ПОНЯТИЕ И РОЛЬ«ИНФОРМАЦИОННЫХТЕХНОЛОГИЙ» В СФЕРЕ ПРОФИЛАКТИКИ ПРАВОНАРУШЕНИЙ

С.У.Шавкатов
Курсант Академии МВД Респулики Узбекстан

Аннотация: *Компьютерная информация и компьютеры являются неотъемлемой частью функционирования человека в современных условиях. Виртуальное пространство постепенно интегрируется во все сферы жизни общества и государства. Сейчас уже речь идет о переходе к построению глобального информационного сообщества с развитой системой информационных телекоммуникаций. Наблюдается также интенсивное внедрение перспективных информационных технологий во все сферы юридической деятельности. успешность правоохранительной деятельности уже во многом зависит от степени и качества обеспеченности новейшими информационными средствами служб органов внутренних дел. Также освоения сотрудниками навыков пользования данными средствами в своей профессиональной деятельности, для успешного и своевременного предупреждения и раскрытия правонарушений и преступлений.*

Ключевые слова: *информационные технологии, кибер безопасность, компьютерные технологии*

Annotation: *Computer information and computers are an integral part of human functioning in modern conditions. The virtual space is gradually being integrated into all spheres of society and the state. Now we are talking about the transition to building a global information community with a developed information telecommunications system. There is also an intensive introduction of promising information technologies in all areas of legal activity. The success of law enforcement activities already largely depends on the degree and quality of provision of the latest information tools of the services of internal affairs bodies. Also, employees develop skills in using these tools in their professional activities, for the successful and timely prevention and disclosure of offenses and crimes.*

Keywords: *information technology, cybersecurity, computer technology*

В настоящее время сложно представить свою жизнь без информационных технологий. Информационная технология — это процесс, использующий совокупность средств и методов сбора,

обработки и передачи данных для получения информации нового качества о состоянии объекта, процесса или явления.

С помощью сотовой связи мы легко можем связаться с человеком, который находится далеко от нас, а Интернет поможет нам найти любую информацию или просто скоротать время за просмотром видеоролика. Можно не утруждать себя походом в магазин, а заказать необходимые вещи через интернет-магазин. Зачем идти за талоном на прием к врачу в больницу, когда можно все это сделать через сайт Портал государственных услуг. Это все значительно упрощает нашу жизнь, но часто ли мы задумываемся над тем, как это может обернуться против нас.

Стремительное развитие информационных и коммуникационных технологий, а также компьютеризация мирового сообщества приводит к неуклонному и стремительному росту правонарушений в сфере информационных технологий. И, как правило, в большинстве случаев, правонарушителями становятся граждане, которые не до конца осознают всю ответственность, предусматривающую правовыми актами Республики Узбекистан.

Преступления в сфере информационных технологий, или киберпреступность – это преступления, совершаемые людьми, использующими информационные технологии для преступных целей.

Как уголовно-правовое и социальное отрицательное явление преступность (система преступлений, которые совершаются в определенный период на конкретной территории) взаимосвязана неразрывно с обществом, подвержена воздействию динамического развития общества.

Главным образом, это выражается тем, что на определенном временном этапе самыми уязвимыми для преступных деяний являются новые области (сферы) взаимодействия субъектов социальных отношений, которые еще не освоены правоприменительной (правоохранительной) практикой. Преступники стремятся в общественно-правовой действительности найти наиболее уязвимые (слабые) места с целью реализации корыстных целей. Они для этого используют разнообразные изысканные и извращенные способы посягательств преступного характера.

На рубеже XX — XXI столетий с возникновением сети Интернет и распространением масштабной информационной кампании по всему миру у преступников появились огромные возможности осуществлять незаконную деятельность, тогда как криминологи

и работники правоохранительных органов столкнулись с отсутствием возможностей им полноценно противостоять.

Сеть Интернет—это киберпространство для передачи (создания, распространения (трансляции), хранения, получения и др.) информации различного рода. Главная проблема «безграничности» (масштабности) данного киберпространства состоит в отсутствии возможности эффективно

контролировать как использование данной информации, так и доступ к ней, регулировать социальные отношения, взаимосвязанные с ней.

Следующий отрицательный фактор основывается на том, что обычно правонарушители осваивают прикладные области и направления взаимодействия быстрее правоприменителей и законодателей.

Подобные причины включают новизну этой сферы социальных отношений, а также отсутствие научных подходов в современной криминалистике (криминологии), законодательной регламентации и правоприменительной практики, практики расследования анализируемых преступлений, социальных и технических ресурсов и возможностей. Суммируя все сказанное выше, выделим ряд предпосылок развития Интернет-преступности:

— отсутствие должного контроля за реализуемой в сети Интернет работой юридических лиц и граждан;

— открытие доступа россиян к ресурсам сети Интернет;

— информационная безграмотность (доверчивость) пользователей, их неспособность оценивать, как действия преступников, так и собственные, компетентно;

— неподготовленность к противостоянию киберпреступности со стороны правоохранительных органов;

— отсутствие нормативно-правовой регламентации пользователей сети Интернет (сайты знакомств, онлайн-борды и др.);

— возможность взаимодействия в сети Интернет анонимно;

— низкий уровень охраны программного обеспечения; — несовершенство парольных систем.

Президентом Республики Узбекистан в 2022 г. утвердил Закон О КИБЕРБЕЗОПАСНОСТИ, в которой были утверждены ключевые направления и цели ИБ в современном Узбекситане, среди которых:

объект информатизации — информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства

обработки информации, помещения, где установлены и эксплуатируются эти средства;

киберпреступность — совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств, с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов;

киберпространство — виртуальная среда, созданная с помощью информационных технологий;

киберугроза — комплекс условий и факторов в киберпространстве, представляющих угрозу интересам личности, общества и государства;

кибербезопасность — состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве;

инцидент кибербезопасности — событие в киберпространстве, приведшее к сбоям в работе информационных систем и (или) нарушениям доступности информации в них, целостности и ее свободного использования;

объект кибербезопасности — комплекс информационных систем, используемых в деятельности по обеспечению киберзащиты информации и кибербезопасности национальных информационных систем и ресурсов, в том числе объекты критической информационной инфраструктуры;

субъект кибербезопасности — юридическое лицо или индивидуальный предприниматель, имеющий определенные права и обязанности, связанные с владением, пользованием и распоряжением национальными информационными ресурсами и оказанием информационных электронных услуг по их использованию, защитой информации и кибербезопасностью, в том числе субъекты критической информационной инфраструктуры;

киберзащита — комплекс правовых, организационных, финансово-экономических, инженерно-технических мер, а также мер криптографической и технической защиты данных, направленных на предотвращение инцидентов кибербезопасности, выявление кибератак и защиту от них, устранение последствий кибератак, восстановление стабильности и надежности деятельности телекоммуникационных сетей, информационных систем и ресурсов;

кибератака — действие, представляющее угрозу кибербезопасности, умышленно осуществляемое в киберпространстве с использованием аппаратных, аппаратно-программных и программных средств;

критическая информационная инфраструктура — комплекс автоматизированных систем управления, информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение;

объекты критической информационной инфраструктуры — системы информатизации, применяемые в сфере государственного управления и оказания государственных услуг, обороны, обеспечения государственной безопасности, правопорядка, топливно-энергетического комплекса (атомной энергетики), химической, нефтехимической отраслях, металлургии, водопользования и водоснабжения, сельского хозяйства, здравоохранения, жилищно-коммунального обслуживания, банковско-финансовой системы, транспорта, информационно-коммуникационных технологий, экологии и охраны окружающей среды, добычи и переработки полезных ископаемых стратегического значения, производственной сфере, а также в других отраслях экономики и социальной сфере;

субъекты критической информационной инфраструктуры — государственные органы и организации, а также юридические лица, владеющие объектами критической информационной инфраструктуры на правах собственности, аренды или на других законных основаниях, в том числе юридические лица и (или) индивидуальные предприниматели, обеспечивающие эксплуатацию и взаимодействие объектов критической информационной инфраструктуры.

Организационно-управленческие меры включают также виктимологическую профилактику совершаемых в сети Интернет преступных деяний. Это связано с тем, что жертвами мошенничества в сети Интернет, как правило, становятся субъекты, не компетентные в защите личной кибербезопасности. Важно регулярно проводить беседы с пенсионерами, подростками и другими гражданами групп риска, активно распространять информацию о разнообразных способах реализации киберпреступлений в сети и СМИ, обязать ежемесячно Интернет-провайдеров рассылать пользователям актуальные правила безопасности [2]. Также и технические меры представляют широкий пласт мероприятий. Однако, они же и выступают

наиболее ресурсозатратными. Сущность их заключается в повышении уровня эффективности деятельности особых подразделений (отделов) правоохранительных органов, специализирующихся на расследовании, мониторинге и контроле совершаемых в Интернете правонарушений. Система подобных мер предусматривает обеспечение данных органов высокотехнологичным оборудованием, а также его регулярным обновлением и наращиванием технических мощностей и иных характеристик, разработку нового ПО, устройств (гаджетов), обеспечение компетентными специалистами, организующими бесперебойную работу в системе мониторинга киберпреступлений. Следовательно, необходимо учитывать тот факт, что информационные технологии современного общества по мере их развития и проникновения в различные сферы повседневной жизни, социум делают уязвимым перед угрозами преступности, однако, способствуют при этом совершенствованию инструментов и методов противостояния ему.

ЛИТЕРАТУРА:

1. Лобачёв Л. Л., Куцаков Ф.В. Предупреждение преступлений в сети интернет // Скиф. 2021. № 12 (64). URL: https://cyberlenink a.ru/article/n/preduprezhdenie-prestupleniy-v-seti-internet (дата обращения: 05.12.2022).

2. Закон Республики Узбекистан О Кибербезопасности // URL: https://lex.uz/ru/docs/5960609