ИНСТИТУЦИОНАЛЬНАЯ ТРАНСФОРМАЦИЯ ПРАВОВОЙ СРЕДЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

УДК 3409
КОД РИНЦ 06.00.00

КИБЕРПРЕСТУПНОСТЬ: ГЛОБАЛЬНАЯ ПРОБЛЕМА И ЕЕ РЕШЕНИЕ

© 2019 Абиева Эмилия Минаминовна*
студент
Самарский государственный экономический университет
E-mail: abieva.emiliya@yandex.ru

В данной теме рассматривается проблема киберпреступности, способов ее решения для того, чтобы облегчить жизнь гражданам, не навредив им. Данная тема является актуальной в настоящее время, методы по борьбе с этим преступлением используются и сейчас, в действительности происходят много случаев в среде технологий, которые являются неправомерными, так как вредят людям, нарушая закон.

Ключевые слова: киберпреступность, кибертерроризм, субъект, объект правонарушения, преступления.

В обществе глобальной проблемой для жизни людей считается киберпреступность, граждане предпринимают различные меры для решения этой проблемы. Ведь данная проблема 21 века является главной проблемой, которая затрагивает полностью все. Само понятие киберпреступление подразумевает совершение преступлений в сфере, затрагивающей высшие технологии, которая включает в себя множество незаконных деяний.

Также можно еще сказать, что киберпреступностью является незаконное действие в электронной среде, совершенное при помощи компьютерных технологий, которое так же имеет некие особенности, которые будут сейчас перечислены. Итак, основными особенностями данных преступлений являются следующее: 1.Высочайшая скрытность деяний. Она представляет некую анонимность любых действий совершенных в интернет среде. 2.Трансграничность, другими словами, разделение преступника от его жертвы большим расстоянием.

* Научный руководитель -**Калашникова Елена Борисовна,** кандидат исторических наук, доцент.

3.Допустимость для совершения преступления в режиме автонома. 4.Неординарность действий закононарушителей. В отличие от других преступлений, данная особенность не дает предусмотреть незаконное деяние преступника. Существуют также несколько разновидностей киберпреступности. 1 - Правонарушения, направленные на компьютерные системы и базы данных. Примером может послужить взлом личных данных мобильного оператора для получения паспортных данных гражданина. 2 - деяния, которые были совершены при помощи технологий, которые имели цель экономической выгоды. 3 - материал, содержащий порнографию, а также ее распространение. 4 - права автора, которые были нарушены. Примером которого может послужить распространение видео на всеобщее обозрение, имея корыстный характер, а также воспользовавшись чужим авторством. Данное преступление можно часто встретить в YouTube. 5-Кибертерроризм. Данный вид преступления считается особо опасным, так как он включает в себя насильственные действия с ожесточенными мерами в высоких технологиях[1].

Но существуют и методы борьбы, которые были созданы властями для устранения данного вида преступления. Стали создавать отдельную структурную расследовательскую программу, борющуюся с данным преступлением. Так как полицейские стали не справляться с данным преступлением по причине того, что у них недостаточно знаний по сфере компьютеров, можно также сказать что их и вовсе нет. Поэтому стал создаваться отдел имеющий название К., которое является особым видом по борьбе с преступлениями, связанными с технологиями.[4] Субъект каждой страны должен иметь региональные отделения. Который по сей день является самым секретным подразделением. Это сделано для того, чтобы злоумышленники не могли распознать уровень предела К. Задачи данного подразделения предусматривают: борьбу с правонарушением авторских прав, незаконные проникновения в личные данные пользователя, а также борьбу с правонарушителями, которые распространяют порнографию в сети интернет. Невозможно узнать информацию данных органов, так как она является скрытным.[3] Киберпреступность имеет также и некие сложности, потому что ведь это не обычные преступления которые можно с легкостью расследовать, где виновник преступления находится не далеко от пострадавшего. Сказанного про обычные преступления нельзя сказать о киберпреступности, так как в некоторых случаях порой даже сложно выявить состав преступления и найти самого виновного данного содеянного [3].

Это все имеет причины, из-за которых данные деяния труднее расследовать, в отличие от преступлений, которые даются легко простым полицейским: Латентность максимальности преступных деяний. В большинстве случаев специальные службы не в состоянии увидеть и предусмотреть факт правонарушения. Примером может послужить взлом базы данных. Злоумышленники могут позаимствовать чужую информацию, которая скрыта для всех, но о том, что они позаимствовали и считали информацию никто не удостоится узнать.

Преступление может иметь крупный масштаб. Примером данного является провинциальный студент, взимающий базу данных какого-то банка, в случае чего изымаются счета клиентов. Данное преступление совершить может один субъект. Образованность злоумышленников имеет высокий уровень. Примером могут послужить интеллектуальные способности, которыми обладают хакеры, ведь известно, что они очень умны и с ними очень трудно вести борьбу. Также сложность имеется при составлении портрета преступника. В обычном случае с ситуациями, не затрагивающими преступления, связанные с технологиями, там гораздо проще составить портрет следователем, который может составить портрет приближенный к преступнику в большинстве случаев эти представления являются верными. Но киберпреступность данной розыскной системой не обладает, правонарушителем может оказаться преступник, которого невозможно охарактеризовать по признаку гендерства и др. Технологии борьбы с правонарушителями превосходят по своему уровню технологическую базу правоохранительных структур.

Виды киберпреступности. Имеются множество видов данного рода преступления. Развиваются технологии, и развивается вместе с ней преступность не в одной сфере, а сразу в нескольких. Первым видом является распространение преступлений, которое является неправомерным действием, совершенным в компьютерной среде, информацией, которая охраняется уголовным законом.[4] Совершение неправомерных действий влекут за собой серьезные последствия. Неправомерными действиями считаются: распространение чужой информации и ее обладание, а также считывание информации, которая является скрытой для всех.[2] Вторым видом является преступление, которое может стать вирусным при распространении и использованных программ, которые влекут за собой последствия.

Существующее преступление можно охарактеризовать следующим: субъект, создав для работы специальную программу или скачав приложение на свой компьютер, после чего в его компьютер стали проникать злоумышленники. Этим может послужить копирование важной информации, принадлежащей определенному лицу, или же удаление информации, а также распространение скрытой информации. Вид третий - это неправильная эксплуатация. Она может произойти, когда определенный субъект провел эксплуатацию компьютера не так, как нужно, и, в случае, чего вся информация на данном компьютере была уничтожена, либо же она может быть передана, либо повреждена.

Для того чтобы верно охарактеризовать преступление, связанное с технологиями и компьютерной средой, нужно подробно рассмотреть состав преступления, разделив его по частям.

Первое, что может быть, это объект преступления, который представляет в свою очередь общественные отношения. Существует так же сторона субъективности, представляющая умысел. Умысел - это когда преступник хочет совершить преступления, имея очень большой интерес, для того, чтобы данное преступле-

ние имело место быть. Цель данного вида преступления - это получение информации скрытого доступа. Стоит учитывать, что без субъекта данное преступление не может совершаться. Субъектом преступления является преступник, совершивший опасное деяние, не всегда он может действовать один, порой преступления совершаются и группами.[2]

На сегодняшний день киберпреступность - проблема, охватывающая различные сферы при помощи программ, содержащих вирус. Именно интернет послужил развитием для данного преступления, при помощи которого злоумышленники стали получать доступ к чужим аккаунтам и базам данных.

Таким образом, стоит отметить, что данный вид преступления имеет высокий уровень латентности, в отличие от иных видов преступлений, он представляет усложненную структуру расследования данного преступления, как было сказано раннее, хакеры обладают сверхъестественным умом и уникальностью скрывать улики совершенных неправомерных действий.

---

[1] Васенин В.А. Информационная безопасность и компьютерный терроризм //крайм ресорч .ру [Электронный ресурс]. - Режим доступа: URL: http://www.crime-research.ru/ (дата обращения 15.05.19)

[2] Номоконов В.А. Глобализация информационных процессов и преступность // Информационных технологий . 2002. С. 98.

[3] Семинар-практикум 6: Меры по борьбе против преступлений, связанных с использованием компьютеров // материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. A/CONF.2Q3/14. Бангкок, 2005. С. 25

[4] Айсанов Р.М. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // "Черные дыры" в российском законодательстве. 2007. N 1. С.279-280.

CYBERCRIME: A GLOBAL PROBLEM AND ITS SOLUTION

© 2019 Abieva Emiliya Minaminovna
Student
Samara State University of Economics
E-mail: abieva.emiliya@yandex.ru

This topic addresses the issue of cybercrime, how to solve it in order to make life easier for citizens without harming them.

This topic is relevant now, methods to combat this crime are used and now, in fact, there are many cases in the environment of technologies that are illegal because they harm people by breaking the law.

Keywords: cybercrime, cyberterrorism, subject, object, offense, crime