INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.3 №3 (2025). March
innovativepublication.uz

Пресечение преступлений совершаемых в киберпространстве

Хамидов Хусанбек Шерзоджон угли

Курсант Министерства внутренних дел

Аннотация: На современном этапе человеческого развития социум зависит от информационных технологий. Масштабные процессы компьютеризации с каждым днём всё сильнее внедряются в правовую сферу деятельности общества, параллельно приводя к росту киберпреступности. Авторами исследуется специфика предупреждения преступлений в сети интернет. Определяется содержание, сущность, порядок и возможность противодействия преступности в цифровом пространстве. Внимание акцентируется на необходимости всестороннего применения законодательства в сети интернет. Раскрывается содержание механизмов противодействия цифровой преступности, производится анализ её преимуществ и недостатков.

Ключевые слова: Преступность, Сеть, Интернет, Законодательство, Виктимология, Профилактика, Ответственность, Правопорядок, Меры, Безопасность.

Аннотация: Киберпреступность — 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 и компьютерных данных.

Ключевые слова: киберпреступность; компьютерная преступность; Интернет.

Актуальность темы исследования объясняется тем, что предупреждение преступлений в сфере высоких технологий носит комплексный, междисциплинарный характер. Практика превентивной деятельности государства показывает, что оно по различным причинам не может осуществлять эффективное противодействие киберпреступлениям. Изучив практические материалы, рассмотрев взгляды специалистов на указанную проблему, авторы предлагают способы ее решения. При подготовке работы авторы изучали статистические материалы о состоянии борьбы с киберпреступлениями, законодательные акты в области предупреждения преступлений, провели анализ теоретических работ отечественных ученых по вопросам предупреждения киберпреступлений.

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности:

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

2) Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств.

3) Особая подготовленность преступников, интеллектуальный характер преступной деятельности.

4) Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств.

5) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления.

Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: «информационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий», «виртуальное преступление».

Согласно действующему законодательству Республики Беларусь, в содержание понятия «компьютерная преступность» включают:

1) преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации,

компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

2) хищения путем использования средств компьютерной техники;

3) изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;

4) иные преступления, так или иначе связанные с использованием компьютерной техники: доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.

Таким образом, к компьютерным преступлениям относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства. Таким образом, комплексная программа борьбы с киберпреступностью должна включать совокупность действий, как государственных структур, так и частного сектора экономики, которая должная включать в себя: международное сотрудничество, направленное на взаимодействие и координацию действий спецслужб; синхронизация национальных законодательств разных стран мира и, исходя из этого, заключение межгосударственных соглашений; разработка стратегии кибербезопасности на уровне национальной экономики; постоянная оптимизация

национального законодательства с учетом новых технических возможностей и угроз; обеспечение объединенного подхода к достижению кибербезопасности, при котором механизм реализации встроен в систему изначально и требует периодически лишь точечной корректировки; всемерная оптимизация взаимодействия правоохранительных органов и служб по борьбе с киберпреступностью, а также с органами судебной власти; формирование материальной базы служб по борьбе с киберпреступностью исходя из принципа «самая современная»; как можно более широкое распространение информации киберугрозах среди населения страны, по возможности массовое повышение киберграмотности; объединение усилий всех участников, заинтересованных в устранении киберпреступности: правоохранительных органов, бизнеса, исследовательских и академических структур.

Список литературы:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ // СПС КонсультантПлюс (дата обращения: 06.12.2021);
2. Александр Владимирович Леонов, Александр Яковлевич Назаренко Проблемы предупреждения преступлений с использованием сети Интернет // Закон и право. 2018. №8. URL: https://cyberleninka.ru/article/n/problemy-preduprezh.. (дата обращения: 06.12.2021).
3. ЦБ отметил смещение интересов хакеров в сторону клиентов банков// РИА Новости [Электронный ресурс]. URL: https://ria.ru/economy/20180220/1515001732.html (дата обращения 03.04.2018 г.)