году – цифровизацией, которая до сегодняшних дней имеет огромнейшее развитие, появилась активность и со стороны граждан, юридических лиц и государства цифровизировать все процессы. Безусловно за этим прогресс, однако, не было разработано достаточно надежных и защищенных средств общения, и работы в онлайн сети.

2. Данная причина исходит из предыдущей, и подразумевает низкую осведомленность и грамотность граждан, относительно методов распознавания поддельных мошеннических веб-сайтов, ссылок.

3. По аналогии из этого исходит следующая причина – отсутствие просветительской работы с гражданами, которая могла бы быть направлена на повышение грамотности и осведомленности населения в области киберпреступлений, например, каким образом они совершаются, что не надо делать в случае, если человек был подвергнут кибератаке и т.д.

4. Отсутствует увеличение активности со стороны правоохранительных органов в раскрытии киберпреступлений, это связано с недостаточным оснащением рабочих мест, а также с нехваткой квалифицированных кадров в рассматриваемой области.

5. Отсутствует необходимый контроль над действиями отдельных лиц и интернет-ресурсами, что исходит из предыдущей причины.

В частности, было предложено криминализовать новые виды деятельности киберпреступлений. Обоснованность этих предложений проистекает из увеличения их общественной угрозы в связи со значительными экономическими последствиями. Однако, как правильно отмечают представители МВД России, «введение новых составов преступлений не является необходимым, в связи с возможностью применения и внесения изменений в уже существующие статьи Уголовного кодекса РФ, для решения вопросов, связанных с новыми формами преступной деятельности в области информационно-телекоммуникационных технологий» [2].

По нашему мнению, решить сложившуюся ситуацию немедленными мерами, к сожалению, не удастся в ближайшее время. Властям не удастся мгновенно исправить ее. Однако следует понимать, что массовое переселение

значительной части населения в цифровое пространство не является временным явлением.

Исходя из этого, необходимо наметить следующие пути решения для устранения условий развития киберпреступлений, в частности:

– расширять нормативное регулирование в области кибербезопасности;
– принимать меры по улучшению работы правоохранительных органов за счет расширения деятельности, обучения и оснащения для выявления, расследования и предотвращения незаконной деятельности в этой среде;
– развивать международное сотрудничество для обмена информацией и опытом;
– проводить просветительскую работу с населением, направленную на безопасное поведение в сети Интернет.

Таким образом, стремление государства к цифровизации, отсутствие должного нормативного регулирования, а также высокая латентность подобных преступлений - порождает новые условия для киберпреступлений в сети Интернет.

Библиографический список:

1. *Денисов, Н. Л.* Тенденции современной киберпреступности / Н.Л. Денисов // Legal Bulletin. – 2020. – №2. – С. 55-60.
2. МВД выступило против уголовной ответственности за социнженерию и фишинг: [Электронный ресурс] – Режим доступа: https://rg.ru/2020/05/19/mvd-vystupilo-protiv-ugolovnoj-otvetstvennosti-za-socinzhen eriiu-i-fishing.html.
3. *Самурханов, М. С.* Понятие и особенности киберпреступности / М.С. Самурханов // Международный журнал гуманитарных и естественных наук. – 2020. – №4-3. – С. 219-221.
4. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50. Ст. 7074.
5. Definition of Cybersecurity Gaps and overlaps in standardisation // European Union Agency For Network And Information Security. – 2015. Heraklion, Greece. – 35 p.
6. *Dennis, M. A.* Defenition of «Cybercrime» / M.A. Dennis // Encyclopædia Britannica. – 2018: [Электронный ресурс] – Режим доступа: https://www.britannica.com/topic/cybercrime.