**Киберпреступность - специфическое явление общества**

На сегодняшний день значительную долю в общем объеме уголовных преступлений занимают преступления, связанные с использованием телекоммуникационных и компьютерных систем. Важно отметить, что в настоящее время до сих пор ведутся многочисленные дискуссии о содержании и значении юридических понятий «компьютерная преступность» и «киберпреступность» [3, c.1].

Между тем термин «киберпреступность», согласно Оксфордскому и Кембриджскому толковому словарю «cybercrime» означает - преступность, связанная, как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей.

Однако, по мнению экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, или против компьютерной системы или сети.

Следовательно, киберпреступления - это правонарушения экономического, политического и социального характера, выражающиеся в форме совершения незаконных деяний (действий, бездействия) во всех сферах общественной жизнедеятельности с помощью сети Интернет, иных средств электронной коммуникации.

В соответствии с действующим уголовным кодексом Российской Федерации под преступлениями в сфере компьютерной информации понимаются:

- неправомерный доступ к компьютерной информации (статья 272);

 - создание, использование и распространение вредоносных компьютерных программ (статья 273);

- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274);

- неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1).

Согласно Конвенции Совета Европы о преступности в сфере компьютерной информации ETS№ 185 от 23.11.2001, выделяются пять групп, некоторые из которых прямо согласуются со статьями Уголовного кодекса Российской Федерации:

Первая группа выключает в себя нормы регламентирующие ответственность за преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- противозаконный доступ (статья 2) - противоправный умышленный доступ к компьютерной системе либо её части);

- неправомерный перехват (статья 3) - (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с неё либо в её пределах);

- воздействие на данные (статья 4) - противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных;

- воздействие на функционирование системы (статья 5) - серьёзное противоправное препятствование функционированию компьютерной системы путём ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных;

- противозаконное использование устройств (статья 6).

Вторая группа включает в себя нормы посвященные правонарушениям, связанным с использованием компьютерных средств:

- подлог с использованием компьютерных технологий (статья 7). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, уничтожение или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных;

 - мошенничество с использованием компьютерных технологий
(статья 8) - намерение неправомерного извлечения экономической выгоды для себя или третьих лиц путем ввода, изменения, удаления или блокирования компьютерных данных или любого вмешательства в функционирование компьютерной системы.

Третью группу составляют преступления, связанные с правонарушениями, связанными с содержанием данных, к которым можно отнести - правонарушения, связанные с детской порнографией (статья 9).

В данном контексте важно отметить, что детская порнография считается тяжким преступлением, даже если лица, вовлечённые в её производство, не имели никакого физического контакта с детьми. Причиной этого является то, что для производства подобных порнографических материалов требуется сексуальная эксплуатация детей. Кроме того, потребители этих материалов зачастую не ограничиваются интересом к картинкам и сексуальными фантазиями, но и практикуют или стремятся практиковать педофилию в реальной жизни, что приводит к устойчивой асоциальной установке, повышающей общественную опасность этих деяний.

Четвертая группа включает в себя нормы посвященные преступлениям, посягающим на общественную безопасность. Наглядным примером может выступать кибертерроризм, под которым подразумевается - вовлечение в совершение преступлений террористического характера или иное содействие их совершению.

Таким образом, можно сделать вывод о том, что киберпеступность явилась результатом информатизации общества и внедрения высоких технологий во все сферы жизнедеятельности людей. [2, c.1]

Очевидно, что в настоящее время активному росту и развитию киберпреступности способствует природа данного явления, а именно:

- повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.);

- трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств;

- особая подготовленность преступников, интеллектуальный характер преступной деятельности;

- нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств;

- возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления;

- многоэпизодный характер преступных действий при множественности потерпевших;

- неосведомленность потерпевших о том, что они подверглись преступному воздействию;

- дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего;

- невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Кроме того, в данном контексте важно отметить, что помимо преобразования самой киберпреступности, необходимо учитывать характеристики хакеров, а именно: «Если первоначально это были лица, обладающие определенными знаниями, умениями, целью которых было, не совершение противоправных действий, а усовершенствование своих знаний.

То в нынешнее время все деяния совершенные этими лицами направлены лишь на получение выгоды, что, так или иначе, приводит к возникновению криминального бизнеса».

Растущий профессионализм киберпреступников и постоянное совершенствование информационных технологий, и, как следствие, постоянная эволюция возможностей для совершения преступлений, создают новые угрозы для общества.

Так согласно официальным данным Генеральной прокуратуры Российской Федерации: «В 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с
65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% - это почти каждое 20 преступление.

 Рисунок 1. *Рынок киберпреступлений в России: количественная оценка 2017-й год.*

На сегодняшний день самыми распространенными киберпреступлениями являются:

- неправомерный доступ к компьютерной информации (статья 272 УК РФ);

- создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ).

Если в 2017 году зарегистрировано 1 883 киберпреступлений (+7,7%), то за первое полугодие 2018 года - 1 233 (+3,4%). При этом на 19,6% уменьшилось количество расследованных преступлений по вышеуказанным статьям (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений, - подчеркивает надзорное ведомство. Раскрываемость данных преступлений составила 41,3%.

*Рисунок 2.Рынок киберпреступлений в России: количественная оценка 2018-й год.*

Так же, распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Их количество в первом полугодии 2018 года возросло в 7 раз».

Однако, не смотря на статистические данные, актуальным остается факт возбуждения уголовных дел по факту мошенничества. Как сообщает Генеральная прокуратура РФ: «Имели место факты вынесения незаконных постановлений об отказе в возбуждении уголовного дела. После их отмены возбуждено 204 уголовных дела (в 2016 году - 161). Наибольшее число таких фактов в республиках Коми, Марий Эл, Удмуртской Республике, Красноярском крае, Волгоградской, Кемеровской, Московской и Челябинской областях».

Таким образом, возникает вопрос: «Как власти намерены урегулировать проблему, связанную с киберпреступлениями?».

Так 6 июля 2018 года стало известно о создании в России автоматизированной системы обмены информации о киберугрозах. Об этом заявил президент Российской Федерации Владимир Владимирович Путин в ходе Международного конгресса по кибербезопасности в Москве: «Будет реализована инициатива бизнеса по формированию системы автоматизированного обмена информацией об угрозах в цифровом пространстве. При кибератаках эта система позволит лучше координировать действия операторов связи, кредитных организаций, интернет-компаний с правоохранительными органами и тем самым оперативно ликвидировать возникающие угрозы». Также президент отметил, что российские власти намерены развивать систему международного обмена информацией о киберугрозах:« В ближайшее время правительство должно определиться со структурой, которая будет отвечать за эту работу». [5, c.2]

По словам главы государства, для борьбы с киберугрозами необходимо выработать новые комплексные решения по предупреждению и пресечению преступлений против граждан в цифровой среде. Для этого важно создать соответствующие правовые условия, обеспечить удобные формы взаимодействия граждан и государственных структур, подчеркнул он: «Будем стремиться, чтобы действующее в России программное обеспечение и инфраструктура основывались на отечественных технологиях и решениях, которые прошли соответствующую проверку и сертификацию. Конечно, не в ущерб конкуренции».

Согласно официальным данным, опубликованным в РИА Новости,
4 октября 2018 года Глава Сбербанка Герман Греф заявил, что в России следует создать отдельное министерство по чрезвычайным ситуациям в цифровой сфере, по аналогии с обычным МЧС: «Я думаю, нужно создавать серьезную инфраструктуру. Министерство чрезвычайных ситуаций у нас существует. Нужно создать министерство, которое бы контролировало чрезвычайные ситуации в диджитальной сфере, которая коснется всей инфраструктуры без исключения». Помимо этого, глава Сбербанка также отметил, что цифровая составляющая проникает в различные сферы, и назвал это одним из ключевых трендов и вызовов будущего. Также он акцентировал внимание на том, что в современном мире киберугрозы приобретают все большее значение и делают заголовки новостей, в связи, с чем предпринимаются попытки создавать из них политические новости, вроде вмешательства в выборы или вмешательства в управление.

Ранее Сбербанк оценил глобальный ущерб от кибератак в 2018 году в $1 трлн. и прогнозировал рост этой суммы до $8 трлн. в 2022 году.

Таким образом, исходя из вышесказанного целесообразно представить нашу комплексную программу борьбы с киберпреступностью, которая должна включать следующую совокупность действий:

- гармонизация уголовного законодательства о киберпреступности на международном уровне;

- разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять электронные доказательства с учетом трансграничности этих преступлений;

- отлаженное сотрудничество правоохранительных органов при расследовании киберпреступлений на оперативном уровне;

- как можно более широкое распространение информации о современных киберугрозах среди населения страны, по возможности массовое повышение киберграмотности;

- объединение усилий всех участников, заинтересованных в устранении киберпреступности: правоохранительных органов, бизнеса, исследовательских и академических структур. [4, c.3]

**Список источников и литературы**

1. http://ru-act.com/ugolovnyj-kodeks/chto-takoe-kiberprestupnost.html
2. https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody- zashchity.html
3. https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza
4. http://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/
5. http://cabinet-lawyer.ru/uk-rf/kiberprestupnost.html