**МИНОБРНАУКИ РОССИИ**
**Федеральное государственное бюджетное**
**образовательное учреждение**
**высшего профессионального образования**
**«Челябинский государственный университет»**
**(ФГБОУ ВПО «ЧелГУ»)**

**Костанайский филиал**

**Кафедра права**

**А.Т. Исмагулова, А.М. Галиаскарова**

# Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан

Монография

**Костанай**
**2016 г.**

**УДК 340.114.6 (035.3)**
**ББК 67.408**
**И 88**

**Рецензенты:** **Ревин В.П.,** заслуженный деятель науки РФ, д.ю.н., профессор (г.Москва)

**Мизанбаев А.Е.,** д.ю.н. (г.Костанай)

**И88 Исмагулова А.Т.**

Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан: монография/А.Т. Исмагулова, А.М. Галиаскарова; Костанайский филиал ФГБОУ ВПО «Челябинский государственный университет». – Костанай: ТОО «New Line Media», 2016. – 160 с.

**ISBN 978-601-7798-10-9**

В монографии освещаются проблемные аспекты регламентации ответственности за правонарушения в сфере информатизации и связи по новому уголовному законодательству Республики Казахстан, а также рассматриваются проблемы, возникающие в борьбе с правонарушениями в сфере применения компьютерных технологий и пути их решения.

Адресуется специалистам в области уголовного права, криминологии, а также студентам специальности и направления подготовки "Юриспруденция", "Правоохранительная деятельность"

**УДК 340.114.6 (035.3)**
**ББК 67.408**

**ISBN 978-601-7798-10-9**

**Содержание**

## Определения

В настоящей монографии применяются следующие термины с соответствующими определениями:

*Блокирование компьютерной информации* - результат воздействия на компьютер, исключающий доступ к ней при сохранности охраняемой законом компьютерной информации.

*Виртуальное пространство* - моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

*Внесение изменений в существующую программу или программный продукт* - изменение теста программы путем исключения его отдельных фрагментов, замены их другими либо их дополнения новыми фрагментами посредством специального программного продукта или вручную.

*Вредоносная программа* - программа, которая содержит «вирусы» с целью уничтожения, блокирования, модификации, копирования программного продукта, нарушение работы компьютера, информационной системы или информационно-коммуникационной сети.

*Доступ к компьютерной информации* - наличие возможности пользоваться информацией и совершать с ней различные операции.

*Информационная безопасность* - состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной

сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны.

*Информационная система* - это совокупность компьютеров, взаимосвязанных между собой как единое целое, с включением дополнительных устройств, обеспечивающих ввод или передачу информации.

*Информационно-коммуникационная сеть* – это соединения нескольких компьютеров или систем компьютера друг с другом каналом связи, обеспечивающее совместное использование периферийных устройств и имеющее программное обеспечение, позволяющее осуществлять эту связь.

*Информационное общество* - это социум с высокоразвитой системой каналов информационного обмена и телекоммуникаций, а также средств и систем защиты циркулирующей по ним информации.

*Информационные ресурсы* - формализованные знания и идеи, различные данные, методы и средства их накопления, хранения и обмена между источниками и потребителями информации.

*Информационные технологии* - система методов и способов сбора, накопления, хранения, поиска, обработки, транспортировки и отображения информации на основе применения средств вычислительной и коммуникационной техники.

*Информация* - совокупность знаний о фактических данных.

*Использование вредоносной программы для компьютера* - это умышленное воспроизведение, распространение, установка и иные действия по введению программы в оборот в первоначальной или измененной форме.

*Киберпреступление* - преступление, которое совершается с помощью компьютерной системы или сети, в рамках компьютерной системы или сети либо против компьютерной системы или сети.

*Киберпреступность* - это преступность в виртуальном пространстве.

*Компьютер* - устройство или система, способное выполнять заданную, чётко определённую изменяемую последовательность операций.

*Компьютерная информация* - это информация, зафиксированная на электронном носителе и передаваемая по телекоммуникационным каналам в форме, доступной восприятию компьютера.

*Компьютерная преступность* - вид преступности, в которых компьютер является как объектом преступления, поскольку ему причиняется материальный ущерб путем физического повреждения, так и орудием совершения преступления, когда его используют для получения политических или деловых преимуществ.

*Компьютерное правонарушение* - предусмотренное уголовным законом общественно опасное деяние, посягающее на охраняемую законом компьютерную информацию, которое причиняет или создает угрозу причинения вреда правам и свободам человека, безопасности физических и юридических лиц (независимо от формы собственности), общества и государства.

*«Компьютерный вирус»* - это совокупность электронного кода, которая сама может создать свои копии и внедрять их в файлы.

*Копирование компьютерной информации* - перенос информации с одного электронного носителя на другой, если это осуществляется помимо воли собственника или владельца информации, при условии получения точного дубликата оригинала охраняемой законом компьютерной информации.

«*Кракер»* - вор, который взламывает систему защиты, незаконно проникает в компьютерную сеть и крадет, подменяет или иным несанкционированным способом использует компьютерную информацию.

*Модификация компьютерной информации* - несанкционированная собственником или законным владельцем любая переработка первоначального состояния охраняемой законом информации, которая трансформирует се содержание.

*Нарушение работы компьютера или информационной сети* - это нештатная техническая ситуации (сбой в работе компьютера, информационной системы или информационной-коммуникационной сети, «зависание»

компьютера и т.п.), при которой нормальное функционирование компьютерной техники невозможно.

*Неправомерный доступ к компьютерной информации* - самовольное получение виновным лицом информации или распоряжение ею (уничтожение, блокирование, модификация, копирование) по своему усмотрению без разрешения ее собственника или законного владельца

*Охраняемая законом компьютерная информация* - сведения, данные, знания, дающие представление о каком-либо явлении или предмете, охраняемые действующим законодательством, находящиеся на электронном носителе, в компьютере, информационной системе или информационно-коммуникационной сети.

*Пользователь информации* - это субъект, обращающийся к информационной системе за получением необходимой информации с целью ее пользования.

*Программа для компьютера* - объективная форма представления совокупности данных и команд, которые предназначены для функционирования электронной вычислительной техники с целью получения определенного результата.

*«Программы-бомбы»* - принцип работы этих программ заключается в том, что действие вредоносных функций начинается либо в определенный период времени («временная бомба»), либо при наступлении определенных условий («логическая бомба»).

*Распространение вредоносных программ для компьютера* - это предоставление доступа к программе для компьютера в компилированном виде, в том числе сетевыми и иными способами, а также путей продажи, проката, сдачи внаем, предоставления взаймы либо создание условий для самораспространения программы.

*Создание вредоносной программы для компьютера* - это процесс написания программы: от возникновения идеи и определения основных

принципов работы программы до написания ее исходного текста и компилирования.

*«Троянцы»* - программы, которые скрытно «живут» в компьютере и выполняют в нем вредоносные функции, либо отдают контроль над компьютером в руки другого человека.

*Уничтожение компьютерной информации* - осуществление действий виновными лицами путем умышленной полной или частичной физической ликвидации информации с физических носителей в компьютере, информационной системе или информационно-коммуникационной сети.

*«Хакер»* - пользователь вычислительной техникой, занимающийся поиском и разработкой незаконных способов проникновения в компьютер, информационную систему или информационно-коммуникационную сеть и несанкционированному использованию последних.

*Электронная информация* - это сведения о чем-либо, хранящиеся и передаваемые с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе.

*Электронный носитель* - материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

## Обозначения и сокращения

ГК РК – Гражданский кодекс Республики Казахстан

ДВД – Департамент внутренних дел

ДКП – Департамент криминальной полиции

КНБ – Комитет национальной безопасности

МВД РК – Министерство внутренних дел Республики Казахстан

МВД РФ – Министерство внутренних дел Российской Федерации

ОЗУ – Оперативное запоминающее устройство

ООН – Организация Объединенных Наций

ОПМ – Оперативно-профилактическое мероприятие

ОС – Операционная система

ОЭСР – Организация экономического сотрудничества и развития

ПС – Программные средства

РК – Республика Казахстан

РФ – Российская Федерация

СКТ – Средства компьютерной техники

СМИ – Средства массовой информации

СНГ – Содружество Независимых государств

СССР – Союз Советских Социалистических Республик

США – Соединенные Штаты Америки

УК РК – Уголовный кодекс Республики Казахстан

УК РФ – Уголовный кодекс Российской Федерации

ФБР – Федеральное бюро расследований

ФРГ – Федеративная Республики Германия

ЭВМ – Электронно-вычислительная машина

# Введение

Процесс построения суверенного, демократического, светского, правового и социального государства в Республике Казахстан, согласно Конституции Республики Казахстан 1995 года [1], неразрывно связан с идеей повышения эффективности мер борьбы с явлениями, препятствующими этому процессу, одними из которых выступают правонарушения.

Современный период развития нашего государства характеризуется не только относительно высоким количественным ростом правонарушений в целом, но и ее качественным изменением. Развитие высоких технологий позволяет большинству населения иметь персональные компьютеры, сотовые телефоны, модемы и иные средства связи, что не только свидетельствует об уровне мобильности общества, но и создает условия для появления новых форм и видов злоупотреблений техническими средствами, в том числе и в криминальных целях.

Электронная торговля, спам и киберпреступность, свобода выражения мнений, защита неприкосновенности частной жизни - вот лишь некоторые из многочисленных областей, где появляется необходимость в глобальных общих правилах, хотя бы для решения проблемы коллизии юрисдикций. К сожалению, традиционная система, базирующаяся на исключительном суверенитете наций-государств, представляется плохо приспособленной к транснациональной сети такого масштаба - к такому мнению приходят многие ученые мира[2, с.1].

Проблема защиты компьютерной информации и информационных систем сейчас является одной из самых актуальных во всем мире. Новые возможности, предоставляемые информационными технологиями, их широкая распространенность и доступность делают эту область чрезвычайно привлекательной для представителей криминальной среды[3, с.5]

Исследователям удалось установить, что каждую секунду киберпреступники причиняют ущерб 18 пользователям по всему миру[4, с.73].

По оценкам экспертов Казахстан занимает 18-е место в мире по количеству получаемого спама и 7-е по опасности веб-серфинга. Почти половина пользователей Интернета в 2010 г., становились объектами атак со стороны хакеров, и эта цифра в 2011 г. увеличилась на 47% [5, с.29]

Впервые уголовная ответственность за компьютерные преступления была предусмотрена в УК Казахстана 1997 г. всего одной статьей 227 "Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ", которая находилась в главе 7 "Преступления в сфере экономической деятельности"[6, с.496]

Законом Республики Казахстан "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам деятельности органов внутренних дел" в 2014 году были внесены изменения в УК, в соответствии с которыми появилась новая глава 7.1 УК РК " Преступления против безопасности информационных технологий"[7]

С 1 января 2015 г. вступил в действие новый - второй по счету Уголовный Кодекс Казахстан[8]. В этой связи Козаченко И.Я. выразил мнение, что концептуальные положения нового УК Республики Казахстан носят взвешенный характер и достаточно адаптированы к взаимодействию с бесконечно многочисленными социально-правовыми регуляторами человеческого общежития[9, с.37-38]. Как справедливо отмечают другие ученые-криминалисты данный кодекс "по законам диалектического развития вобрал в себя добротные классические устои и наряду с этим новаторские идеи"[10, с.5].

Так, данный юридический документ содержит ряд нововведений, в том числе и по "компьютерным правонарушениям". Еще на стадии законопроектных работ совершенно справедливо акцентировалось внимание на необходимости усиления защиты информационной безопасности Казахстана[11, с.75-80]. Обосновывая принятие нового УК Казахстана, законодатели ссылались на то, что нынешнее состояние уголовного

законодательства характеризуется отсутствием продуманной и четкой последовательности в его постоянных изменениях, недостаточности, а порой и отсутствием уголовно-правовой регламентации современных противоправных посягательств, особенно в сфере информационных технологий, медицины, экологии, градостроительства и архитектурной деятельности[12].

В новом УК Казахстана, нормы, устанавливающие ответственность за правонарушения в сфере компьютерной информации расположены в самостоятельной главе 7 "Уголовные правонарушения в сфере информатизации и связи" и включают 9 основных составов правонарушений[8].

Таким образом с введением нового Уголовного кодекса ответственность за деяние в сфере компьютерной информации в структуре УК РК получила статус обособленного объекта уголовно-правовой охраны.

Следует отметить то, что в большинстве стран мира с высоким уровнем технологического развития борьба с компьютерными преступлениями или как в нашем государстве (правонарушениям) давно является одним из приоритетных направлений государственной политики. Изложенное подчеркивает не только своевременность, но и необходимость обращения к данной проблеме с позиции именно комплексного исследования, как самих криминальных деяний, так и их состояния и тенденций развития, а также уголовно-правовых и организационно-технических форм предупреждения.

Интеграция информационных технологий имеет место и в криминальной среде, подрывая информационную безопасность государства. В Законе Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» национальная безопасность Республики Казахстан - состояние защищенности национальных интересов Республики Казахстан от реальных и потенциальных угроз, обеспечивающее динамическое развитие человека и гражданина, общества и государства [13]. Борьба с правонарушениями в информационной области стала составной частью политики государства, что явилось причиной внесения изменений и дополнений в ряд действующих законодательных актов. Так, принятие Закона

Республики Казахстан «Об информатизации» 11 января 2007 года восполнило пробелы, существенно влиявшие на проблемы процесса информатизации в современном казахстанском обществе [14]. Вместе с тем, основное назначение данного закона ограничивается его социальной управленческой направленностью и не охватывает многих деталей, связанных с применением средств из сферы высоких технологий в различных целях, в том числе - в корыстных.

Однако следует отметить, что, обладая широким спектром знаний в сфере информационных технологий, правонарушители имеют низкие шансы в своем изобличении, так как в этой области сотрудники правоохранительных органов подготовлены недостаточно. Необходимость привлечения специальных научных знаний для расследования подобных правонарушений обусловливает возникновение ряда вопросов организационного и правого характера.

Произошедшие перемены в обществе непременным образом влияют на реализацию всех тех деклараций, которые провозглашены на законодательном уровне. С введением нового УК РК законодатель решил актуальные проблемы несовершенства уголовно-правовой конструкции норм о преступлениях (теперь по новому УК правонарушений) в сфере компьютерной информации. Все это свидетельствует о необходимости научного анализа 7 главы «Уголовные правонарушения в сфере информатизации и связи», с проведением более глубоких исследований в целях выработки предложений, которые могли бы способствовать снижению роста правонарушений в сфере информатизации и связи.

Тенденция к расширению сфер криминальной деятельности по средствам и с помощью информационных технологий определяет необходимость научной проработки и более глубокого познания причинного комплекса правонарушений в сфере компьютерной информации и, следовательно, актуальность настоящего исследования, его значимость для теории и практики.

Несмотря на постоянно возрастающую актуальность правонарушений в сфере информатизации и связи, следует отметить, что фундаментальных

исследований по данной проблематике в Казахстане очень мало. Работы, которые были опубликованы в последнее десятилетие, в своей общей массе посвящены рассмотрению криминологических и криминалистических аспектов компьютерных преступлений или правонарушений.

В свою очередь, вопросы, связанные с решением этих проблем, а также историей данного вида преступлений (правонарушений), его особенностей, причин и условий, личности «компьютерного» правонарушителя нашли свое отражение в трудах ученых: Б.Х. Толеубековой, Р.А. Назмышева, Т.Е. Сеитова, Ж.К. Аманова, Т.М. Лопатиной, С.М. Рахметова.

Большой вклад в исследование данной проблемы внесли такие ученые России как: Ю.М. Батурин, В.А. Бессонов, В.Б. Вехов, А.М. Жодзишский, К.А. Зуев, В.Д. Зеленской, В.В. Крылов, Г.Б. Кочетов, А.Н. Караханьян, В.Д. Козаченко, И.Я. Курушин, В.Д. Ларичев, В.Ю. Максимов, Н.С. Шеннон, Л.И. Шершнев, Н.И. Шумилов и других.

Теоретическая и практическая значимость указанных исследований без сомнения велика. Однако в настоящее время остается потребность в более глубоком исследовании проблем, направленных на повышение эффективности уголовного закона в сфере борьбы с компьютерными правонарушениями, что напрямую связано с изучением уголовно-правовой характеристики компьютерных правонарушений, разработкой системы мер предупредительного характера, комплексного анализа правовых и организационно-технических мер противостояния компьютерной преступности. Все это предопределило выбор темы исследования и актуальность проведения углубленного анализа данной проблемы с позиции уголовно-правовой теории и правоприменительной практики.

## 1 Правонарушения в сфере информатизации и связи -новая глава уголовного законодательства Республики Казахстан

### 1.1 Исторические аспекты возникновения и развития уголовных правонарушений в сфере информатизации и связи

1974 году на рынке появляются компактные, сравнительно недорогие персональные компьютеры для бесконечного круга пользователей всемирной глобальной сети, что приводит к таким же глобальным изменениям во всех отраслях человеческих отношений[15, с.3]. Верно считают многие ученые, что по мере появления в XX веке различных достижений науки и техники, таких как: средства коммуникации, телеграф, телефон, радио, кино, телевидение, компьютер параллельно проходил и иной процесс: многие из них стали приниматься на вооружение преступного мира [16, с. 11]. Однако внедрение во все сферы деятельности компьютерной техники сыграло наиболее существенную роль в деле технического вооружения преступности. «Невидимость» компьютерного правонарушителя и одновременно «удлинение его рук» путем доступа к любым охраняемым секретам - военным, финансовым, иным - делают его весьма привлекательным для представителей преступного мира.

История последних десятилетий свидетельствует о появлении и прогрессирующем, по сравнению с другими видами криминальных посягательств, росте правонарушений с использованием возможностей информационных технологий.

Под воздействием последних происходит глобальный процесс информатизации общества, на смену экстенсивного пути развития экономики приходит интенсивный, компьютерная техника повсеместно внедряется в жизнь современного человека, общественная и производственная деятельность которого подвергается процессу сплошной компьютеризации прямо на глазах.

Проникновение в жизнедеятельность человека современных информационных технологий - это следствие процесса информатизации всего общества, который предполагает трансформацию индустриального общества в

информационное. Информационное общество - это социум с высокоразвитой системой каналов информационного обмена и телекоммуникаций, а также средств и систем защиты циркулирующей по ним информации [17, с. 20].

Суть информационного общества состоит не столько в производстве собственно информации, информационных продуктов и услуг, сколько в создании информационных технологий, способных обеспечивать производство, обработку и распространение информации, а также в разработке инфраструктур, ориентированных на применение средств и процессов информатизации. В процесс информатизации вовлекаются как отдельные физические и юридические лица, так и государственные органы, целые административно-территориальные образования, которые могут выступать авторами, владельцами или потребителями информации, программных информационных продуктов, информационных систем, технологий или услуг.

В процессе информатизации сферы материального производства, социальной сферы и сферы услуг немаловажная роль отводится компьютеризации, которая является порождением процесса информатизации общества и технической реализацией автоматизации производственной, управленческой, социальной и бытовой деятельности человека.

Процесс компьютеризации характеризуется:

- интеграцией естественных и гуманитарных наук;

- интенсификацией интеллектуального труда;

- изменением характера физического труда: встраивание процессоров в разного рода машины и оборудование, создание автоматизированных рабочих мест на базе персональных компьютеров, построение автоматизированных систем управления производством;

- стимулированием развития науки и техники: конструирование роботов различных уровней вплоть до создания искусственного интеллекта;

- усилением общественного характера новых технологий через создание глобальных, в том числе и мировых, информационных систем: превращением человека в явление био- социально - техногенное [18, с. 74].

Информатизация современного общества привела к формированию новых видов правонарушений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 15-20 лет резко увеличилось количество правонарушений с использованием компьютера или иной электронной аппаратуры, хищения наличных и безналичных денежных средств. Для совершения правонарушений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это правонарушения, в которых используются высокие технологии.

Так, по мнению начальника отдела по делам о преступлениях в сфере экономики и компьютерной информации Контрольно-методического управления Следственного комитета при Министерстве внутренних дел Российской Федерации (далее - МВД РФ) г. Егорова, в СССР первое преступление было совершено в 1979 году в Вильнюсе. Ущерб государству тогда составил 80 тысяч рублей - на эти деньги можно было приобрести 8 автомобилей «Волга». В России одним из первых наиболее крупных компьютерных преступлений считается уголовное дело о хищении 125,5 тыс. долл. США и подготовке к хищению еще свыше 500 тыс. долл. во Внешэкономбанке СССР в 1991 году.

В Казахстане первое наиболее крупное преступление с использованием компьютерных технологий имело место в 1994 году. Тогда это было первое уголовное дело против бывшего оператора Алатауского филиала КРАМС - банка г. Алматы Э.Р. Ордабаева, который путем использования ключевой шифровальной дискеты осуществил две фиктивные бухгалтерские проводки на сумму 6 млн. 795 тыс. тенге на счет малого предприятия «Анжелика» [19, с. 41].

В 1997 году в сфере высоких технологий на территории Российской Федерации было зафиксировано уже 300 преступлений, а в 2000 году - более 1300 [20]. На Украине в 2002 году было возбуждено 31 уголовное дело. В Казахстане до 2002 года было зарегистрировано всего 17 сходных преступлений.

Стремительное развитие глобальных информационных технологий, поставило перед органами внутренних дел Республики Казахстан задачи по выявлению новых видов преступлений (правонарушений) в сфере высоких технологий, в том числе и компьютерных. Все чаще современные информационно-телекоммуникационные и компьютерные технологии стали применяться криминальным миром для осуществления хищений и мошенничеств, распространения порнографии.

В этой связи, в системе Министерства внутренних дел Республики Казахстан (далее - МВД РК) в Департаменте криминальной полиции (далее - ДКП), в апреле 2003 г. было создано новое подразделение - Управление «К» (специальной оперативно-аналитической работы и раскрытия преступлений в сфере высоких технологий).

Одним из основных направлений деятельности подразделений по борьбе с правонарушениями в сфере высоких технологий является выявление и раскрытие правонарушений в телекоммуникационных и информационных системах:

- борьба с правонарушениями, связанными:

- с незаконным доступом к компьютерной информации;

- с незаконным оборотом радиоэлектронных и специальных технических средств;

- распространением предметов и информации, запрещенных в свободном обороте (порнографии, контрафактной продукции, вредоносных программ);

- борьба с правонарушениями в сфере телекоммуникаций, а также организация работы по использованию возможностей информационно-телекоммуникационных и компьютерных технологий для раскрытия правонарушений.

Можно согласиться с мнением ученых, что существующая практика свидетельствует о высокой степени латентности данного вида преступлений, недостатке квалифицированных специалистов, отсутствия следственной и судебной практики [21, с. 156].

Вместе с тем, для выявления и раскрытия данных правонарушений имеются реальные предпосылки.

На сегодняшний день Управлением «К» наработана практика проведения для органов внутренних дел технологической экспертизы средств компьютерной техники и программного обеспечения, в том числе выявления незаконного завладения паролями с помощью вредоносных программ типа «Троянец», модификации информации путем перевода системного времени компьютера для совершения хищений денежных средств, выявления информации порнографического содержания, а также использования телекоммуникационных ресурсов за чужой счет и перепрограммирования сотового телефона.

В качестве примера можно привести раскрытие хищения денежных средств путем мошенничества с использованием электронных платежных систем 3,5 миллиона тенге у Учреждения футбольного клуба «Наша компания» в г. Лисаковск Костанайской области.

Данное преступление не имело аналогов в Республики Казахстан. Оно было совершено с применением высоких компьютерных технологий и выхода в среду «Интернет». Учитывая латентность данного вида преступления, злоумышленник надеялся, завладев крупной суммой остаться безнаказанным.

По инициативе Управления «К» впервые в Республике успешно проведена технологическая экспертиза ЭВМ, получена распечатка соединений электронного почтового ящика, расположенного на сервере в другой стране (России), результаты которых подтвердили факт проникновения в программное обеспечение и несанкционированное изменение времени.

С МВД РФ достигнута договоренность о дальнейшем взаимодействии по обмену передовым опытом, а также оказанию содействия в наработке практики раскрытия компьютерных преступлений и использования специального оборудования и передовых технологий. Так в г. Москве были организованы курсы для обучения сотрудников подразделений «К».

В целях активизации раскрытия преступлений в сфере высоких технологий, совместно с подразделениями по борьбе с компьютерными преступлениями Российской Федерации и Киргизии проведено два оперативно-профилактических мероприятия, направленных на выявление фактов незаконного распространения предметов и информации, запрещенных в свободном обороте (порнографии, вредоносных программ, контрафактной продукции).

Кроме того, при поддержке Организации по безопасности и сотрудничеству в Европе разработан и внедряется пилотный проект «Создание основы оперативно-информационной системы в казахстанской полиции». В подразделениях «К» ДКП МВД РК и Департаменте внутренних дел (далее – ДВД) г. Алматы созданы отделы специальной оперативно-аналитической работы, которые анализируют все поступающие сведения и выдают объемную информацию для раскрытия правонарушений и установления криминальных и иных связей подозреваемых лиц.

В целях реализации положений Конвенции о преступности в сфере компьютерной информации [22] в структуре МВД РК в 2006 году был создан Национальный контактный пункт по борьбе с преступлениями в сфере информационных технологий, который обеспечивает межгосударственное взаимодействие и оперативное реагирование по фактам несанкционированного доступа к компьютерной информации.

Для создания системы коллективной безопасности в странах ближнего зарубежья, внедряется программа «СНГ-ВИЗИТ», предусматривающая обеспечение визово-миграционного контроля, в рамках которой продолжается развитие системы биометрической идентификации личности.

Управлением принимаются все возможные меры по пресечению криминальных посягательств на законные права и интересы граждан, охраняемые Конституцией Республики Казахстан.

Тем не менее по данным Управления «К», количество правонарушений с использованием информационных технологий с каждым годом возрастает.

Подобная тенденция, по мнению специалистов, складывается за счет роста пользователей сети Интернет, увеличения потока контрафактной продукции, большая часть которой поступает в Казахстан железнодорожным транспортом из бывших стран Содружества Независимых государств (далее - СНГ) и Китая [23]. Еще одним фактором, способствующим столь широкому росту правонарушений в указанной сфере, стало широкое использование безналичного расчета.

Так по данным ДКП МВД РК в период с 4 по 6 февраля 2015 года на территории республики проведено оперативно-профилактическое мероприятие «Контрафакт», направленное на выявление, пресечение и раскрытие правонарушений с использованием информационных технологий, а также выявление лиц, незаконно изготовляющих, тиражирующих и распространяющих продукцию, запрещенную в свободном обороте. В ходе проведения ОПМ выявлено 268 правонарушений.

В том числе по видам:

- нарушение авторских прав – 243;
- нарушение работы информационной системы – 3;
- неправомерное завладение информацией – 2;
- распространение вредоносных компьютерных программ – 3;
- неправомерное изменение ИМЕЙ-кода сотового телефона – 1;
- распространение порнографии – 8;
- распространение произведений, пропагандирующих культ жестокости – 2;
- незаконные использование СТС – 3.

Изъято 44276 единиц продукции запрещенной в свободном обороте, в том числе 44 тыс. контрафактных CD-DVD дисков, 125 дисков порнографического содержания, 31 дисков с нелицензионным программным обеспечением, 3 СТС и 72 единиц иной контрафактной продукции.

При проведении рейдовых мероприятий проверено 315 мест реализации аудио-видео продукции, 195 компьютерных клубов и Интернет-кафе, 82 фирм

по продаже компьютерной техники, на учет поставлено 151 лицо, задержанных за совершение указанных правонарушений.

Кроме того, в период проведения операции выявлена и пресечена деятельность 5 цехов (ДВД г. Астаны, г. Алматы, Актюбинской, Восточно-Казахстанской и Кызылординской обл.), по производству контрафактной продукции, пресечен 1 канал ввоза контрафактных дисков из Кыргызской республики (ДВД г. Алматы– 5 тыс. дисков).

Имеются яркие примеры работы в ДВД г. Астаны, г. Алматы, ВКО, Жамбылской области.

Сотрудниками подразделения «К» ДВД г. Алматы в помещении магазина «Компьютерная лавка» обнаружен цех, оборудованный для изготовления контрафактной продукции, где были установлены цветной принтер для изготовления полиграфии и нанесения голограмм на диски, также системный блок компьютера на котором установлены 6 CD-рекордеров для записи и копирования фильмов. На месте помимо техники также изъято 1520 экземпляров контрафактной продукции.

В ходе проведения ОРМ сотрудниками отдела «К» УКП ДВД г. Алматы на рынке «Азия» расположенного по ул. Северное кольцо, была пресечена деятельность канала оптовой поставки с территории Кыргызской Республики на территорию Республики Казахстан контрафактной аудиовизуальной продукции. По данному факту задержан житель г. Алматы, у которого в ходе осмотра его бутика обнаружено и изъято 4850 DVD дисков с внешними признаками контрафакта, которые предназначались для оптовой продажи на территории г. Алматы.

Сотрудниками УКП ДВД Жамбылской области в ходе ОПМ «Контрафакт» задержан житель Костанайской области, который изобличен в совершении преступления, предусмотренного ст. 207 ч. 1 УК РК («Нарушение работы информационной системы или информационно коммуникационной сетей». Так, в период времени с декабря месяца 2013 года по сентябрь месяц 2014 года он, используя специальное техническое средство, осуществлял

регулярные и непрерывные звонки (дозвоны) на диспетчерские телефоны таксопарка ТОО «НурАкбота Сервис» г.Тараз, вследствие чего нарушалась работа информационно-коммуникационной системы.

В 2014 году подозреваемый открыл в г.Тараз таксопарк «Адал-Такси» и пытался развить свой бизнес путем подавления конкурентов.

Изъято техническое средство под условным наименованием «SIM-BOX», назначена компьютерно-технологическая экспертиза. Ведется досудебное расследование по ст. 207 ч 1 УК РК – нарушение работы информационной системы и информационно-коммуникационной сети[24].

Все чаще жертвами правонарушений становятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Чаще всего мишенями лиц, совершающих правонарушения в сфере информационных технологий становятся банки. Особая актуальность вопросов защищенности технических средств приема, передачи и накопления информации от несанкционированного доступа была отмечена и отечественным законодателем, в частности Законом Республики Казахстан от 06 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» введением понятия «информационная безопасность» [13].

Остается актуальной проблема борьбы с организованной преступностью, которая, прибегая к услугам высококвалифицированных специалистов, стала все чаще использовать различные технические средства - от обычных персональных компьютеров и традиционных средств связи до сложных вычислительных систем и глобальных информационных сетей, в том числе и Интернет. Сфера применения компьютерных технологий в преступных целях весьма обширна. Так, по данным ДВД г. Алматы, практически каждый второй поддельный денежный знак изготавливается с использованием компьютерной обработки и распечатки на цветном принтере. Объясняется это, прежде всего общедоступностью такого рода информационных технологий и простотой их эксплуатации.

Компьютерно-информационные технологии функционируют относительно давно и их развитие, происходит огромными темпами, что связано с большой заинтересованностью ими широких слоев населения. Правонарушения, связанные с использованием компьютерной техники, - это лишь специализированная часть криминальной деятельности в информационной сфере [25, с. 189]. К данной категории относятся и правонарушения, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. С закреплением в УК РК отдельной главы 7 «Уголовные правонарушения в сфере информатизации и связи», предусматривающей ответственность за такого рода деяния, правоохранительные органы получили реальное средство борьбы с лицами, использующими компьютерную технику в криминальных целях.

Огромен и вред от такого рода правонарушений. По оценкам специалистов, в среднем экономический ущерб только от одного такого деяния в США составляет 450 тыс. долларов. Ежегодные же потери оцениваются: в США - 100 млрд. долларов; в Великобритании - 4,45 млрд. долларов; в странах Западной Европы - 30 млрд. долларов [26, с. 50]. Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Кроме того, следует отметить, что подобные правонарушения все чаще совершаются сотрудниками фирмы, банка или другого учреждения, которым в конечном итоге и наноситься ущерб. Например, в США компьютерные правонарушения, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами. В Казахстане то же существует такая тенденция. Так, в 2000 году в Лондоне были арестованы О. Зезов и И. Яримак, граждане Республики Казахстан, по обвинению в неавторизированном компьютерном проникновении, заговоре, нанесении вреда коммерции путем вымогательства и попытке нанесения вреда путем вымогательства с использованием корпоративной информации компании Bloomberg LP. Сумма шантажа составляла 200 тысяч долларов. Оба казахстанца были арестованы в аэропорту в момент передачи денег. Примечательно, что оба

они работали в компании, производящей базы данных для Bloomberg LP, и воспользовались полученной в ходе этого информацией для достижения своих криминальных целей. Суд над ними состоялся лишь летом 2002 года, исходя из сложности доказывания такого правонарушения. В США, где проходило судебное разбирательство, максимальный срок наказания по совокупности за эти правонарушения составляет 28 лет [27].

Компьютерные технологии и международные компьютерные системы создали новые условия, которые содействуют совершению правонарушений на национальном и международном уровнях. Преступные группы и сообщества в полной мере используют новейшие технологии для отмывания денег, добытых преступным путем, распространения неправдивой информации, несанкционированного доступа к информационным системам и совершения иных правонарушений. Доходы преступников, связанные с незаконным использованием новейших технологий, занимают третье место в мире после доходов от торговли наркотиками и оружием [28, с. 24].

В настоящее время существуют следующие крайне неблагоприятные тенденции развития правонарушений в сфере компьютерной информации, а именно:

- возрастание общего числа правонарушений в сфере компьютерной информации;

- корыстная мотивация большинства совершенных компьютерных правонарушений;

- усложнение способов совершения компьютерных правонарушений и появление новых видов противоправной деятельности в сфере компьютерной информации;

- высокий уровень криминального профессионализма компьютерных преступников;

- омолаживание компьютерных правонарушений и увеличение доли лиц, ранее не привлекавшихся к уголовной ответственности;

- увеличение материального ущерба от компьютерных правонарушений в общей доле ущерба от прочих видов правонарушений;

- рост удельного веса неправомерного доступа к компьютерной информации в структуре всех правонарушений в сфере компьютерной информации;

- рост неправомерного доступа к компьютерной информации в крупных городах (Астана, Алматы, Караганда).

Помимо перечисленных тенденций, прямо вытекающих из анализа статистических данных, опросы следователей и судей, специализирующихся в сфере борьбы с неправомерным доступом к компьютерной информации, а также предпринимателей и потенциальных потерпевших от неправомерного доступа к компьютерной информации, позволили выявить еще и такую тенденцию, как рост латентности (скрытости) этого вида правонарушений.

Наибольшую общественную опасность представляют правонарушения, связанные с неправомерным доступом к компьютерной информации. Однако компьютерная техника и средства коммуникаций на территории Республики Казахстан используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение электронного времени, а также денежных средств посредством электронной транзакции - вот далеко не полный перечень компьютерных правонарушений, с которыми вынуждены бороться правоохранительные органы США, Канады, стран Европы и т.д.), а в большей степени как средства криминальной деятельности. Причина - высокая латентность данного вида правонарушений и слабо развитые, а иногда даже отсутствующие компьютерно-информационные сети. «Невидимость» компьютерных правонарушений обусловлена во многом нежеланием самих жертв заявлять в правоохранительные органы [29, с. 14].

Одним из основных факторов, порождающих деформации правосознания, является высокая вероятность того, что лицо, совершившее компьютерное правонарушение, уйдет от ответственности. Сверхвысокий уровень латентности правонарушений в сфере компьютерной информации – явное

подтверждение безнаказанности лиц, их совершивших. Так шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка, даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1% компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, составляет меньше 10% [30, с. 32].

В виду высокого уровня латентности никто не знает точно всех масштабов компьютерной преступности. Считается, что только 10-15 % компьютерных преступлений становятся достоянием гласности преступности [17, с. 69].

Так, по данным Национального отделения Федерального бюро расследования (далее – ФБР) по компьютерным преступлениям от 85 до 97 % компьютерных посягательств даже не выявляются [31, с. 5]. По оценкам иных экспертов латентность «компьютерных» преступлений в США достигает 80 %, в Великобритании до 85 %, в ФРГ (далее – Федеративная Республика Германия) 75 %, в России более 90 % [32, с. 467].

По данным Информационно-аналитического Департамента Агентства Республики Казахстан по борьбе с экономической и коррупционной преступностью, в Казахстане в 2011 году было возбуждено 69 уголовных дела, в 2012 году - 74, в 2013 - 79 по ст. 227 ч. 1 УК РК от 16 июля 1997 года, что является ярким свидетельством латентности данного вида преступления [33].

Причины высокого уровня латентности компьютерных преступлений (ныне правонарушений) объяснимы:

- во-первых, возрастание функциональных возможностей информационных и компьютерных технологий затрудняет процесс обнаружения факта совершения компьютерного правонарушения;

- во-вторых, лица, ведущие дознание и следствие зачастую не обладают достаточным уровнем знаний в области компьютерной техники. Как показывают результаты анкетирования следователей и оперативных сотрудников Управления «К» при ДКП МВД РК, которое занимается

профилактикой и расследованием преступлений в сфере высоких технологий, высокая латентность компьютерных преступлений во многом связана с низким уровнем специальной подготовки сотрудников правоохранительных органов, их недостаточной активностью в борьбе с преступлениями в сфере компьютерной информации и игнорирование общественной опасности данной категории преступлений со стороны руководства органов внутренних дел и прокуратуры;

- в-третьих, отсутствие или недостаточность системы защиты компьютерных систем и сетей [21, с. 146].

Высказанные соображения позволяют сформулировать следующее краткое определение: латентная преступность в сфере компьютерной информации - это та часть реально существующей в определенных пространственно-временных границах фактической преступности в сфере компьютерной информации, которая представляет собой кумулятивный (накопительный) массив данных преступлений (правонарушений) и совершивших их лиц, не выявленных органами уголовной юстиции и не учтенных уголовной статистикой, в пределах сроков давности привлечения к уголовной ответственности.

Негативные последствия латентной преступности в сфере компьютерной информации состоят в том, что она:

- искажает представления о фактических размерах преступности в сфере компьютерной информации, ее состоянии, структуре, динамике, о величине и характере ущерба, причиненного неправомерным доступом к компьютерной информации - как одного из наиболее латентных преступлений (правонарушений) в сфере компьютерной информации;

- уменьшает степень достоверности прогнозов преступности в сфере компьютерной информации, затрудняет определение направлений борьбы с ней;

- препятствует реализации принципа неотвратимости ответственности за совершенные преступления (правонарушений) в сфере компьютерной информации;

- способствует росту преступности в сфере компьютерной информации, особенно рецидивной;

- снижает активность граждан в борьбе с преступностью в сфере компьютерной информации.

Путями преодоления латентности преступлений (правонарушений) в сфере компьютерных технологий, в том числе и неправомерного доступа к компьютерной информации, можно назвать следующие:

- использование социологических методов и приемов выявления и измерения латентной преступности в сфере компьютерной информации: массовый опрос населения, анкетирование, экспертные оценки;

- преодоление правового нигилизма руководителей учреждений, предприятий, организаций и отдельных граждан путем освещения проблем компьютерной преступности в средствах массовой информации;

- повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов.

Еще одна из причин роста таких преступлений (правонарушений) в Казахстане – это разрыв в уровнях развития информационного общества по сравнению с Западом, порождающий иногда абсурдные ситуации, нестыковки моральных, правовых стандартов и норм. Создаются условия для соблазна, искушения воспользоваться более удобной и дешевой формой обеспечения информацией. Взять, например, проблему сохранения интеллектуальной собственности. Лицензионные программы стоят очень дорого для массового потребителя и нет моральных преград пользоваться «взломанными» программами, которые во много раз дешевле [34, с. 43].

Одним из новых направлений для криминальной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет (International Network – международная система связи). В настоящее время Интернет,

использующая в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками, объединяющую около 30 000 мелких локальных сетей и более 30 миллионов пользователей, число которых постоянно растет. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом криминального посягательства, но и очень эффективным средством совершения преступлений (правонарушений).

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных минипроцессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам Интернет позволяет передавать не только аудио, но и видео, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, - возможность осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма за-интересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. Кроме того, существует проблема распространения в сети информации порнографического характера, которая, согласно ст. 311 нового УК РК, является уголовно-наказуемым деянием. Вот только несколько примеров из международной практики:

- осенью 1998 года полицейские органы 12 стран мира в ходе совместной операции «Собор» арестовали 107 членов закрытого Интернет - клуба «Страна чудес», имевших доступ к 100 тысячам файлов детской порнографии. План операции придумали британцы, задержавшие 11 интернет - педофилов и раскрывшие их базу в Сассексе. По этому делу в США было арестовано 32 человека, в Германии - 18, в Италии - 16. По итогам операции «Собор» осенью 2000 года в Великобритании появился спецотдел «компьютерной полиции» по борьбе с интернет - маньяками и хакерами;

- С. Савушкин и О. Пьяницкий, жители России, находясь в Ростове-на-Дону, открыли порно-сайт на сервере Paradise Web Hosting в Америке. Банковский счет был открыт в Real Internet Company Inc. в Канаде. Переведя на этот счет от 9 до 25 долларов в качестве абонентской платы, любой человек мог ознакомиться с порнографической информацией самого различного характера. В ходе оперативно - следственных мероприятий по виртуальному адресу был вычислен реальный адрес одного из злоумышленников, и вскоре оба они были задержаны. Их доходы составили 1-2 тысячи долларов в месяц, однако эта цифра лишь то, что удалось доказать следствию. Реальные цифры скрыты за тайной канадских банковских вкладов [35].

Особо следует отметить опыт зарубежных стран для борьбы с такими правонарушениями. Так, в США в «компьютерной столице» страны - Сан-Хосе в штате Калифорния ФБР объединило службы, занимающиеся расследованием компьютерных преступлений в единую бригаду, что существенно повысило не только уровень раскрытия преступлений, но и сделало возможным практически мгновенную реакцию ФБР не только на заявления о данных преступлениях, но и на самостоятельное их выявление.

Следует отметить, что понятие «компьютерных» или же «информационных» правонарушений базируется исключительно на действующем уголовном законодательстве в этой области. Действительно, в Республике Казахстан – глава 7 «Уголовные правонарушения в сфере информатизации и связи» предусматривает 9 составов правонарушений, в

России, например, глава 28 Уголовного кодекса Российской Федерации (далее – УК РФ) «Преступления в сфере компьютерной информации» предусматривает три состава преступлений - ст. 272-274 [36]. Название соответствующей главы в УК РФ некоторые российские ученые связывают с тем, что в формулировании соответствующих составов преступлений законодателем акцент был сделан на защиту именно самой компьютерной информации. Вместе с тем в ходе проведенного нами анализа действующего в Казахстане уголовного законодательства было установлено, что при совершении ряда других правонарушений могут использоваться информационные технологии, и как показывают приведенные выше примеры различных тенденций развития подобных правонарушений, используются они преступниками довольно эффективно. Приведем перечень некоторых действий преступников, использующих информационные технологии, и соответствующие им составы правонарушений, предусмотренных в законодательстве РК:

1. Распространение через каналы сети Интернет и местных локальных сетей:

- заведомо ложных сведений, порочащих честь и достоинство лица или подрывающих его репутацию – ст. 130 УК РК «Клевета»;

- информации, связанной с унижением чести и достоинства лица, выраженной в неприличной форме - ст. 131 УК РК «Оскорбление»;

- сведений о частной жизни лиц, составляющих их личную или семейную тайну – ст. 147 УК РК «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите», тайну переписки, телефонных переговоров, почтовых, телеграфных или других сообщений – ст. 148 УК РК «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;

- информации, призывающей к развязыванию агрессивной войны – ст. 161 УК РК «Пропаганда или публичные призывы к развязыванию агрессивной войны», к насильственному изменению государственного строя – ст. 180 УК РК «Сепаратистская деятельность», составляющей государственную тайну – ст.

185 УК РК «Незаконное собирание, распространение, разглашение государственных секретов» и т.п.;

- информации порнографического характера – ст. 311 УК РК «Незаконное распространение порнографических материалов и предметов».

2. Мошенничество в сфере использования азартных игр (лотереи и тотализаторы), организации финансовых пирамид, фиктивных брачных контор и фирм по оказанию несуществующих услуг – ст. 190 УК РК «Мошенничество».

3. Получение вознаграждения за неразглашение сведений, полученных в ходе несанкционированного доступа к информации, составляющей коммерческую или банковскую тайну, – ст. 194 УК РК «Вымогательство», ст. 223 УК РК «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну».

4. Незаконное копирование и продажа программных продуктов, находящихся на серверах компаний, которые являются владельцами этих программ, с присвоением их авторства другим лицом либо компанией – ст. 198 УК РК «Нарушение авторских и (или) смежных прав», а также использование преступником логотипа или наименования товара другой фирмы – ст.222 УК РК «Незаконное использование товарного знака».

5. Изготовление с использованием средств компьютерной техники поддельных денежных знаков и документов – ст. 231 УК РК «Изготовление, хранение, перемещение или сбыт поддельных денег или ценных бумаг», ст. 232 УК РК «Изготовление или сбыт поддельных платежных карточек и иных платежных и расчетных документов», ст. 233 УК РК «Нарушение порядка и правил маркировки подакцизных товаров акцизными марками и (или) учетно-контрольными марками, подделка и использование акцизных марок и (или) учетно-контрольных марок» и т.п.

Таким образом, уголовная ответственность за использование информационных технологий для совершения правонарушений охватывает довольно большой перечень общественных отношений, гораздо обширнее, на

наш взгляд, чем отношения в области компьютерной информации, но менее обширный, чем информационные отношения.

Исходя из вышеизложенного необходимо отметить, что с развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называли веком энергетики, то XXI - веком информатики. По мнению В. П. Сальникова ныне действует правило: «кто владеет информацией, тот владеет миром» [37, с. 101]. Научно-технический прогресс принес человечеству такие незаменимые в современной жизни новшества, как компьютеры и Интернет. Повсеместное внедрение данных технологий повлекло за собой возникновение новых видов ресурсов - информационных. Информация обрела реальную цену и с развитием информационных технологий становится все более ценным товаром. Но новые технологии стимулировали возникновение и развитие и новых форм преступности, в первую очередь компьютерных. Основную часть в этой сфере совершается с помощью компьютерных сетей. В последние годы специалистами замечена тенденция стремительного роста компьютерных преступлений (правонарушений) посредством глобальной компьютерной сети Интернет. Поэтому многие ученые предлагают дополнять составы компьютерных правонарушений, такими новыми составами, как "компьютерная клевета", "компьютерный шпионаж", "компьютерное хищение". Это объясняется тем, что компьютерные правонарушения посягают не просто на экономические интересы общества и государства, но и на национальную безопасность, а также на конституционные права человека, его честь и достоинство[29, с.19]

## 1.2 Интернет как межгосударственная сфера криминальных посягательств с использованием высоких технологий

Современную жизнь человека невозможно представить без использования сети Интернет. И, как правильно отмечают некоторые ученые

"Всемирная паутина- информационно-телекоммуникационная сеть Интернет является не только бесспорным достижением современности, она впитала в себя многие известные пороки общества и уже начала создавать новые формы и виды преступной деятельности"[30]. Верно считают Даровских Ю.В. и Д.А. Григорьев, что используют сеть Интернет для распространения наркотиков, детской порнографии, совершению иных правонарушений, распространению экстремизма[31, с. 81]

Кроме того значительные достижения человечества в развитии высоких технологий, беспрецедентное расширение международной коммерческой и экономической деятельности привели к росту транснациональной преступности, к совершению преступлений, механизм которых заведомо предусматривает одновременную или продолжаемую преступную деятельность в нескольких государствах, к совершению преступлений межгосударственного характера (в частности, незаконный оборот наркотиков, фальши-вомонетничество, пиратство, неправомерный доступ к компьютерной информации и т.д.) [32, с. 8]**.**

Так, гражданин Российской Федерации Владимир Левин, находясь в Санкт-Петербурге, осуществил более 40 попыток перевода денег из американского «Сити-банка» в банки, расположенные в Великобритании, ФРГ, Израиле, Финляндии.

Преступность не только распространяется до межгосударственных масштабов, но и становится более криминально профессиональной и технически вооруженной. «...Специалистами прогнозируется рост организованной преступности, связанной с использованием электронных средств, одним из которых является компьютер. Финансовые системы мира, несомненно, во все большей степени будут подключаться к существующим и вновь образуемым электронным компьютерным сетям, на которые в настоящее время опирается все мировая экономика, что неизбежно приведет к появлению все большего желания обогащения со стороны преступных, групп и сообществ» [33]**.** Преступные группы и сообщества активно используют в своей

деятельности новейшие разработки науки и техники: от современнейших транспортных средств, средств связи и вооружения до компьютерных систем и информационно-обрабатывающих технологий.

Сегодня объем информации (коммерческой, финансовой, военной, частной), сохраняемой и передаваемой с помощью компьютеров, компьютерных систем и их сетей, превысил все вообразимые пределы. Появился новый вид предпринимательской деятельности - информационный бизнес, товаром в котором выступают информационные и коммуникационные технологии. «Информационные технологии - товар не совсем обычный. На рынке они выступают в двух ипостасях: как продукт потребления и как средство производства, поскольку от них зависит информационное обеспечение рынка. Ни в каком другом виде человеческой деятельности этого нет, и это характеризует качественно новый уровень развития общества» [34, с. 17]**.**

По данным Торговой палаты США ежегодные потери до 330 миллионов долларов - это минимальный вред от компьютерных преступлений. Во Франции эти потери доходят до 1 млрд. франков в год, в Германии при помощи компьютеров ежегодно похищается около 4 млрд. марок [35, с. 7]**.**

Электронное мошенничество, корпоративный шпионаж в коммерческих сетях, взломщики, вторгающиеся в компьютерные системы через Интернет - это реалии сегодняшнего дня. В уголовно-правовом аспекте Интернет можно рассматривать в двух плоскостях:

а) как инструмент для совершения преступлений [36, с. 4];

б) как пространство, дающее возможность преступникам обмениваться информацией криминального характера и ведения разнообразной преступной деятельности.

С одной стороны Интернет предоставляет неограниченные возможности общения миллионам пользователей компьютеров, представляет собой новую эру в области информационного обмена. С другой, внедрение средств электронно-вычислительной техники в обыденную жизнь, рост парка современных компьютерных систем, доступность пользования глобальной

компьютерной сетью Интернет привели к превращению последней в гигантское виртуальное киберпространство, в государство без границ [37, с. 21]. В этом киберпространстве «обитают» пользователи, представляющие собой сообщество людей, сопоставимое с населением большого государства.

Мировое сообщество вступило в эру информационного бума - ведь современная цивилизация во многом зависит от новых телекоммуникационных технологий, которые используются практически во всех сферах деятельности человека. Они необратимо изменили образ жизни граждан, способы их общения. Но у прогресса есть и негативная сторона - снизилась уверенность общества в неотъемлемом праве граждан на защиту конституционных прав и свобод, включая на защиту частной жизни. Каждый из нас становится все более зависимым от информации, циркулирующей в глобальных компьютерных сетях, ее достоверности, защищенности, безопасности. Развитие информационных и сетевых технологий привело к появлению так называемой киберпреступности. Этот термин казахстанским законодательством юридически не определен, и, тем не менее, само понятие уже прочно вошло в нашу жизнь.

Существует много споров вокруг приставки «кибер-» в отношении преступлений, совершаемых в сети Интернет. По большому счету, киберпреступность - это преступность в так называемом виртуальном пространстве. Само виртуальное пространство некоторые специалисты определяют как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи [38, с. 38]. Это определение вполне соответствует рекомендациям экспертов ООН. По их мнению, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы

или сети, в рамках компьютерной системы или сети либо против компьютерной системы или сети. Следовательно, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

Киберпреступники используют в сетях самые различные виды атак, позволяющие им проникнуть в корпоративную сеть, перехватить управление ею или подавить информационный обмен в сетях. Компьютерные вирусы, в том числе сетевые черви, модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем, логические бомбы, срабатывающие при определенных условиях, «троянские кони», отсылающие своему «хозяину» через Интернет различную информацию с зараженного компьютера, - все это своего рода атаки [39].

Оружие киберпреступников постоянно совершенствуется, способы информационных атак становятся все более изощренными, и в перспективе можно ожидать появления новых нетрадиционных видов сетевых атак и компьютерных преступлений.

Первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений стала Конвенция о преступности в сфере компьютерной информации, принятая Советом Европы 23 ноября 2001 г. [22]. В ней определены скоординированные на национальном и межгосударственном уровнях действия, направленные на недопущение несанкционированного вмешательства в работу компьютерных систем, отражены киберпреступления, совершенные в информационной среде, или против информационных ресурсов, или с помощью информационных средств. Поскольку Конвенция направлена на усиление борьбы с кибер-преступностью, что предполагает тесную кооперацию между правоохрани-тельными структурами различных государств, она наделяет правоохрани-тельные органы государств-участников весьма широкими полномочиями.

По словам экспертов, жертвами киберпреступников могут стать как один человек, так и группа лиц. В первом случае преступники создают различные сайты, чаще всего сексуального характера, от имени какого-либо лица. В этом

случае правонарушители размещают в сайтах знакомств фото и анкету с указанием адреса и телефона девушек под видом женщин легкого поведения. Ко второй категории потенциальных жертв киберпреступников относятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Так, по данным МВД РК, наибольшее количество правонарушений было совершено в отношении таких компаний, как Microsoft, «1С», «Меломан», «Азия хит», но были и случаи причинения ущерба другим предприятиям и учреждениям, в том числе государственным. Пострадали от рук киберпреступников и некоторые банки и компании сотовой связи [23].

Согласно данным Управления «К» возраст граждан, совершающих преступления в сфере информационных технологий, колеблется в промежутке от 13 до 25 лет. При этом киберправонарушителей условно можно разделить на две категории: профессиональные хакеры и подростки хулиганы. Первые, как правило, люди с высшим образованием, разбирающиеся не только в способах незаконного проникновения в информационные банки данных, но и в юридических тонкостях ухода от ответственности за эти действия. Ко второй группе относятся, как уже было сказано, подростки 13–15 лет, имеющие домашний компьютер и доступ к мировым информационным ресурсам и совершающие компьютерные правонарушения из хулиганских побуждений.

В августе 2008 г. семнадцатилетний житель Экибастуза создал сайт в Интернете от имени оператора сотовой связи «Билайн». На нем была размещена недостоверная информация о том, что компания проводит специальную акцию. Для участия в «акции» нужно было отправить на сайт коды карт экспресс-оплаты. Взамен юный мошенник предлагал возвращение оплаченной суммы в пятикратном размере. Сайт через две недели после его существования был разоблачен службой безопасности ТОО «КаР-Тел» [40].

В начале августа 2008 г. представители информационного агентства «Казахстан Сегодня» сообщили, что их веб-сайт систематически подвергается массированным DoS-атакам, в связи с чем доступ к сайту агентства был

некоторое время затруднен. Об этом сообщили в компании SoftDeCo, которая предоставляет услуги хостинга. Вместе с массированными хакерскими атаками сайт-блога продолжалась блокировка данного сайта. По заявлению владельцев сайта, причиной этому послужили публикации ряда статей о коррупции в государственных органах

Закон о СМИ относит веб-сайты к средствам массовой информации и приостановление либо прекращение выпуска (выхода в эфир) СМИ может осуществляться только по решению собственника либо суда, о чем в уполномоченный орган направляется уведомление (п. 5 ст. 13 закона о СМИ). [41].

В начале 2010 г. «Газета.kz» стала жертвой кибермошенников. Неизвестные преступники через Интернет проникли в редакционные компьютеры и вывели из строя несколько программ. Журналисты, которые вели деловую переписку с иностранными корреспондентами и коллегами по офису, в один момент потеряли все. Кто-то изменил пароли, необходимые для входа в программу, и забрал всю хранящуюся в компьютерах информацию.

Через несколько дней пришли письма, в которых мошенники предлагали вернуть все данные и восстановить поврежденные программы всего за пять долларов. Деньги следовало перевести на указанный в письме электронный банковский счет. Редакция «Газеты.kz» обратилась в полицию.

Как отмечает глава Управления «К» отдела по борьбе с преступлениями в сфере информационных технологий Инна Петрищева, это нарушение можно рассматривать по нескольким статьям УК РК, но самое главное – это незаконное проникновение в закрытые компьютерные сети [42].

Также известно, что в прошлом году мошенники заработали через Интернет около пяти миллиардов долларов. И хотя наша страна не полностью охвачена Всемирной сетью, отечественные хакеры и киберпреступники работают на высоком уровне.

Сейчас отдел по борьбе с правонарушениями в сфере информационных технологий занимается отловом телефонных мошенников, хакеров и производителей пиратских DVD.

Если вы стали жертвой хакеров, ничего не предпринимайте. Ваш компьютер – это место правонарушения. Не стоит удалять ставшую ненужной программу или соглашаться на условия мошенников. Ведь взломанная программа – это вещественное доказательство.

Глава Управления «К» называет подобные действия DoS-атакой, поскольку рассылаемый взломанной программой вирус разойдется моментально и без вашего участия. В обычной ситуации вас бы могли назвать соучастником этих мошенников, хотя на самом деле вы являетесь пострадавшим.

За последнее десятилетие в Казахстане наблюдается рост числа пользователей сети Интернет. Так по итогам 2007 года плотность пользователей Интернет составляла 4 на 100 жителей; в 2008 году — 11 на 100 жителей; в 2009 году — 28 на 100 жителей; в 2010 году — 59 на 100 жителей; в 2011 году — 71 на 100 жителей; в 2012 году — 84 на 100 жителей; в 2013 году — 87 на 100 жителей; в 2014 году — 91 на 100 жителей [23].

Во многих странах мира в целях пресечения факта информационного правонарушения в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль хакера, позволяющий выявить уровень его квалификации и технической подготовки [43, с. 28]. Но следует отметить, что хотя компьютерные специалисты и могут многое сказать о хакере и о методах его работы, но они никогда не смогут понять психологию его криминального мышления. Подобными вопросами занимаются клинические психологи, судебные эксперты и другие специалисты совместно с органами внутренних дел. Эксперты считают, что налаживание подобной практики и в нашей республике, где правонарушения в сфере информационных технологий пока неразвиты, позволит еще в зачаточной форме уничтожить основы киберправонарушений.

Доказать причастность лица к совершению информационного правонарушения непросто. Национальный контактный пункт по борьбе с

правонарушениями в сфере информационных технологий ведет системную борьбу с правонарушениями подобного рода. В настоящее время осуществляется постоянный обмен информацией со странами СНГ и дальнего зарубежья. Кроме того, МВД РК было инициировано введение уголовной ответственности за неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства. В настоящее время достигнута договоренность с представителями банковских структур о сотрудничестве по выявлению фактов электронного мошенничества.

Уникальность Интернет заключается в том, что она не находится под юрисдикцией ни физического лица, ни какой-либо страны. Это информационное пространство не имеет государственных границ, оно пронизывает пространство десятков государств мира, объединяя многомиллионную многонациональную сеть пользователей. В нем отсутствуют государственное регулирование и иные формы контроля за безопасностью, законностью пользования, сохранностью циркулирующей информации.

В Интернете существуют безналичные финансы (в виде электронных банковских расчетов), электронная наличность (в виде дебетовых пластиковых карт и электронных монеток), кредитные карты. Как любое государство Интернет «населяют», наряду с позитивными пользователями, криминально ориентированные «кибер-сограждане».

Совершая правонарушение в киберпространстве Интернета, виртуальный преступник остается безнаказанным. Нормы международного права остаются неприменимыми, поскольку Интернет не имеет государственных границ. В связи с этим, Американская Ассоциация юристов выступила с предложением законодательного регулирования киберпространства Интернета. В этих целях разрабатывается специальная «киберюрисдикция», предусматривающая для сайтов «электронную прописку», которая будет выдаваться при регистрации

сайта. Вводятся понятия «кибергранница», «кибертрибунал», который будет ответственен за соблюдение законности в киберпространстве.

Мировая практика идет двумя путями в правовом решении проблемы преступности с использованием высоких технологий:

- принятие правовых норм по отдельным видам преступлений и видоизменение традиционных уголовно наказуемых деяний в национальных уголовных законодательствах;

- принятие отдельных правовых норм, объединенных единым объектом преступного посягательства.

Решение проблем преступности в сфере компьютерной информации в Модельном уголовном кодексе стран СНГ [44], носящем рекомендательный характер для законодательства этих стран, идет по второму пути. В этом Кодексе содержится раздел ХП «Преступления против информационной безопасности» с одноименной главой 30.

С целью пресечения и профилактики такого рода криминальных посягательств в современных уголовных кодексах государств - стран СНГ введены статьи, предусматривающие уголовную ответственность за правонарушения в сфере обращения компьютерной информации.

С учетом того, что на территории бывшего СССР сохранилось «единое криминальное пространство», а национальные уголовные законодательства имеют свои особенности, государства - члены СНГ предпринимают совместные усилия по противодействию существующей преступности. Правовой основой такого содружества является Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, подписанная 22 января 1993 года главами государств Содружества [45].

На сегодняшний день в Казахстане киберпреступность пока не имеет таких масштабов, как в зарубежных странах. Но тенденция развития киберпреступности во всех странах мира, независимо от их географического положения, вызывают необходимость выделения все больших сил правоохранительных органов для борьбы с данным видом преступлений. Это

проблема касается не только работников правоохранительных органов, но и сотрудников спецслужб, служб безопасности банков, специалистов и экспертов в области информатики, представителей учебных и научно-исследовательских учреждений, в том числе и экспертов по компьютерным вирусам, компьютерной технике и программному обеспечению.

Эффективное решение проблемы киберпреступности требует согласованных международных действий и сотрудничества. Однако это возможно только в том случае, если существует общее понимание проблемы как таковой и необходимости рассмотрения соответствующих решений.

## 1.3 Состояние борьбы с компьютерными правонарушениями в зарубежных странах

Одним из методов исследования и последующей подготовки научно-обоснованных рекомендаций является сравнительное правоведение. Оно дает возможность использовать положительный опыт других государств в процессе принятия собственных законодательных решений.

Термин «компьютерная преступность» был введен в США в начале 60-х годов Д.Б. Паркер, которая выделила новый вид преступлений, в которых ЭВМ является как объектом преступления, поскольку ей причиняется материальный ущерб путем физического повреждения, так и орудием совершения преступления, когда ее используют для получения политических или деловых преимуществ [46, с. 8].

Широкое внедрение электронно-вычислительных машин в повседневную жизнь резко увеличило число преступлений в сфере компьютерной информации. Начались интенсивные научные исследования этого феномена, процесс формирования национального законодательного массива. Первой страной, внесшей изменения в законодательство в связи с появлением «злоупотреблений при помощи компьютера» стала Швеция. В сентябре 1973 года там был принят «Закон о данных», статья 21 которого предусматривала

уголовную ответственность за неправомерное обращение с данными (несанкционированный доступ к компьютерной информации).

В США первые составы отдельных компьютерных преступлений были сформулированы в 1979 году на Конференции Американской ассоциации адвокатов в Далласе:

- использование или попытка использования компьютера, вычислительной системы или сети компьютеров с целью получения денег, собственности или услуг, прикрываясь фальшивыми предлогами и ложными обещаниями или выдавая себя за другое лицо;

- преднамеренное несанкционированное действие, имеющее целью изменение, повреждение, уничтожение или похищение компьютера, вычислительной системы, сети компьютеров или содержащихся в них систем математического обеспечения, программ или информации;

- преднамеренное несанкционированное нарушение связи между компьютерами, вычислительными системами или сетями компьютеров [47, с. 4].

К 1983 году законы, относящиеся к компьютерной преступности, были введены в 18 штатах, а к 1986 году эта цифра увеличилась более чем в два раза. На федеральном уровне разработка законодательства по компьютерной преступности ведется с 1984 года. Первый американский закон в этой области назывался «Закон об использовании электронных устройств, обеспечивающих несанкционированный доступ к ЭВМ, злоупотреблениях и мошенничестве при помощи компьютера».

В Уголовном кодексе США компьютерное преступление определяется как ряд мероприятий с использованием компьютера с целью извлечения выгоды, которые нанесли или могли нанести, ущерб или прямое незаконное использование компьютеров в совершении преступления или любое незаконное действие, для успешного осуществления которого необходимы знания компьютерной технологии [48, с. 18].

В период с 1981 по 1986 годы были внесены соответствующие изменения в уголовные законодательства Великобритании, Канады. Дании. Австрии, ФРГ. Наиболее последовательная реформа уголовного законодательства была проведена в ФРГ. В преступлениях с использованием ЭВМ были выделены две основные группы:

- экономические преступления (компьютерные мошенничество, шпионаж и диверсии);

- преступления против индивидуальных интересов (связанные с нарушением прав граждан на личную тайну).

Принятие в 1986 году (после 10 лет разработки и обсуждения) Второго закона о борьбе с экономическими преступлениями позволило ФРГ догнать стран - мировых лидеров в области законодательного реформирования вопросов уголовной ответственности за компьютерные преступления. Закон содержит семь статей, относящихся к компьютерной преступности: о мошенничестве с использованием ЭВМ, о фальсификации компьютерных данных, об утаивании электронных данных, о получении данных разведывательными средствами, об изменении данных в ЭВМ, о компьютерном саботаже [49, с. 85].

Затем аналогичные изменения были проведены Францией, Японией, Грецией, Австрией. В настоящее время уголовные законодательства более 100 стран мира содержат нормы, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации

Криминологические прогнозы констатируют рост преступности в мире, средний ее прирост составляет 5 % в год. Наиболее интенсивно растет корыстная и «беловоротничковая» преступность. Особую опасность представляют преступления, связанные с компьютерными операциями, безналичными деньгами, технологическими секретами, новыми видами мошеннических действий высокообразованных людей [32, с. 470].

С проблемой быстрорастущей компьютерной преступности возникает потребность мирового сообщества в создании правовых норм-ориентиров для развития и совершенствования национальных законодательств.

Межгосударственное сотрудничество в области борьбы с преступностью, в разрешении проблем экономического, социального и гуманитарного характера предусмотрено п. 3 ст. 1 Устава Организации Объединенных Наций (далее – ООН). На 7 Конгрессе ООН в 1985 году были разработаны руководящие принципы в области предупреждения преступности, выработанные на основе анализа ее новых форм, в том числе порожденных научно-техническим прогрессом, который связан с увеличением числа преступлений, когда преступниками становятся люди, с одной стороны, не подготовленные к управлению автоматизированными системами и совершающие преступления по неосторожности, с другой - те, кто, овладев новой техникой, используют ее возможности для злоупотреблений, что, в частности, привело к возникновению компьютерного мошенничества [50, с. 86].

В целях определения международной политики в борьбе с компьютерными преступлениями и создания эталонной схемы закона об уголовной ответственности за их совершение Organization for Economic Cooperation and Development – Организацией экономического сотрудничества и развития (далее – ОЭСР) были проведены исследования национальных уголовных законодательств и опубликован в 1986 году доклад на тему; «Преступления, связанные с применением компьютеров: анализ политики в области права». Был рекомендован минимальный Список правонарушений, относящихся к компьютерным преступлениям, и принято за основу следующее определение компьютерного преступления: «Компьютерным преступлением считается всякое незаконное, неэтичное и несанкционированное поведение, касающееся автоматизированных процессоров и трансмиссии данных» [51, с. 5].

Вслед за ОЭСР аналогичные исследования в целях унификации национальных уголовных законодательств и формулирования состава компьютерного преступления были проведены в рамках Европейского Совета, Кабинет Министров которого принял в сентябре 1989 года Рекомендацию № R (89)9. Она включает Минимальный и Необязательный списки нарушений.

В 1994 году эксперты ООН классифицировали компьютерные преступления на:

- мошенничество путем манипуляций на компьютере:

- компьютерный подлог;

- причинение ущерба путем изменения данных или программ;

компьютерный саботаж (незаконное изменение, подавление или уничтожение компьютерных данных или функций, с целью помешать нормальному функционированию системы);

- несанкционированный доступ к компьютерным системам и услугам;

- незаконное копирование программ [52, с. 7].

Не меньший интерес мирового сообщества вызывает и проблема защиты частной тайны, содержащейся в «компьютеризированной» форме. ОЭСР в 1977 году выработала в качестве общих принципов рекомендации построения уголовно-правовой защиты частной жизни, которые были одобрены 22 странами - ее членами.

Рекомендации содержали следующие принципы: а) сбор данных должен ограничиваться определенными рамками, производится законным путем и с ведома и согласия субъекта; б) данные должны соответствовать заявленной цели и быть точными и полными; в) цели сбора должны быть четко определены не позднее периода сбора; г) персональные данные не должны раскрываться и использоваться для иных целей, кроме как с согласия субъекта; д) при сборе данных должны соблюдаться меры защиты; е) субъект имеет право доступа к данным и их контроля; ж) сборщик данных должен отчитываться за соблюдение перечисленных принципов. На основе рекомендаций в Великобритании, США, Японии, Израиле, Италии, Австрии, Австралии были приняты специальные законы о защите персональных данных и частной тайны.

Расширение использования компьютерных технологий в самых разнообразных сферах жизни общества порождает общественно-опасное посягательства в виде злоупотребления не только на экономические интересы общества, но и частные интересы граждан. Существует вероятность

перерастания компьютерных преступлений в преступления против личности (с учетом компьютеризированного медицинского обслуживания), в посягательства на государственные интересы (с учетом компьютеризации систем управления всеми видами транспорта, атомными электростанциями).

Одним из условий создания эффективной системы противодействия компьютерной преступности является развитие и совершенствование законодательства, обеспечивающего уголовно-правовую защиту компьютерной информации.

На седьмом пленарном заседании Межпарламентской ассамблеи государств-участников СНГ 17 февраля 1996 года был принят Модельный уголовный кодекс для стран-участников СНГ, содержащий раздел XII «Преступления против информационной безопасности» [53].

Кроме того, в Модельном кодексе предусматривается ответственность за совершение преступлений, связанных с использованием компьютера или посягающих на компьютерную информацию.

Например, хищение, совершенное путем использования компьютерной техники (ст. 243); причинение имущественного ущерба путем обмана, злоупотребления доверием или модификации компьютерной информации (ст. 250); незаконное получение информации, составляющей коммерческую или банковскую тайну путем перехвата в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств (ст. 269); нарушение правил обращения с содержащими государственную тайну документами или компьютерной информацией (ст. 300) [53, с. 167].

Законодательство стран СНГ по-разному оценивает степень общественной опасности компьютерных преступлений. За их совершение предусмотрена ответственность в виде лишения свободы, штрафа, ареста, ограничения свободы, исправительных работ, лишения права занимать определенные должности или заниматься определенной деятельностью, выполнения общественных работ. Наиболее строгое наказание предусмотрено за создание, использование и распространение вредоносных программ для компьютера.

На сегодняшний день в Республике Казахстан ежемесячно происходит более 500 атак хакеров на информационные сети государственных органов Казахстана [54]. Электронные взломщики регулярно пытаются взломать базы данных банков и коммерческих предприятий, чтобы снять крупные суммы денег или получить конфиденциальную информацию. Борьба спецслужб с киберпреступностью осложняется тем, что и государственные органы, и частные компании зачастую скрывают информацию о нападениях. К тому же, большинство хакеров, совершают электронные налеты из-за рубежа.

Широкое использование современных информационных технологий в управленческих и финансовых структурах, а также в обществе в целом выдвигает решение проблемы информационной безопасности в число приоритетных задач [55, с. 5]. Кроме прямого ущерба от возможной утечки, информация может превратиться в средство подавления свободы человека, стать источником серьезной угрозы государственности и духовной жизни личности.

В этой связи приняты государственные программы обеспечения информационной безопасности, обеспечения защиты государственных секретов, Концепция обеспечения информационной безопасности, а также ряд других организационных и практических мер, которые реализуются государственными органами Республики Казахстан во взаимодействии с Комитетом национальной безопасности (далее - КНБ).

Анализ уголовного законодательства стран СНГ позволяет утверждать, что большинство стран принимает необходимые меры, направленные против преступности в сфере компьютерной информации. Однако нормы законодательства не совершенны и нуждаются в значительной доработке. Делается попытка четкого определения применяемой терминологии и унификации уголовно наказуемых деяний. Об этом свидетельствует подписанное 1 июня 2001 г. в г Минске главами государств Содружества Соглашение «О сотрудничестве государств-участников Содружества Независимых государств в борьбе с преступлениями в сфере компьютерной информации» [56], где определены такие понятия, как «преступление в сфере

компьютерной информации», «компьютерная информация», «вредоносная программа» и «неправомерный доступ».

Согласно данному Соглашению, в целях обеспечения эффективного предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации, стороны договорились принимать необходимые организационные и правовые меры для выполнения положений данного Соглашения, а также стремиться к гармонизации национального законодательства в области борьбы с правонарушениями в сфере компьютерной информации [17, с 114].

В рамках Протокола о сотрудничестве в области борьбы с преступлениями в сфере компьютерной информации с участием спецслужб государств - участников СНГ в Республике Казахстан имеется определенный практический опыт. В структуре КНБ создано подразделение по борьбе с компьютерными правонарушениями, задачами которого являются выявление, предупреждение и пресечение правонарушений, направленных на информационные ресурсы государственных органов.

Одним из приоритетных вопросов в данной области является развитие сотрудничества с европейскими и западными странами. Так, в настоящее время заинтересованными госорганами республики рассматривается вопрос о присоединении Казахстана к Конвенции о преступности в сфере компьютерной информации, принятой Советом Европы в 2001 году, что позволит расширить географию борьбы с компьютерными преступлениями, а также перенимать опыт зарубежных правоохранительных органов в данной сфере.

Ни для кого не секрет, что злоумышленник, совершив ту или иную компьютерную атаку, старается замести следы своих соединений и изменить журналы регистрации провайдера.

Практика показывает, что количество возбужденных уголовных дел по киберпреступлениям не так велико, ввиду сложности обнаружения злоумышленников и сбора доказательственной базы. Однако, компьютерных правонарушений гораздо больше, нежели статей, предусматривающих

уголовную ответственность за киберпреступления. Возможно, более детального исследования требуют правонарушения, совершенные посредством сети Интернет, в итоге которого будут сформированы нормы для уголовного и уголовно-процессуального законодательства, которые будут учитывать специфику совершения киберпреступлений.

Таким образом, научно-технический прогресс привел к возникновению ранее не известных видов правонарушений в сфере компьютерной информации и трансформации традиционных преступлений на основе использования возможностей компьютерной техники.

Опасность, которую представляет компьютерная преступность, воспринята мировым сообществом как реально существующая угроза общественной безопасности, о чем свидетельствует наличие соответствующих правовых норм в национальных законодательствах и масштабность проводимых исследований.

Поскольку компьютерные правонарушения могут нанести вред жизненно важным объектам и не имеют территориальных ограничений, возникла необходимость выработки системы международных, законодательных мер противодействия данным видам криминальных посягательств, которая на протяжении ряда лет реализуется международными организациями разного уровня, включая ООН.

Совершенно очевидно, что казахстанскому законодателю следует учесть опыт зарубежных государств и оценить пригодность вышеупомянутых правовых инструментов для защиты компьютерной информации. Разработка национального уголовного законодательства в рамках противодействия компьютерным правонарушениям должна проводится с учетом позитивного нормотворческого опыта высокоразвитых государств, международных норм-рекомендаций и быть неразрывно связанной с развитием норм таких отраслей права, как конституционного, гражданского, административного (особенно, института интеллектуальной собственности, института права на доступ к информации и защиты частной тайны).

## 2 Общая характеристика уголовных правонарушений в сфере информатизации и связи

### 2.1 Понятие и виды уголовных правонарушений в сфере информатизации и связи

В настоящее время существуют два основных течения научной мысли в определении понятия «компьютерного правонарушения». Одна часть исследователей относит к компьютерным правонарушениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным правонарушением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства [57, с. 118]. Надо сказать, что законодательство многих стран, в том числе и в Республике Казахстан, стало развиваться именно по этому пути.

Термин «компьютерные правонарушения» можно рассматривать в трех аспектах:

1) правонарушения, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых. Данные правонарушения не направлены на совершение противоправных операций с информацией, содержащейся в компьютерах и базах данных, и должны квалифицироваться по статьям гл. 6 УК РК - как уголовные правонарушения против собственности;

2) правонарушения, направленные на получение несанкционированного доступа к компьютерной информации, создание компьютерных «вирусов» - вредоносных программ и заражение ими других компьютеров. Ответственность за такие правонарушения предусмотрена ст. ст. 205, 210 УК РК;

3) правонарушения, в которых компьютеры и другие средства компьютерной техники используются злоумышленниками как средство совершения корыстного правонарушения и умысел направлен на завладение

чужим имуществом путем внесения изменений в программы и базы данных различных организаций.

Под компьютерным правонарушением следует понимать предусмотренные уголовным законом общественно опасные деяния, в которых компьютерная информация является либо средством, либо объектом посягательства.

Можно выделить следующие характерные особенности этого социального явления:

- неоднородность объекта посягательства;

- выступление электронной информации, как в качестве объекта, так и в качестве средства правонарушения;

- многообразие предметов и средств криминального посягательства;

- выступление компьютера либо в качестве предмета, либо в качестве средства совершения правонарушения.

На основе этих особенностей можно сделать вывод, что компьютерное правонарушение – это предусмотренное уголовным законом общественно опасное деяние, совершенное с использованием средств компьютерной техники.

В определении понятия «компьютерное правонарушение» выделяются следующие основные подходы:

1) К компьютерным правонарушениям относятся такие общественно опасные деяния, в которых компьютер является как объектом, так и орудием посягательства.

2) К компьютерным правонарушениям относятся общественно опасные деяния в сфере автоматизированной обработки информации.

3) Отрицание существования самостоятельных компьютерных правонарушений. Компьютер рассматривается как инструмент совершения известных уголовному закону криминальных посягательств.

Основное разграничение между предметом, орудием и средством совершения правонарушения должно проводиться по характеру использования

материальных предметов в процессе посягательства. Если компьютерная информация на электронном носителе подвергается «атаке» в криминальных целях, речь идет о предмете правонарушения. Если с помощью одной компьютерной информации происходит посягательство на другую компьютерную информация, то компьютер по праву можно считать орудием или средством совершения правонарушения [58, с. 394].

Схожесть понятий «орудие» и «средство» совершения правонарушения заключается в том, что как орудие, так и средство правонарушения применяются для реализации криминальной цели и воздействуют на предмет правонарушения. В связи с этим, сторонники третьей точки зрения считают, что использование компьютера в качестве инструмента совершения общественно опасного посягательства является квалифицированным признаком состава и охватывается понятием «применение технических средств».

Таким образом, «компьютерное правонарушение» можно признать либо как самостоятельную уголовно-правовую категорию, либо как «компьютерный аспект» совершения традиционных правонарушений.

Законодатель уголовным проступком признается совершенное виновно деяние (действие либо бездействие), не представляющее большой общественной опасности, причинившее незначительный вред либо создавшее угрозу причинения вреда личности, организации, обществу или государству, за совершение которого предусмотрено наказание в виде штрафа, исправительных работ, привлечения к общественным работам, ареста.

С этой позиции компьютерные правонарушения обладают всеми вышеперечисленными признаками:

1) Так как уголовный закон Республики Казахстан обозначил что уголовным проступком признается деяние, не представляющее большой общественной опасности чем преступление многие ученые ставят под сомнение наличие в целом такого признака как "общественная опасность". Тем не менее на наш взгляд, существует общественная опасность компьютерных правонарушений. Ущерб, наносимый компьютерными правонарушениями,

значительно превышает ущерб традиционно совершаемых хищений. Повсеместное внедрение производственную и обыденную жизнь компьютеров, компьютеризированных расчетов и банковских операций, применений компьютерных технологий в документоведении, расширение диапазона возможностей выхода в иные, в том числе и зарубежные информационные сети - все это делает компьютерные правонарушения общественно опасными. Причем наносимый ущерб может иметь как материальный, так и нематериальный характер, затрагивая интересы как личности, общества, так и государства в целом.

2) Вина в теории уголовного права определяется как психическое отношение виновного лица к совершенному им общественно опасному деянию и наступившим в результате общественно опасным последствиям, выраженное в форме умысла (ст. 20 УК РК) или неосторожности (ст. 21 УК РК). В случаях, когда в результате совершения умышленного правонарушения были причинены тяжкие последствия, которые по закону влекут боле строгое наказание и которые не охватывались умыслом лиц; возможны ситуации уголовной ответственность за совершение правонарушения с двумя формами вины (ст. 22 УК РК).

Применительно к компьютерным правонарушениям существует несколько точек зрения в отношении формы вины. По мнению таких авторов как Т.Б. Сеитов, Б.Х. Толеубекова, Т.М. Лопатина данные правонарушения могут совершаться как умышленно, так и неосторожно. Особенность компьютерных правонарушений обуславливается тем, что одни и те же действия с одним тем же умыслом могут приводить при различных состояниях компьютерной техники к не прогнозированным виновным последствиям. И, следовательно, неосторожная форма вины возможна. Вместе с тем, такой подход противоречит законодательному установлению, что деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК РК. Есть авторы, которые занимают иную позицию и

считают, что субъективная сторона характеризуется только прямым умыслом [59, с. 585].

Разделяя последнюю точку зрения, необходимо внести некоторые уточнения. Совершая уголовно-наказуемое компьютерное правонарушение, виновное лицо действует умышленно, но мотивы и цели при этом могут быть различными. Одни занимаются компьютерными взломами с целью получения доступа к нематериальным эквивалентам материальных ценностей и их последующего присвоения, другие - действуют из «спортивных» целей. В результате, сознавая незаконность своих действий и предвидя возможность или неизбежность наступления общественно опасных последствий, виновное лицо действует с прямым или косвенным умыслом. Если же наступившие последствия не охватывались умыслом виновного, и влекут по закону более тяжкое наказание, то речь идет о двойной форме вины.

3) Факт существования компьютерных правонарушений признак уголовным законодательством не всех стран. Вместе с тем, признание их противоправности вытекает из высокой степени общественной опасности компьютерных правонарушений. Ни одна из отраслей права не обладает таким арсеналом санкций, как уголовное право, которые были бы адекватны ущербу, причиняемому компьютерными правонарушениями и реализовывали бы цели общей и частной превенции. Богатый нормотворческий опыт ведущих индустриально развитых государств свидетельствует о том, что в таких странах как США, Япония, Великобритания, Германия проводится политика уголовно-правового преследования за компьютерные правонарушения. Существование последних этих странах расценивается как объективная реальность.

Таким образом, под компьютерным правонарушением следует понимать предусмотренное уголовным законом общественно опасное деяние, посягающее на охраняемую законом компьютерную информацию, которое причиняет или создает угрозу причинения вреда правам и свободам человека, безопасности физических и юридических лиц, независимо от формы собственности, общества и государства.

Многосторонность научных положений рассматриваемой проблемы свидетельствует о наличии иной позиции, согласно которой компьютерные правонарушения являются частью информационных правонарушений, посягающих на информационные отношений. В свою очередь, информационные отношения являются разновидностью общественных отношений, возникающих при формировании информационных ресурсов, функционировании информационных процессов, использовании информационный технологий, средств их обеспечения и защиты.

По мере развития научно-технического прогресса, совершенствования компьютерной техники непрерывно возрастает число криминальных ухищрений, растет количество видов компьютерных правонарушений. В самом общем виде классификация компьютерных преступлений разработана группой экспертов Организации экономического развития ООН: экономические компьютерные преступления; компьютерные преступления, связанные с нарушением личных прав, особенно прав на личную жизнь; компьютерные преступления против частных интересов.

Наиболее распространенными правонарушениями с использованием компьютерной техники являются: компьютерное пиратство, компьютерное мошенничество, распространение вредоносных (вирусных) программ и компьютерный саботаж. К компьютерному пиратству относят, прежде всего, деятельность «хакеров» - неправомерный доступ к компьютерной информации с помощью подбора паролей, кодов, шифров, взломов электронных замков и т.п. Когда результатом подобной деятельности являются модификация информации и утечка денежных средств - она превращается в компьютерное мошенничество. Второй вид компьютерного пиратства - незаконное копирование, тиражирование и сбыт компьютерных программ. Подобная деятельность нарушает авторские права создателей и разработчиков программ, причиняет материальный ущерб им и законным владельцам компьютерных программ. К тому же страдают пользователи программного продукта, так как качество копий уступает качеству оригинала.

В настоящее время в научной литературе имеется обширный классификационный разброс:

1. В.Д. Курушин и А.В. Шопин классифицируют «компьютерные правонарушения» следующим образом:

- незаконное использование компьютера в целях моделирования или анализа преступных действий для осуществления в компьютерных системах;

- незаконное проникновение в информационно-вычислительные сети или массивы информации;

- хищение прикладного и системного программного обеспечения;

несанкционированное копирование, изменение или уничтожение информации;

- шантаж, информационная блокада или другие виды компьютерного давления на соперника;

- передача компьютерной информации лицам, не имеющим к ней доступа;

- подделка, мистификация или фальсификация компьютерной информации;

- разработка и распространение компьютерных вирусов;

- несанкционированный просмотр или хищение информационной базы;

- небрежность при разработке, изготовлении и эксплуатации информационно-вычислительных сетей и программного обеспечения, приводящая к тяжким последствиям;

- механические, электрические, электромагнитные и другие виды воздействия на информационно-вычислительные сети, заведомо вызывающие их повреждение [60, с. 9].

2. Ю.М. Батурин, А.М. Жодзишский предлагают иную классификацию:

- нарушение правил обработки информации персонального характера;

- несанкционированный доступ в компьютерную систему;

- угроза возникновения конфликта;

- заражение компьютерным вирусом;

- уничтожение элементов компьютерной техники;

- изменение объектов компьютерной техники;

- изъятие объектов компьютерной техники;

- хищения [52, с. 29].

3. Б.Х. Толеубекова применительно к современным условиям Казахстана формулирует следующую классификацию:

- компьютерное мошенничество;

- информационное пиратство;

- незаконное копирование информации;

- кража компьютеров и их компонентов;

- кража из кассовых аппаратов [21, с. 39].

4. В руководстве ООН по «Профилактике и пресечению компьютерной преступности» предложена такая классификация:

- компьютерное мошенничество;

- компьютерный подлог;

- повреждение или модификация данных компьютера или программ;

- незаконный доступ в компьютерную систему;

- незаконное производство компьютерных программ [42].

Приведенные примеры классификации «компьютерных правонарушений» не являются исчерпывающими, существуют и иные. Их многочисленность объясняется: а) состоянием правовой урегулированности отношений в сфере компьютерной информации; б) их теоретической разработанностью, в) глубиной криминальной пораженности информационного пространства, г) уровнем использования международного законодательного опыта в практике национального правоприменения.

В нашем новом уголовном законе Казахстана "компьютерные преступления" теперь называются "уголовные правонарушения", которые делятся на уголовные проступки и преступления. В том случае, если деяние влечет наказание в виде лишения свободы, это является преступлением.

В рамках последней определенный научный и познавательный интерес представляет кодификатор рабочей группы Интерпола, которым пользуется в

настоящее время Национальное центральное бюро Интерпола более 10 стран. Данная классификация предусматривает как возможность появления новых видов «компьютерных преступлений», так возможность тесного международного сотрудничества.

Большинство компьютерных преступлений - это проявления профессиональной и организованной преступности, нередко носящей групповой транснациональный характер. Причем часто в состав группы входит непосредственный работник кредитной организации или иной компании, которая впоследствии оказывается пострадавшей (по некоторым оценкам, при хищениях с использованием компьютерных средств до 80% таких деяний совершались «изнутри»).

Транснациональный характер компьютерной преступности, быстрые темпы ее распространения обусловливают неизбежность объединения сил и средств многих государств по противостоянию этому явлению. В настоящее время создается острая необходимость разработки международно-правовой базы предотвращения инцидентов, связанных с обменом информацией, борьбы против «информационного терроризма», разработки комплекса мер международного характера, предотвращающих деструктивное использование средств воздействия на национальные и глобальные информационные ресурсы.

Можно сделать вывод, что понятие «компьютерного преступления» является одним из центральных в сегменте преступлений в сфере компьютерной информации, но до сих пор остается более чем не определенным. В мировой практике «… признано, что дать определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления» [61, с. 9]. Сложность в формулировке этого понятия существует, как по причине невозможности выделения единого объекта криминального посягательства, так и множественности предметов посягательств с точки зрения их уголовно-правовой охраны. В поисках истинного юридического значения выражения «компьютерное преступление» многие ученые и практики разошлись во

мнениях более чем на четыре стороны. Относительно только объекта данного преступления в науке существует уже как минимум три мнения: сторонники первого считают, что объектом является сам компьютер, второго - компьютерная информация, записанная на электронных носителях компьютера, а третьего, что общественные отношения по безопасному (законному) использованию информации являются объектом данного преступления.

Компьютерное правонарушение по своей сути очень специфично и своими корнями уходит вглубь профессиональной среды специалистов в области информационных технологий. Это особый мир или отдельная страна со своими законами, понятиями, лидерами, целями и даже наказаниями. Здесь нельзя навести свой порядок, установить свой «устав». Единственный путь для уголовно-правовой науки видится в том, чтобы на основе глубокого анализа пытаться смоделировать юридические понятия и в дальнейшем грамотно регулировать отношения в данной области.

## 2.2 Юридическое понятие объекта и предмета уголовных правонарушений в сфере информатизации и связи

Так как для оценки характера и степени общественной опасности деяния и его правильной квалификации важно установить конкретное охраняемое уголовным законом социальное благо, на которое происходит посягательство, необходимо уяснить особенности непосредственного объекта уголовных правонарушений в сфере информатизации и связи.

Как следует из теории уголовного права, непосредственным объектом является какое-либо отдельно взятое общественное отношение, сущность которого состоит в охране уголовно-правовой нормой возможности действовать определенным образом или пребывать в известном состоянии.

Одни ученые считают, что непосредственным объектом компьютерных правонарушений являются общественные отношения, связанные с безопасностью информации [62, с. 25]. Другие полагают, что для каждого

состава правонарушения существует свой непосредственный объект [63, с. 14]. Наиболее последовательной, как нам представляется, является последняя позиция.

Исходя из данной посылки, непосредственным объектом правонарушений в сфере информатизации и связи выступают охраняемые уголовным законом общественные отношения, обеспечивающие; а) конфиденциальность охраняемой законом компьютерной информации; б) безопасность компьютерной информации и компьютеров; в) безопасность эксплуатации компьютера, информационной системы или информационно-коммуникационной сети.

Определяя понятие объекта правонарушений, необходимо остановиться на соотношении объекта и предмета криминального посягательства. «Уголовно-правовое значение предмета правонарушения определяется не его физическими свойствами, а характером и содержанием выражающихся в нем общественных отношений. В уголовно-правовом смысле предмет всегда выступает в связи с конкретными общественными отношениями» [64, с. 89]. Уголовный закон охраняет не вещи и предметы сами по себе, а те общественные отношения, на которые направлено посягательство. Иными словами, воздействуя на предмет криминального посягательства, правонарушитель нарушает (или предпринимает попытку нарушить) само общественное отношение, находящееся под охраной уголовного закона.

Соотношение объекта и предмета криминального посягательства в сфере компьютерной информации имеет важное значение для уголовно-правовой характеристики правонарушения, ввиду того, что компьютер и компьютерная информация (в таких формах, как цифровая, сжатая, зашифрованная) представляют собой особую материю.

В определении понятия предмета уголовного правонарушения в сфере информатизации и связи мнения ученых разделились. Одни считают, что предметом является компьютерная информация [65, с. 9], другие относят к предмету, компьютер, компьютерную систему или компьютерную сеть [67, с.

23]. Нарушение нормального осуществления информационных отношений происходит посредством посягательства на информацию, которая выступает предметом рассматриваемых правонарушений, является общепризнанным фактом [66, с. 496].

Информация - это не просто совокупность знаний о фактических данных, это благо, которое имеет определенную ценность. С введением нового Гражданского кодекса Республики Казахстан (далее – ГК РК) информация стала самостоятельным объектом гражданских прав, наряду с деньгами, ценными бумагами, результатами интеллектуальной деятельности (ст. 115 ГК РК), т.е. товаром со всеми вытекающими из этой правовой дефиниции последствиями [68]. Отсюда любое «завладение» и «пользование» документированной информацией без согласия ее собственника или законного владельца (за исключением случаев, прямо указанных в законе) является неправомерным, поскольку нарушает права последнего.

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина [69] , принятая Генеральной Ассамблеей ООН 10 декабря 1948 г., в ст. 19 закрепила право каждого человека на свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Следуя приоритету норм международного права, Конституция Республики Казахстан, в ч. 4 ст. 29 подтвердила и гарантировала это право граждан, ограничив его сведениями, составляющими государственную тайну. Вместе с тем Конституция РК содержит ряд иных ограничений, связанных с распространением информации. В частности, ст. 23 закрепляет право граждан не неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

В соответствии со ст. 2 Закона РК «Об информатизации» информация определяется как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления» [14].

В информационном обществе информация становится стратегическим ресурсом. В обозримом будущем мировое сообщество может быть поделено на два «противостоящих» лагеря. Мощные индустриальные державы за счет высокого научно-технического и экономического потенциала страны, высокого информационно-образовательного уровня населения могут занять доминирующее положение и осуществить глобальный информационный контроль над мировым сообществом.

Понятие «информация» может быть рассмотрено в различных аспектах:

Информация в философском понимании представляет собой совокупность сведений о природе и обществе, процессах, протекающих в них и отражающихся в сознании людей.

Социальная информация включает все виды информации, проходящей через сознание людей: математическую, экономическую, правовую, статистическую т.д.

Информация с позиций кибернетики рассматривается как циркулирующая по электронным каналам связи.

Информация в техническом аспекте определяется как содержание данных, которое видят в них люди.

Информация в уголовно-правовом смысле представляет собой сведения о лицах, явлениях и процессах, содержащихся в информационных системах (банках данных).

Как научная категория информация представляет собой многоаспектное явление, которое имеет количественную и качественную стороны [70, с. 74]. Количественная сторона информации фиксируется при помощи математических, статистических методов измерения, которые нашли свое применение как в науках о неживой природе (физике, химии, геологии), так и в науках об обществе (психологии, социологии, экономике). Качественная сторона информации характеризует ее содержание, смысл, социальную значимость и общественную (частную) ценность. Именно качественная характеристика социальной информации определяет необходимость в ее уголовно-правовой защите.

Социальную информацию можно классифицировать по разным основаниям:

- по сфере применения: массовая; персональная.

- по категориям: политическая; экономическая; правовая; военная; статистическая и т.д.

- по источникам: официальная; неофициальная.

- по объему: общая; отраслевая.

- по содержанию: документальная; иная.

- по режимам доступа: общедоступная; конфиденциальная (государственная, коммерческая, служебная тайна).

- по соотношению со временем: о прошлом; о настоящем; о будущем.

- по проблематике сведений: об экологии; о безопасности; о внешнеполитической обстановке и т.д.

- по мотивации: позитивная; нейтральная; негативная.

- по формам собственности: государственная; негосударственная (принадлежащая физическим и юридическим лицам).

- по форме выражения: устная; на бумаге; компьютерная: на электронных носителях, в компьютере, информационных системах или информационно-коммуникационных системах.

В соответствии с формой представления социальная информация может выражаться на электронных носителях, сохраняться в компьютерах, компьютерных системах и сетях. В таком качестве она определяется как компьютерная. В данном случае речь едет не просто об информации, а об информации, которая неотделима от компьютера, о компьютерной информации.

Компьютерная информация - это информация, зафиксированная на электронном носителе и передаваемая по телекоммуникационным каналам в форме, доступной восприятию компьютера [71, с. 32].

Само понятие «компьютерная информация» как предмет криминального посягательства трактуется по-разному:

- как неотъемлемая инструментальная часть компьютера;

- как определенная совокупность данных, представляющая ценность для отдельного человека, организации, предприятия, учреждении, фирмы, общества, государства.

В первом случае «компьютерная информация» выступает как форма и является объектом гражданско-правовой охраны, объектом интеллектуальной собственности, авторского, патентного и изобретательского права. Во втором случае «компьютерная информация» выступает как содержание и в зависимости от категории доступа может являться объектом уголовно-правовой охраны.

На компьютерную информацию ограниченного доступа в процессе криминального посягательства осуществляется неправомерное воздействие, за которое предусматривается ответственность в ст. ст. 205, 206, 208, 211, ч.1 ст. 213 УК РК. В качестве предмета уголовного правонарушения в сфере информатизации и связи («пассивная информация») могут выступать банки данных, различные компьютерные программы, компьютеризованные объекты авторского права и т.д.

В случаях, когда использование компьютерной информации носит активный характер, информация выступает в качестве орудия совершения правонарушения («активная информация»). С ее помощью осуществляется воздействие на «пассивную информацию». Если взять любое компьютерное правонарушения, то воздействовать на предмет такого правонарушения можно посредством компьютерной информацией, которая в этом случае будет вы ступать в качестве орудия правонарушения. В качестве «активной информации» могут выступать компьютерные команды, «вирусные» программы.

Ст. 210, ч. 2 ст. 213 УК РК предусматривает ответственность за создание, использование или распространение вредоносных компьютерных программ и программных продуктов, а также за создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.

Предметом криминального посягательства в этих случаях следует считать вредоносную программу или вредоносный программный продукт и программу для изменения идентификационного кода абонентского устройства.

Законодатель под вредоносной программой понимает программу, которая может привести к уничтожению, блокировании модификации либо копированию информации, нарушению работы компьютера, информационной системы или информационно-коммуникационной сети; выполняющую эти функции без санкционирования собственником или законным владельцем информации.

К таким программам относятся «компьютерные вирусы», «черви», «троянцы», «программы-бомбы». Примером «программ-троянцев» являются программы-антивирусы, фото и видео галереи с «exe». «bat», «com» файлами и т.д.

Наиболее известным случаем использования «логической бомбы» является инцидент, произошедший в начале 80-х годов на Волжском автомобильном заводе. Занимаясь программированием автоматизированной системы подачи механических узлов на главный конвейер, программист умышленно внес в программу команду, приведшую к остановке системы после прохождения заданного числа деталей. В результате с конвейера в срок не сошло 200 автомашин. Заводу был причинен значительный материальный ущерб.

Вредоносные программы могут сочетаться. Широко известная пользователям компьютеров вредоносная программа «Чернобыль» сочетает в себе особенности «вируса» и особенности «временной бомбы».

Как следует из приведенных примеров, подобные вредоносные программы могут быть в равной степени опасны как для отдельных пользователей компьютера, так и для безопасности государства в целом. Вероятность опасности глобального масштаба существует в связи с распространенностью компьютерной сети Интернет, число клиентов которой ежегодно прогрессирует.

Новое казахстанское уголовное законодательство включает в себя ряд неизвестных ранее составов правонарушений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации вызвана возрастающим значением и широким применением этой информации во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе.

## 2.3 Основные способы совершения уголовных правонарушений в сфере информатизации и связи

Важным элементом уголовно-правовой характеристики правонарушения является способ его совершения, то есть совокупность определенных приемов, используемых преступником при реализации своих намерений. Правонарушения совершаются различными способами. Иногда достижение криминальных целей становится возможным на основе применения комбинаций способов. Не являются исключением и компьютерные правонарушения. Техническая и правовая практика свидетельствует об огромной изобретательности компьютерных правонарушителей. Рассмотрим наиболее распространённые способы совершения компьютерных правонарушений в Республике Казахстан.

По законодательству РК предусмотрены следующие способы совершения уголовно-наказуемых посягательств в сфере компьютерной информации:

1. Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть.

Несанкционированный доступ к информации может осуществляться в широком диапазоне целей от удовлетворения бытового любопытства до компьютерного шпионажа, осуществляемого в криминальных целях.

Наступление уголовно-правовой ответственности связывается с общественно опасными последствиями, являющимися следствием несанкционированного (неправомерного) доступа к информации, охраняемой законом.

Способы достижения неправомерного доступа к охраняемой законом компьютерной информации могут быть следующими: использование чужого имени либо условного пароля, изменение физических адресов технических устройств, модификация программного носителя информации, нахождение слабых мест и «взлома» защиты системы, угадывание кода, соединение с тем или иным компьютером, подключенным к телефонной сети и т.д. Неправомерным доступом к компьютерной информации является доступ к сети Интернет ограниченного пользования, приведший к уничтожению, блокированию, модификации, копированию информации, в случае, если лицо не имело право доступа к ней.

Так, с помощью методов «брешь», «люк», «неспешный выбор» находится ошибка в программе или слабое место в системе защиты и осуществляется несанкционированный доступ к информации. Преступник, используя метод «маскарад», выдает себя за законного пользователя и проникает в сеть. Несанкционированный доступ может осуществляться с использованием различных методов манипуляции. Преступник, используя «взламывающую программу», применяя метод «подмена кода», обходит систему защиты и проникает к информации. Зная пароль (код), преступник, применяя метод «троянский конь», внедряется в программное обеспечение компьютера.

Таким образом, используя известные способы совершения компьютерных правонарушений или их комбинацию, можно совершить несанкционированный доступ к охраняемой законом компьютерной информации. При наступлении последствий, указанных в ст. 205 УК РК, возникают основания применения уголовно-правовой ответственности. Специфика этих способов заключается в том, что они связаны с профессиональными знаниями жесткой логической структуры аппаратной и программной частей компьютера. Рядовой пользователь вряд ли способен их применить.

2. Нарушение работы информационной системы или информационно-коммуникационной сети выражается в снижении работоспособности отдельных звеньев компьютера, отключении элементов компьютерной сети.

Нарушение работы информационной системы или информационно-коммуникационной сети выражается в нештатной технической ситуации (сбой в работе компьютера, информационной системы или информационно-коммуникационной сети, «зависание» компьютера и т.п.), при которой нормальное функционирование компьютерной техники невозможно. Обязательным условием при этом является сохранение физической целостности компьютерной системы [65, с. 25]. В противном случае содеянное дополнительно квалифицируется по статьям о правонарушениях против собственности.

3. Создание компьютерной программы, программного продукта с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети.

Создание программы для компьютера - это написание ее алгоритма, то есть последовательности логических команд с дальнейшим» преобразованиями его в электронном языке компьютера [66, с. 543]. Чаще всего для этого используется язык программирования АССЕМБЛЕР, СИ, СИ++, ТУРБО-СИ, ТУРБО-АССЕМБЛЕР.

Способ совершения правонарушения подразумевает создание не просто программ для компьютера, а вредоносных программ, т.е. программ, которые содержат «вирусы», «сетевые вирусы», «логические бомбы» с целью уничтожения, блокирования, модификации, копирования программного продукта, нарушение работы компьютера, информационной системы или информационно-коммуникационной сети. «Вирусы» могут быть внедрены в

операционную систему, прикладную программу, в сетевой драйвер. Такие «вирусные программы» распространяются по коммуникационным сетям, проникают в компьютер и «заражают» его, присоединяясь к другим программам.

Наиболее сложной и опасной разновидностью компьютерный вирусов являются сетевые вирусы, иначе «компьютерные черви». Объектом нападения последних являются системы обработки данных, включающие в свой контур вычислительные комплексы, персональные компьютеры, соединенные в локальные, отраслевые, государственные или межгосударственные сети.

Общественная опасность создания «вирусных» программ состоит в том, что они могут в любой момент парализовать работу не только отдельного компьютера, но и целой компьютерной сети.

Первым создателем «вируса» считается студент Калифорнийского университета (США) Фрэд Коуэн, который проводил опыты с компьютерными программами, в последствии названные «компьютерными вирусами». С первой компьютерной «эпидемией» связывается имя Роберта Таппана Морриса, студента Корнельского университета (США), который заразил «вирусом» более 6 тысяч компьютеров и 70 компьютерных систем, причинив ущерб около 100 миллионов долларов [72, с. 293].

«Логическая бомба» и ее разновидность «временная бомба» встраиваются в программный продукт путем внесения набора определенных команд, которые задействуются при определенных условиях или в определенный момент времени и приводят к общественно опасным последствиям.

Высокая степень общественной опасности вредоносных программ обусловила позицию законодателя, который связывает уголовную ответственность не с фактом наступления общественно-опасных последствий, а с фактом создания программ, которые заведомо могут привести к наступлению последствий, перечисленных в диспозиции статьи. В силу высокой сложности структуры и принципа действия «вирусных» программ правильно квалифицировать действия преступника невозможно без специалиста в области компьютерной техники.

4. Внесение вредоносных изменений в существующую программу или программный продукт.

Внесение изменений в существующие программы (или в отдельно взятую программу) означает модификацию алгоритма компьютера: изменение алгоритма, исключение фрагментов алгоритма, замены их другими, дополнения новыми фрагментами и т. д. Суть таких изменений заключается в том, что программа становятся вредоносной и может привести к различным нежелательным последствиям, вплоть до уничтожения информации.

Способ внесения изменений в программу может быть различным: декомпилирование программы, использование специального программного продукта и т.д. Законодателя связывает уголовную ответственность с фактом внесения изменений в программу, которые заведомо могут привести к наступлению общественно опасных последствий.

4. Использование вредоносных программ для компьютера.

Термин «использовать» обозначает что-либо употребить для какого- либо дела [72, с. 672]. Под использованием как способом совершения правонарушения понимается выпуск в свет, введение вредоносной программы (или программ) в хозяйственный оборот (в числе в модифицированном виде) для применения по назначению или воспроизведения.

Использование вредоносной программы происходит вопреки воле собственника или владельца информации. Причем виновное лицо осознает, что программа вредоносна и ее использование может привести к общественно опасным последствиям, к таким как уничтожение, блокирование, модификация, копирование компьютерной информации, нарушение работы компьютера, информационной системы или информационно-коммуникационной сети. Такие программы, как правило, не входят в состав штатного программного обеспечения и являются не прошедшими антивирусный контроль. Факт использования «вирусной» программы как правило устанавливается с помощью информационно-технологической экспертизы.

5. Распространение вредоносных программ для компьютера.

Распространение вредоносной программы (программ) означает ее передачу одному (или нескольким) пользователям компьютера. Распространение может осуществляться разными способами:

а) по компьютерной сети (локальной, региональной, государственной, международной);

б) путем предоставления доступа другим пользователям к «вирусной» программе;

в) путем воспроизведения на чужом компьютере записи вредоносной программы с дискеты, копирования вредоносной программы с диска на диск, через модем, компьютерную сеть, электронную почту;

г) созданием условий для самораспространения программы [73, с. 93].

Распространение «вирусных» программ для компьютера возможно в активной форме (внедрение «вирусной» программы в компьютер, информационную систему или информационно-коммуникационную сеть любым способом, предоставляющим свободный доступ к ней) и в пассивной форме (не воспрепятствование самораспространению «вирусной» программы или распространению ее третьими лицами). Ответственность наступает как для разработчиков, так и для пользователей, сознательно распространяющих «вирусные» программы.

6. Использование или распространение вредоносных компьютерных программ и программных продуктов. Под использованием вредоносных компьютерных программ и программных продуктов понимается его эксплуатация (или иное всякое потребление) с целью применения записанной на нем «вирусной» программы.

Под распространением вредоносных компьютерных программ для компьютера понимается его передача третьим лицам (путем продажи, проката, дарения, сдачи внаем, обмена, предоставления взаймы, копирования). Ответственность наступает для пользователей, сознательно распространяющих электронные носители с «вирусными» программами, независимо от наступления общественно опасных последствий, поскольку они создают

реальную опасность уничтожения, блокирования, модификации, копирования информации или нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети

## 2.4 Характеристика субъективных признаков уголовных правонарушений в сфере информатизации и связи

Выяснение и изучение мотивации криминального поведения имеет важное уголовно-правовое значение. Мотивы совершения правонарушения, составляют волевое содержание лица, совершившего правонарушение, характеризуют личность правонарушителя, зачастую влияют на квалификацию деяния, способствуют вынесению судом справедливого наказания.

Мотив и цель в некоторых случаях являются необходимыми признаками субъективной стороны умышленных уголовных правонарушений (например, корыстный мотив при злоупотреблении должностным или служебным положением, цель похищения денежных средств при несанкционированном доступе к данным и т.д.) встречаются составы, в которых мотив и цель включены в качестве квалифицирующих признаков (например корыстные побуждения при неправомерном распространении электронных информационных ресурсов ограниченного доступа).

Некоторые мотивы указаны в уголовном законе в общей части в качестве отягчающих и смягчающих обстоятельств (совершение уголовного правонарушения вследствие стечения тяжелых личных или семейных или иных обстоятельств, под влиянием угрозы или принуждения, либо материальной, служебной или иной зависимости, совершение уголовного правонарушения по мотиву национальной, расовой и религиозной ненависти или вражды, из мести за правомерные действия других лиц, а также с целью скрыть другое уголовное правонарушение или облегчить его совершение и т.д.) во всех этих случаях элементам уголовно-правовой характеристики

преступлений относятся мотив и цель. Однако для большинства умышленных уголовных правонарушений мотив и цель не является необходимыми элементами субъективной стороны и следовательно, не входят в уголовно-правовую характеристику. Между тем во всех случаях при расследовании конкретного уголовного правонарушения мотив и цель должны быть выяснены. Это имеет важное значение не только для определения судом справедливого наказания за содеянное, но и дает важную информацию для предупреждения правонарушений в сфере информатизации и связи.

Исходя из результатов изучения зарубежных исследователей по этому вопросу, в настоящее время можно выделить, пять наиболее распространенных мотивов совершения компьютерных правонарушений, расположенных в рейтинговом порядке:

1. Корыстные соображения – 66% (совершаются в основном правонарушителями третьей группы, кракерами и ламмерами);

2. Политические цели – 17% (шпионаж, преступления направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений – совершаются хакерами по найму либо правонарушителями третьей группы);

3. Исследовательский интерес – 7% (студенты, молодые программисты-энтузиасты называемые хакерами);

4. Хулиганские побуждения и озорство – 5% (хакеры, кракеры, ламмеры);

5. Месть – 5% (хакеры, кракеры, ламмеры)

Диапазон мотивов совершения правонарушений в сфере информатизации и связи широк и не ограничивается перечисленным. В нем выделяются также месть за негативное отношение работодателя; нанесение ущерба авторским правам; уничтожение секретных материалов; интеллектуальный вызов, безответственность, компьютерный шпионаж, самоутверждение и др.

На основе криминального мотива формируется цель уголовного правонарушения, как своеобразная мысленная модель будущего результата, к

достижению которого стремится субъект - правонарушитель, совершая противоправное деяние.

На основании эмпирического анализа литературных источников по данной проблеме представляется возможным выделить следующие наиболее типичные криминальные цели, для достижения которых правонарушителями использовались средства компьютерной техники: фальсификация платежных документов; хищение безналичных денежных средств; перечисление денежных средств на фиктивные счета; отмывание денег; легализация преступных доходов (например, путем их дробления и перевода на заранее открытые законные счета с последующим их снятием и многократной конвертации); совершение покупок с фиктивной оплатой (например, с генерированной или взломанной кредитной карточкой); продажа конфиденциальной информации; похищение программного обеспечения и незаконное ее распространение и т.д. и т.п.

В нашем новом УК помимо обязательного признака субъективной стороны вины в некоторых составах уголовных правонарушений выделяются специальные цели совершения деяний. Так, в части 2 статьи 209 УК Республики Казахстан "Принуждение к передаче информации" содержится такая цель совершения уголовного правонарушения, как - получение информации из национальных электронных информационных ресурсов или национальной информационной системы. В статье 210 УК РК "Создание, использование или распространение вредоносных компьютерных программ и программных продуктов" указана такая цель, как "неправомерное уничтожение, блокирование, модификация, копирование, использование информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети".

Блокирование информации - это запрещение дальнейшего выполнения последовательности команд или выключение из работы какого-либо устройства, или выключение реакции какого-либо устройства компьютера [76, с. 23].

В юридической литературе термин «блокирование информации трактуется по-разному: как невозможность ее использования при сохранение такой информации, как закрытие информации, что делает се недоступной для использования правомочным пользователем, как создание условий (в том числе с помощью специальных программ), искусственно затрудняющих доступ пользователей или полностью исключающих пользование компьютерной информацией.

Из приведенных определений следует, что блокирована осуществляется путем воздействия на компьютерную информацию (при условии ее сохранения), в результате которого выполнение информацией своих функций не возможно. Блокирование связано с таким техническим воздействием на компьютер, которое делает информацию недоступной собственнику или законному владельцу никакими существующими техническими средствами. Вряд ли можно говорить о блокировании информации в уголовно-правовом смысле в случаях, когда доступ к ней невозможен в силу профессиональной квалификации пользователя.

Таким образом, под блокированием информации следует понимать результат воздействия на компьютер, исключающий доступ к ней при сохранности охраняемой законом компьютерной информации.

Модификация информации - внесение любых изменений, за исключением необходимых для функционирования программы или базы данных, на конкретных технических средствах пользователя или под управлением его конкретных программ.

Модификация информации - наиболее сложный в правовом смысле вопрос. Модификация - это внесение изменений, не меняющих сущности объекта [77, с. 47]. Легальность внесенных изменений должна определяться с учетом норм авторского права.

В уголовно-правовом смысле под модификацией одни юристы понимают изменение первоначальной информации без согласия ее собственника или иного законного лица [66, с. 541]. Другие рассматривают модификацию информации как изменение логической и физической базы данных. Третьи полагают, что модификация заключается в несанкционированной переработке первоначальной информации (удаление и добавление записей, содержащихся в файлах, создание файлов, перевод программы компьютера или базы данных с одного языка на другой и т.п.).

Анализ мнений специалистов позволяет определить модификацию компьютерной информации как несанкционированная собственником или законным владельцем любая переработка первоначального состояния охраняемой законом информации которая трансформирует ее содержание.

Копирование информации - создание копий файлов и системных областей дисков.

От копирования компьютерной информации следует отличать тиражирование (размножение) информации, преследующее иные цели.

Понятие копирование в уголовно-правовом смысле у ученых вызывает некоторые разногласия. В одних случаях, копирование рассматривается как снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению [66, с. 542]. В других, как изготовление второго и последующих экземпляров базы данных, файлов, а также их запись в память компьютера. В третьих - как тиражирование информации при сохранении оригинала. При этом способ копирования не имеет определяющего значения. Копирование по смыслу закона выступает способом несанкционированного проникновения, которое является уголовно наказуемым деянием. Поэтому нельзя согласиться с мнением, что копирование компьютерной информации от руки, ее фотографирование с экрана дисплея, считывание информации путем перехвата излучений компьютера не образуют состава данного преступления.

Нам представляется наиболее точным определение понятия «копирование информации» как перенос информации с одного электронного носителя на другой, если это осуществляется помимо воли собственника или владельца информации [76, с. 74] при условии получения точного дубликата оригинала охраняемой законом компьютерной информации.

Личность человека, совершившего преступление, а теперь по нашему УК Республики Казахстан правонарушения, является объектом изучения наук криминалистического профиля, которые решают логически взаимосвязанные задачи: что такое личность преступника (правонарушителя); какие признаки составляют ее содержание; какова ее роль в совершении преступления (правонарушения); как воздействовать на нее, чтобы предотвратить совершение преступления (правонарушения).

Понятие «личность» характеризует социальное качество человека, которое не возникает с рождением, а формируется в процессе общественных отношений. Личность человека это система социально-психологических свойств и качеств, в которых отражены связи и взаимодействие человека с социальной средой посредством практической деятельности [78, с. 164].

Личность человека, выступая в единстве всех ее социальных, нравственных и психологических свойств и признаков, формируется в процессе его жизни и деятельности.

Формирование личности является сложным, противоречивым и в общем необратимым процессом, развивающимся «по спирали». Этот процесс начинается в подростковом возрасте. Любое преступление (правонарушение), в какой бы форме оно не совершалось, не случайно по отношению к личности, поскольку оно подготовлено развитием его социальных, нравственных, психологических свойств. В криминологическом изучении личности преступника (правонарушителя) выделяются два основных подхода.

Первый подход предусматривает изучение личности конкретного преступника (правонарушителя). В данном случае о личности преступника

(правонарушителя) можно говорить лишь применительно к субъекту преступления (правонарушения) в его уголовно-правовом представлении.

Второй подход дает представление об общих свойствах группы лиц, могущих совершить преступление (правонарушения). Применительно к компьютерным преступлениям (правонарушениям) диапазон таких лиц широк и включает в себя беспечных подростков, не достигших возраста уголовной ответственности и манипулирующих со своими компьютерами. Они сочетают в себе устойчивые элементы профессионализма в области информатики и программирования с элементами своеобразного фанатизма и изобретательности.

Говоря о характеристике личности преступника (правонарушителя), необходимо учитывать следующие составляющие:

- пол,
- возраст,
- уровень образования,
- социальный статус,
- семейное положение,
- социально-полезная деятельность,
- характеристика преступной деятельности,
- мотивация преступной деятельности,
- нравственно-психологические особенности личности,
- уровень правового сознания и др.

Вышеперечисленные признаки не являются исчерпывающими. Они формируют содержание научного понятия «личность преступника», теперь с новым уголовным законодательством Казахстана мы будем их называть ("личность правонарушителя"). В действительности эти признаки присущи конкретным правонарушителям в неодинаковой мере, их вариантность определяется личностными свойствами последних.

Применительно к уголовным правонарушениям в сфере информатизации и связи попытаемся рассмотреть основные характеристики личности правонарушителя по материалам отечественной и зарубежной литературы.

Начнём с того, что, как и у обывателей, так и у работников следственных органов давно сложился яркий стереотип компьютерного правонарушителя. Это юнец 15-ти – 20-ти лет, с тёмными, длинными, чуть косматыми волосами, в очках, молчаливый, замкнутый, рассеянный, с блуждающим взглядом, помешанный на компьютерах, напрочь игнорирующий события в окружающем мире. Нельзя сказать, что данный стереотип не имеет права на существование и ни в чём с оригиналом не схож. Как показывает статистика и независимые исследования, 20 из 100 «обитателей» криминального мира с «компьютерным уклоном» являют собой стопроцентно «чистых» стереотипных компьютерных правонарушителей. Остальные 80 в это стереотип не вписываются либо вообще, либо частично [52, с. 146].

В личностном плане субъекты уголовных правонарушений в сфере информатизации и связи характеризуются противоречиво. От молодого человека, работающего за дисплеем по 12 - 16 часов подряд, неряшливого вида, питающегося урывками и неприхотливо, не обращающего внимание на внешний мир, до высококвалифицированных, респектабельных специалистов, занимающих высокое социальное положение. Свыше 80 % правонарушителей в компьютерной сфере – мужчины [73, с. 112].

Обычно правонарушения в сфере компьютерной информации совершаются в одиночку, что характерно для мужчин. Женщины же, напротив, в большинстве входят в состав групп [83, с. 59].

По уровню специального образования диапазон весьма широк - от высококвалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя: 40% -лица, имеющие среднее специальное образование; 40% - высшее; 20% - среднее [73, с. 114].

По профессиональной подготовленности и социальному статусу выделяются следующие группы:

Первая группа характеризуется как самый низший уровень.

Сюда входят нарушители правил пользования компьютера, распространители вирусов и т.п.

Вторая группа представлена «хакерами» и «кракерами». «Хакеры» (hacker) – пользователи компьютеров, занимающиеся доскональным изучением и поиском слабых мест компьютерных сетей, операционных систем и систем информационной безопасности. Иногда в литературе и средствах массовой информации (далее - СМИ) таких лиц называют: «киберпанками».

К хакерам относятся увлеченные компьютерной техникой лица, преимущественно из числа молодежи – школьники и студенты, совершенствующиеся на взломах различных защитных систем. Хакеры объединены в региональные группы, издают свои СМИ (газеты, журналы, BBS (bulletin board system – электронные доски объявления), Web-странички), проводят электронные конференции, кодекс хакерской чести, имеют жаргонный словарь, который постоянно пополняется и распространяется, также имеются все необходимые сведения для повышения мастерства начинающего – методики проникновения в конкретные системы и взлома систем защиты [84, с. 12].

К хакерам следует относить лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. По мнению некоторых авторов, эти субъекты воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам. Именно это и является в социально-психологическом плане побуждающим фактором для совершения различных деяний, большинство из которых имеют криминальный характер.

Под воздействием указанного выше фактора лицами рассматриваемой группы изобретаются различные способы несанкционированного проникновения в компьютерные системы, нередко сопровождающиеся преодолением постоянно усложняющихся средств защиты данных. Следует подчеркнуть, что характерной особенностью правонарушителей этой группы

является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей. Ситуация здесь условно сравнима с той, которая возникает при различного рода играх, стимулирующих умственную активность игроков, например при игре в шахматы. Когда в роли одного игрока выступает гипотетический правонарушитель, а в роли его соперника – обобщенный образ компьютерной системы и интеллект разработчика средств защиты от несанкционированного доступа. Подробно данная ситуация исследуется в математической науке в теории игр – модели поведения двух противоборствующих сторон. При этом одной из сторон является человек, а другой – компьютер. Взаимодействие человека с компьютером осуществляется по определенному игровому алгоритму с целью обучения, тренировки, имитации обстановки и с развлекательными целями.

Обобщенные данные позволяют обозначить следующую социально-психологическую характеристику этого круга лиц. Представители данной специальности обычно весьма любознательны и обладают незаурядным интеллектом и умственными способностями. При этом не лишены некоторого своеобразного озорства и «спортивного» азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются в психологическом плане как своеобразный вызов личности, поэтому они стремятся, во что бы то ни стало найти эффективные способы доказательства своего превосходства.

Как правило, это и приводят их к совершению правонарушения. Постепенно некоторые субъекты рассматриваемой категории не только приобретают необходимый опыт, но и находят интерес в этом виде деятельности. В конечном итоге происходит переориентация их целеполагания, которое из состояния «бескорыстной игры», переходит в свое новое качество: увлечение заниматься подобной «игрой» лучше всего с получением некоторой материальной выгоды.

Обобщенный портрет «хакера» примерно выглядит так: мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере; в прошлом к уголовной ответственности не привлекался; является яркой мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник; по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках группы окружающих его людей: любит уединенную работу: приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы [73, с. 118].

В виртуальном мире, как и в реальном уже сложилась четкая классификация. Есть хакеры – программисты энтузиасты, а есть кракеры. Кракерами стали называть хакеров совершающих хищения. К ним также относятся и компьютерные хулиганы и вандалы, которые просто крушат сайты.

Кракеры, как и хакеры, занимаются поиском уязвимых мест в вычислительных системах и осуществлением атак на них.

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная задача хакера в том, чтобы, исследуя информационную систему, обнаружить слабые места (уязвимости) в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей. Другая задача хакера - проанализировав существующую безопасность информационной системы, сформулировать необходимые требования и условия повышения уровня ее защищенности.

Основная задача кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации – обычно для ее копирования, подмены или для объявления факта взлома. Итак, кардинальное различие между хакерами и кракерами в том, что первые - исследователи компьютерной безопасности, а вторые – непосредственно преступники.

Общими признаками для хакеров и кракеров являются: завышенная оценка своих профессиональных и, как следствие, интеллектуальных способностей; использование специфического жаргона не только в кругу специалистов, но и при повседневном общении; отсутствие интереса к проблемам повседневной жизни [85, с. 163]. Хакерство и кракерство – это образ жизни, который накладывает отпечаток на внешность, поведение, круг общения, личностные цели и социальные ориентиры. Правонарушения, как правило, совершаются открыто, могут использоваться оригинальные способы, собственные ноу-хау; методы взлома атакованного компьютера, информационной системы или информационно-коммуникационной сети могут тиражироваться среди «коллег».

Два наиболее опасных типа злонамеренных кракеров — это так называемые информационные маклеры и мета-хакеры. Информационные маклеры нанимают хакеров и оплачивают их услуги, чтобы получить интересующую информацию, а затем продают ее правительствам иностранных государств или деловым конкурентам.

Мета-хакеры — более изощренные хакеры, контролирующие других хакеров, причем делающие это порой незаметно для последних. Как правило, с корыстной целью используются уязвимые места, обнаруженные этими подконтрольными хакерами. Мета-хакер эффективно использует других хакеров фактически как интеллектуальные инструментальные средства.

Другой типичной разновидностью хакеров являются бригады, известные как «элита». Они формируют закрытые клубы, члены которых свысока смотрят на обычных хакеров, использующих традиционные инструментальные средства для взлома. Эта так называемая элита разрабатывает собственные инструментальные средства и всегда пользуется дружеской поддержкой и оценкой своего мастерства со стороны себе подобных.

Еще одной характерной разновидностью является группа, известная как «темные хакеры» («darksiders»). Они используют хакерство для финансовых махинаций или для создания злонамеренных разрушений. Они не согласны с

классической мотивацией для хакеров, которая заключается лишь в получении ощущения успеха и власти. Эти хакеры не считают электронное нарушение границ нечестным по своей сути. Однако важнейшей их особенностью является скорее то, что darksiders переступают невидимую границу, проведенную другими хакерами, и сами становятся вне законов этики хакерского мира. Не секрет, что этические нормы «хакерского большинства» осуждают хакерство для получения нечестных денег или причинения явного вреда.

К числу особенностей, указывающих на совершение уголовного правонарушения в сфере информатизации и связи лицами рассматриваемой категории, можно отнести следующие:

1. Отсутствие целеустремленной, продуманной подготовки к уголовному правонарушению;

2. Оригинальность способа совершения уголовного правонарушения;

3. Непринятие мер к сокрытию уголовного правонарушения;

4. Совершение озорных действий на месте происшествия.

Близко к рассматриваемой выше группе лиц способных совершить компьютерное правонарушение можно отнести, как мне представляется, еще одну, группу лиц отличающихся от хакеров и кракеров непрофессионализмом, дилетантством и наивностью.

Ламмеры – это лица, которые на волне всеобщего «Интернет психоза» пытающиеся быть хакерами. В последнее время участились случаи, когда компьютерными правонарушениями начинают заниматься «чайники» (неопытный пользователь ПК), считающие что компьютерные правонарушения остаются безнаказанными. Для совершения криминальных деяний ими используются готовые рецепты вроде программ генерации фальшивых номеров кредитных карточек и т.д. Компьютерные правонарушения с использованием генерированных номеров кредитных карточек приняли сегодня широко распространились по странам СНГ.

Попытки «выхватить» что-нибудь из сети предпринимают многие любители Интернета, причем большинство из них и не подозревает, что за

ними «могут прийти». Ламмеры по неопытности полагают, что за хищение виртуальных денег им ничего не будет. Вообще большинство людей, искренне считающих себя хакерами, таковыми не являются. Они используют заранее написанные «программы-ломалки» и очень слабо представляют себе, как работает сеть. К сожалению подобных правонарушителей-дилетантов, становится слишком много. Так что средний "правонарушитель" теперь обыкновенный «lamer», т.е. малоквалифицированный человек.

Третья группа характеризуется более высоким социальным положением и респектабельностью. В нее входят бухгалтера, управляющие финансами фирм, адвокаты и т.д. - воспитанники экономико - политической среды. Они вовремя осознали свои возможности в конкретный момент времени и в потенциале, определили «рыночную» цену своих знаний, сделали из увлечения карьеру. Их знания в большинстве случаев обширнее и систематизированнее, а следовательно и ценнее, чем у представителей второй группы. Они – настоящая сила как в бизнесе, так и в криминальном мире.

В связи с этим представляет интерес профиль типичного «беловоротничкового» компьютерного правонарушителя, составленный Консультативно - исследовательской фирмой Managment Safeguards INc. (США):

-приходит на работу очень рано, задерживается дольше других, иногда работает в выходные дни;

- хорошо знает, как работает система охранной сигнализации;

- имеет ключи от всех основных замков в служебные помещениях;

-делает все возможное, чтобы завоевать доверие руководства и работать самостоятельно без контроля;

-не поддерживает дружеских и деловых отношений с другими сотрудниками, предпочитая работать самостоятельно, потому что мало кому доверяет [86, с. 25].

Правонарушители третьей группы характеризуются организованностью совершения компьютерных правонарушений с обязательным использованием

действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми криминальными навыками.

Лиц данной группы можно охарактеризовать как высококвалифицированных специалистов, имеющих высшее техническое образование, возможно более одного высшего образования (техническое + экономическое и/или юридическое).

Знания в области компьютерных технологий практически исчерпывающие: люди этой группы владеют несколькими языками программирования всех уровней, в совершенстве знают особенности аппаратной части современных компьютерных систем (не только персональных, но и сетевых систем и специализированных информационных комплексов), имеют навыки профессиональной работы с несколькими компьютерными платформами (IBM PC, Apple Macintosh, SUN Microsystems), основными операционными системами (UNIX и клоны, LINUX в различных вариантах), MS DOS, Windows 3.X/NT/9X, OS/2, Novell NetWare/IntranetWare, SUN OS) и большинством пакетов прикладного программного обеспечения специализированного назначения (любое офисное, сетевое программное обеспечение, пакеты разработки приложений и др.), прекрасно информированы об основных системах электронных транзакций (сетевые протоколы, протоколы защищённой связи (биржевые, банковские и правительственные каналы), системах сотовой связи, системах и методах стойкой и супер-стойкой криптографии и успешно используют эти знания в «повседневной деятельности».

Имеют связи во многих властных структурах (причём многие «покровители» обязаны им за определённые услуги), которые используют при необходимости для проникновения на закрытые объекты и для получения кодов доступа в сильно защищённые от «взлома» системы.

Работают в основном «для прикрытия», обычно начальниками или замами начальников отделов информационных технологий в банках, в иностранных компаниях и государственных учреждениях, основная же

деятельность развёртывается в нелегальной и полулегальной сфере. Связь с «соратниками по ремеслу» поддерживают практически постоянную, но в основном на чрезвычайно конфиденциальном и индивидуальном уровне, крайне редко в прямом общении, в основном через сетевую связь, защищённую стойкой криптографией. Постоянно совершенствуют приёмы и инструменты «работы». Практически недосягаемы для органов правосудия. В общем, на лицо стопроцентные профессионалы своего дела.

Именно эта группа правонарушителей и представляет собой основную угрозу для общества. На долю именно этих правонарушителей приходится максимальное число совершенных особо опасных посягательств, например до 79% хищений денежных средств в крупных и особо крупных размерах и различного рода должностных преступлений, совершаемых с использованием средств компьютерной техники.

В этой группе выделяются «узкие профессионалы», технический уровень которых позволяет заниматься созданием вредоносных компьютерных программ или их модификацией. Создание такой программы представляет собой комплекс операций, состоящих из подготовки исходных данных, предназначенных для управления процессами уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети. Такую работу могут исполнить только высококвалифицированные специалисты: профессионально подготовленные компьютерщики; программисты; лица, могущие модифицировать программу с целью сделать ее вредоносной. К ним примыкают и лица, занимающиеся незаконным обращением вредоносных программ или электронных носителей с такими программами.

Четвертая группа представлена самой высокой ступенью. Сюда входят лица, занимающиеся компьютерным шпионажем. Представители этой группы хорошо подготовлены в техническом и организационном отношениях. Их

целью является получение стратегических важных данных о противнике в экономической, технической и других сферах.

На основании вышеизложенного, а также с учетом анализа специальной литературы, обобщенную характеристику личности «компьютерного» правонарушителя, данные которой в равной степени можно отнести к любой из рассмотренных групп, представляется возможным изложить следующим образом.

Возраст правонарушителей колеблется в широких границах (от 15 до 45 лет): на момент совершения правонарушения возраст 33% правонарушителей не превышал 20 лет, 13% - были старше 40 лет и 54%- имели возраст 20-40 лет. Большинство лиц данной категории составляют мужчины (80%), но доля женщин быстро увеличивается из-за профессиональной ориентации некоторых специальностей и профессий (секретарь, делопроизводитель, бухгалтер, кассир, и т.д.)

По уровню специального образования диапазон также весьма широк – от высоко квалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя. 52% правонарушителей имели специальную подготовку в области автоматизированной обработки информации, а 97% - являлись служащими государственных учреждений и организаций, использующих компьютерную технологию в своих производственных процессах, а 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

Большинство правонарушителей (77%) при совершении правонарушения имели средний уровень интеллектуального развития, 21% - выше среднего и только 2% - ниже среднего. При этом 40% правонарушителей имели средне специальное образование, 40%- высшее и 20%- среднее. С исследовательской точки зрения интересен тот факт, что из каждой тысячи компьютерных правонарушений только семь совершаются профессиональными программистами.

В последнее время, как свидетельствует статистика, резко увеличивается количество уголовных правонарушений, совершенных в составе организованных групп и сообществ за счет активного участия в них

правонарушителей третьей группы. Так, 39% правонарушителей действовали без соучастников, тогда как 62% - в составе преступных групп. В поведении правонарушителей рассматриваемой группы, как правило, не наблюдается отклонений от принятых общественных норм и правил. По своему общественному положению большинство из них являются служащими, нередко занимающими ответственные руководящие посты и соответственно обладающие доступом либо к средствам компьютерной техники, либо к учету и распределению материальных ценностей и благ, либо и то и другое вместе. В этом случае необходимо отметить высокий удельный вес руководящих работников всех рангов (более 25%), обусловленный тем, что управляющим обычно является специалист долее высокого класса, обладающий профессиональными знаниями, имеющий право отдавать распоряжения исполнителям и непосредственно не отвечающий за работу средств компьютерной техники.

Вместе с этим более высокий удельный вес руководящих работников среди совершивших хищения (23%) и более высокий процент правонарушений совершенных в составе организованной преступной группы (35%), характеризуют компьютерные хищения как организованные и групповые правонарушения. К косвенным признакам представителя рассматриваемого нами социального типа можно отнести внимательность, бдительность, осторожность, оригинальность (нестандартность) мышления и поведения, активную жизненную позицию.

В профессионально-классификационном плане круг «компьютерных» правонарушителей чрезвычайно широк. Обычно это разные категории специалистов и руководителей: бухгалтеры, программисты, системные администраторы, инженеры, финансисты, банковские служащие, адвокаты, начальники отделов и служб и т. д. Всех их можно разделить на две основные группы, исходя из классифицирующего признака категории доступа к средствам компьютерной техники:

1. Внутренние пользователи.

2. Внешние пользователи, где пользователь – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Пользователи бывают двух видов: зарегистрированные (санкционированные) и незарегистрированные (несанкционированные, незаконные).

По оценкам основная опасность в плане совершения компьютерного правонарушения исходит именно от внутренних пользователей: ими совершается 94% правонарушений, тогда как внешними пользователями – только 6%, при этом 70%- клиенты пользователи, 24 обслуживающий персонал.

Правонарушителями из числа внешних пользователей, как свидетельствует практика, обычно бывают лица, хорошо осведомленные о деятельности потерпевшей стороны. Их круг настолько широк, что уже не поддается какой-либо систематизации, и классификации им может быть любой даже случайный человек. Например, представитель организации, занимающейся сервисным обслуживанием, ремонтом, разработкой программных средств, хакеры, кракеры, ламмеры и т. д.

Рассмотрение характеристик личности компьютерного правонарушителя имеет важное значение в практической деятельности по предупреждению рассматриваемой категории правонарушений и учитываются при статистическом анализе уголовных правонарушений по лицам; при установление причин и условий, способствующих совершению компьютерных правонарушений; при профилактике соответствующих правонарушений.

## 3 Уголовно-правовой анализ состава уголовных правонарушений в сфере информатизации и связи

### 3.1 Характеристика объективных и субъективных признаков состава правонарушения "Неправомерного доступа к информации, в информационную систему или информационно-коммуникационную сеть"

Исходя из диспозиции ст. 205 УК РК, непосредственным объектом неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть выступают общественные отношения, обеспечивающие сохранность и конфиденциальность информации на электронном носителе.

Более подробно об объекте было изложено в предыдущей главе монографии.

Под собственником информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, имеющий право в полном объеме реализовывать полномочия владения, пользования и распоряжения указанными объектами [87, с. 10]. Под владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, имеющий право в полном объеме реализовывать полномочия владения, пользования и распоряжения в пределах, установленных законом. Под пользователем информации понимается субъект, обращающийся к информационной системе за получением необходимой информации с целью ее пользования.

Диспозиция анализируемого состава правонарушения определяет неправомерность доступа не ко всякой охраняемой законом компьютерной информации, а только к информации на электронном носителе, в информационную систему или информационно-коммуникационную сеть.

К электронным носителям относятся устройства, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью

средств вычислительной техники: магнитные диски, дискеты, магнитные ленты, оптические диски, стримеры и т.п. В компьютере информация может находиться в оперативном запоминающем устройстве (далее - ОЗУ), в котором при запуске компьютера определенное время может храниться, обрабатываться и передаваться охраняемая законом компьютерная информация. В информационной системе компьютера информация может находиться в ОЗУ периферийных устройств (к примеру, в лазерном принтере могут выстроиться «в очереди» на печать несколько документов, которые содержат охраняемую законом информацию). ОЗУ устройств связи, сетевые устройства и каналы связи относятся к информационно-коммуникационной сети компьютера, в которых также может находиться охраняемая законом информация (к примеру, модемы и факс-модемы имеют свои ОЗУ и «буферные» устройства, в которых некоторое время может находиться предназначенная для дальнейшей передачи информация).

Уголовно-правовой запрет на доступ к информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть распространяется только на охраняемую законом информацию. Применительно к уголовному законодательству Республики Казахстан охраняются следующие виды информации:

Сведения, отнесенные к государственной тайне (ст.ст. 175, 176, 185 УК РК);

Сведения, носящие конфиденциальный характер: персональные данные, сведения о частной жизни (ст.ст. 138, 147 УК РК);

Сведения, связанные с выполнением профессиональных функций; врачебная тайна, адвокатская тайна, тайна вклада, тайна переписки, телефонных, переговоров, почтовых отправлений и сообщений (ст. ст. 148, 321 УК РК);

Сведения, являющиеся служебной тайной, банковской тайной коммерческой тайной (ст. 223 УК РК);

Сведения, являющиеся объектом авторских и смежных прав (ст. 198 УК РК).

К обязательным признакам объективной стороны неправомерного доступа к информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть относятся:

- общественно опасное деяние в виде неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть;

- общественно опасные последствия в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства;

- причинная связь между совершенным общественно опасным деянием и наступившими общественно опасными последствиями.

Общественно опасное деяние в данном составе всегда проявляется в активной форме поведения виновного, то есть в действии. Неправомерный доступ к информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть в форме бездействия осуществить нельзя.

Под неправомерным доступом к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть следует понимать самовольное получение виновным лицом информации или распоряжение ею (уничтожение, блокирование, модификация, копирование) по своему усмотрению без разрешения ее собственника или законного владельца.

Чтобы вменить лицу проанализированные выше общественно опасные последствия и квалифицировать его действия по ст. 205 УК РК, необходимо установить наличие причинной связи между совершенным, деянием в виде неправомерного доступа к охраняемой законом компьютерной информации и наступившими последствиями, обозначенными в диспозиции статьи. Для этого требуется доказать тот факт, что деяния было необходимым и закономерным условием наступления вредных последствий и предшествовало этим последствиям по времени.

Помимо обязательных признаков объективной стороны состава теория уголовного права выделяет факультативные к которым относятся место, время, обстановка, орудия, средства и способ совершения преступления. Применительно к составу неправомерного доступа к охраняемой законом компьютерной информации, факультативные признаки объективной стороны на квалификацию содеянного не влияют, но могут учитываться при индивидуализации наказания.

Состав правонарушения, предусмотренного ст. 205 УК РК, является материальным, поэтому квалифицирующее уголовно-правовое значение отводится моменту окончания правонарушения. Одни авторы правонарушение связывают с моментом отсылки компьютеру последней команды вызова хранящейся информации [65, с. 11]. Другие, и их большинство, с моментом наступления хотя бы одного из последствий, перечисленных в законе [59, с. 498].

Таким образом, моментом окончания неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, информационную систему или информационно-коммуникационную сеть следует считать наступление общественно опасных последствий: существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Совершение деяний, не повлекших перечисленные выше последствия, состава данного правонарушения не образуют либо образуют стадию покушения на совершение неправомерного доступа к охраняемой законом информации, содержащиеся на электронном носителе, в информационную систему или информационно-коммуникационную сеть.

Таким образом, имеющаяся у законного владельца или пользователя возможность восстановить неправомерно уничтоженную информацию с помощью программных средств, получить ее от другого пользователя или использовать имеющуюся копию уничтоженной информации не освобождает виновного от уголовно-правовой ответственности.

В науке уголовного права субъективная сторона состава правонарушения рассматривается как «психическое отношение лица к совершенному им правонарушению которое характеризуется конкретной формой вины, мотивом и целью правонарушения» [74, с. 104].

Установление субъективной стороны состава неправомерного доступа к охраняемой законом компьютерной информации обусловлено определенной сложностью. Ведь безошибочных программ не бывает. Доказать умысел в действиях виновного лица нелегко: на его стороне презумпция невиновности. Сложность доказывания умысла затрудняется и сложностью доказывания совершенных им действий, ставших причиной наступления указанных в законе последствий. «Это затруднение связано с большой сложностью компьютерных систем и большим кругом лиц, имеющих прямое или косвенное отношение к последствиям преступления» (в нашем государстве - правонарушения) [43, с. 315].

В отношении субъективной стороны рассматриваемого состава наличествует несколько диаметрально противоположных точек зрения. По мнению одних ученых данное правонарушение может быть совершено как умышленно, так и по неосторожности. Другие предполагают наличие только прямого умысла. Последняя позиция разделяется большинством авторов Осуществляя неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть виновное лицо сознает общественно опасный характер своего действий, предвидит возможность или неизбежность наступления общественно - опасных последствий, указанных в диспозиции статьи Уголовного кодекса, желает их наступления (прямой умысел) или не желает, но сознательно допускает наступления этих последствий либо относится к ним безразлично (косвенный умысел).

Интеллектуальный элемент умысла при неправомерном доступе к охраняемой законом информации к информации, в информационную систему или информационно-коммуникационную сеть характеризуется: осознанием субъектом правонарушения совершаемого им деяния и предвидением

возможности (или вероятности) того, что охраняемая законом информация может повлечь существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Волевой элемент умысла определяется желанием (или сознательным допущением) либо безразличным отношением к наступлению указанных в статье общественно-опасных последствий.

Говоря об умысле, необходимо учитывать то обстоятельство, что неправомерный доступ к охраняемой законом информации, в информационную систему или информационно-коммуникационную сеть совершаются субъектами, которые обладают достаточной профессиональной эрудицией, чтобы отдавать отчет своим действиям и предвидеть вариантность будущих последствий. Совершение волевого осознанного действия виновным лицом, которое обладает личной технической осведомленностью, компьютерной грамотностью, предполагает видимость и наступивших последствий. Все это позволяет признать, что уголовно наказуемый неправомерный доступ к охраняемой законом информации, в информационную систему или информационно-коммуникационную сеть совершается с умышленной формой вины.

Субъекты компьютерных правонарушений являются технически образованными лицами, которые управляют компьютеризированными системами, эксплуатируют и обслуживают их. Поэтому совершение ими общественно опасных деяний с использованием компьютерных технологий происходит с осознанием возможности наступления последствий, представляющих опасность для компьютерных программ, для работы компьютера, информационной системы или информационно-коммуникационной сети.

Как было отмечено выше в науке уголовного права часто возникают вопросы: может ли быть уголовно наказуемо несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины?

Теория уголовного права по степени общественной опасности дифференцирует неосторожность на такие формы как самонадеянность и небрежность. Моделирование преступного умысла применительно к анализируемому составу позволяет предположить, что при самонадеянности виновное лицо предвидит наступление общественно опасных последствий своего «легкомысленного» обращения (в виде неправомерного доступа) с информацией, но рассчитывает без достаточной на то аргументации их предотвратить; при небрежности виновное лицо не предвидит возможности наступления общественно опасных последствий в результате действий, связанных с неправомерным доступом к компьютерной информацией, хотя при должной внимательности и осмотрительности оно должно было и могло предвидеть эти последствия.

Нельзя не принимать во внимание и вероятность наступления в результате самонадеянного или небрежного обращения с компьютерной техникой в процессе неправомерного доступа к охраняемой законом информации общественно опасных последствий. Разработчики компьютеров приблизились к технологиям, позволяющим, через информационной системы управлять производственными процессами, переводить вредные технологии на обслуживание вычислительной техникой. В таких условиях и самонадеянность, и небрежность могут вызвать катастрофические последствия, в том числе и тяжкие.

В формировании формы вины большую роль играет мотив и цель поведения. Мотив - психическое переживание, побуждение, которое вызывает у человека решимость к действию или благоприятствующее его совершению. Цель - желаемый результат конкретного преступного акта. Мотивы и цель совершения данного преступления могут быть самыми разными; от корысти, мести, исследовательского интереса, злобы до хулиганских побуждений, политического и служебного эгоцентризма.

Зарубежные и отечественные исследователи излагают перечень мотивов неправомерного доступа, связывая их в одних случаях, с социально-

психологическими свойствами различных групп преступников, в других - с особенностями способов совершения преступления. Так, у «неквалифицированных» пользователей мотивы и цели могут отсутствовать полностью. Для «любителей» характерны такие мотивы, как хулиганские побуждения, самоутверждение, исследовательский интерес. Для «профессиональных» компьютерных правонарушений характерны корыстные мотивы. Для «пользователей» компьютеров мотивы и цели могут быть самыми разнообразными [18, с. 56].

Для данного состава мотив и цель не являются обязательным элементом субъективной стороны и на квалификацию содеянного не влияют, но учитываются при индивидуализации наказания.

По общему правилу субъектом неправомерного доступа к охраняемой законом компьютерной информации может быть любое вменяемое физическое лицо, достигшее к моменту совершения правонарушения шестнадцатилетнего возраста. Особенность субъекта анализируемого правонарушения состоит в том, что пользователь, не обладающий специальными знаниями, вряд ли может причинить компьютерной информации вред, за который законодатель предусматривает уголовную ответственность.

Опасность неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть заключается в том, что в сферу криминальной деятельности втягиваются профессионалы из не криминогенного контингента: а) лица, не связанные трудовыми отношениями с организацией, «атакованной» в криминальных целях; б) сотрудники-пользователи компьютеров, злоупотребляющие своим должностным положением или положением в компании. К первой группе относятся:

- «профессионалы» - это высококвалифицированные специалисты, действия которых характеризуются предварительной подготовкой, целеустремленностью, сокрытием следов правонарушения, прямым умыслом и корыстной направленностью;

- «любители» - это лица, сочетающие профессионализм в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности;

- «пользователи» компьютеров - это лица, обладающие достаточными навыками в работе с компьютерами и совершающими правонарушения «разово», то есть в случае, когда представляется возможность совершить незаконную операцию при помощи компьютера;

- жертвы «компьютерной революции» - это лица, имеющие ограниченные знания в области эксплуатации информационных технологий, в результате чего их неосторожными действиями уничтожается компьютерная информация.

Ко второй группе относятся внутренние пользователи компьютера, которые по роду своей деятельности имеют доступ к компьютера, информационно-коммуникационным сетям и осведомленные об используемых компанией способах и средствах защиты компьютерной техники.

Западные специалисты подразделяют представляющий опасность персонал на следующие категории в зависимости от сфер деятельности:

а) операционные правонарушения - совершаются операторами, периферийных устройств ввода информации в компьютер и обслуживающими линии телекоммуникации;

б) правонарушения, основанные на использовании программного обеспечения, совершаются лицами, в чьем ведении находятся библиотеки программ, системными программистами, прикладными программистами, хорошо подготовленными пользователями;

в) для аппаратурной части компьютерных систем опасность совершения правонарушения представляют: инженеры-системщики, инженеры по терминальным устройствам, инженеру, связисты, инженеры-электронщики;

г) определенную угрозу совершения компьютерных правонарушений представляют и сотрудники, занимающиеся организационной работой: управлением компьютерной сетью, руководством операторами, управлением базами данных, руководством работой по программному обеспечению;

д) определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование компьютеров;

е) особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Отечественные исследователи внутренних пользователей подразделяют на следующие группы:

К первой группе относятся служащие, которые в силу функциональных обязанностей имеют доступ к компьютерной информации.

Ко второй группе относится вспомогательный технический персонал, по востребованности имеющий доступ к компьютерной информации.

К третьей группе относятся лица, косвенно имеющие доступ к средствам компьютерной техники в силу занимаемого ими служебного положения.

К четвертой группе относятся лица, которые не имеют доступа к средствам компьютерной техники, к компьютерной информации и не имеет специальных познаний в этой области (например, уборщики помещений, сотрудники службы охраны и т.д.) [18, с. 46].

Несмотря на то, что особое внимание исследователей уделяется «внешним» правонарушителям, в действительности подавляющее большинство правонарушений совершается «внутренними» правонарушителями. Около 90 % злоупотреблений в финансовой сфере,- связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих работников банков. Причем на криминальный путь становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории служащих.

Компьютерные правонарушения, совершаемые в компаниях, связаны, как правило, с ошибками или умышленным «нападением» служащих компаний:

ошибки персонала - 55 %:

проблемы физической защиты - 20%;

нечестные сотрудники - 10%:

обиженные сотрудники - 9%;

распространение «вирусов» - 4%;

внешнее нападение- 1-3% [31, с. 43].

Выделение типовых моделей разных категорий правонарушителей, знание их основных черт способствует процессу определения круга лиц, среди которых может оказаться субъект правонарушения.

Лицо, использующее свое служебное положение или имеющее доступ к компьютеру, информационной системе или информационно-коммуникационной сети, - это законный пользователь, обладающий правом доступа и обработки определенного рода информации в связи с выполнением своих служебных обязанностей, вытекающих из трудовых отношений (заключенного контракта) [88].

Неправомерный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры «электронные корсары», «компьютерные пираты» - так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети. Техника правонарушения проста – набирая один номер за другим, они дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственном компьютере и устанавливается автоматическая связь и необходимый код. Таким образом, можно внедриться в чужую компьютерную систему.

Несанкционированный противоправный доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, правонарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, подобно покупателю, изучающему товары на витрине.

Также программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей компьютерной логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению возможности совершения противоправного деяния. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что правонарушитель проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого способа правонарушения. Самый простейший путь его осуществления – это получить коды и другие идентифицирующие шифры законных пользователей. Это возможно:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;

- незаконным, несанкционированным подслушиванием через телефонные линии.

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и

намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом незаконно получить некоторую ценную информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе компьютера, своеобразный аналог инструкций и приспособлений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа - мощный и опасный инструмент в руках преступника. Несанкционированный доступ также может осуществляться в результате системной поломки компьютера. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Говоря фигурально, все происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В результате он может проникнуть в чужие сейфы и похитить все, что в них хранится.

### 3.2 Характеристика объективных и субъективных признаков состава правонарушения "Создания, использования и распространения вредоносных компьютерных программ и программных продуктов"

Следует отметить, что данное правонарушение отнесено к наиболее общественно опасным деяниям из числа правонарушений, посягающих на компьютерную информацию, что выражается в размере санкций и в конструировании ч. 1 ст. 210 УК РК в виде формального состава. Наибольший вред собственникам, владельцам и законным пользователям компьютерных средств и информационных ресурсов приносят именно вредоносные программы.

Объектом данного правонарушения являются общественные отношения по безопасному использованию информации, содержащейся в информационной

системе или передаваемой по информационно-коммуникационной сети, а также программного обеспечения компьютерной информации.

В качестве предмета правонарушения выступают компьютерные программы и программные продукты, которые являются разновидностью компьютерной информации. Законодатель в ч. 1 ст. 210 УК РК предусматривает возможность «...внесение изменений в существующую программу или программный продукт», тем самым определяет программные средства в качестве предмета правонарушения, которые могут быть подвергнуты противоправному воздействию, оговоренному в уголовном законе: уничтожению, блокированию, модификации, копированию и др.

К обязательным признакам объективной стороны правонарушения, предусмотренного ч. 1 ст. 210 УК РК относится общественно опасное деяние в виде: а) создания компьютерной программы, программного продукта б) внесение изменений в существующую программу или программный продукт, в) использование такой программы или программного продукта, г) их распространение.

Общественно опасное деяние в данном составе всегда проявляется в активной форме поведения виновного, то есть в действии. Понятие «создание вредоносной компьютерной программы » - это сложный многоэтапный процесс написания программы: от возникновения идеи и определения основных принципов работы программы до написания ее исходного текста и компилирования. В диспозиции статьи подразумевается создание программ для компьютеров, которые могут быть «вредными» и «безвредными». Определение вредоносности программы осуществляется только специалистами на основании информационно-технологической экспертизы и с учетом установления общественно-опасного характера последствий их действия.

С программно-технической точки зрения «компьютерный вирус» - это специальная компьютерная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять самые различные нежелательные Действия (например, испортить, стереть файл,

засорять оперативную память компьютера, создавать помехи в работе компьютера и т.п.). «Компьютерные вирусы» способны к само воспроизводству, модификации, маскировке и даже консервации на определенный период, они могут порождать новые вирусы. Они являются средством несанкционированного уничтожения, блокирования модификации, копирования компьютерной информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети.

В современном мире существует более 5 млн. видов программ-вирусов, и их количество ежегодно возрастает. По некоторым данным, в мире ежедневно создается от пяти до десяти новых вирусных программ [89].

В последнее время появились программы - генераторы вирусов, которые позволяют получить текст нового вируса. Сам же процесс создания «вируса» может осуществляться одним из следующих способов: непосредственно в компьютере, информационной системе или информационно-коммуникационной сети, вне компьютерной системы с последующим внедрением «вируса».

Количество вирусов постоянно увеличивается. Все «вирусы» можно разбить на несколько групп:

а) системные вирусы (поражают загрузочные секторы электронной памяти);

б) файловые вирусы (поражают исполняемые файлы);

в) комбинированные вирусы (сочетающие свойства вышеуказанных вирусов в определенной алгоритмической совокупности).

По способу заражения компьютерной техники вирусы подразделяются на:

а) резидентные (находится в оперативной памяти компьютерной системы потерпевшей стороны и является активным вплоть до ее выключения или перезагрузки. Активизируется после каждого включения компьютерной системы);

б) нерезидентные (не заражают оперативную память компьютерной системы, являются активными некоторое время и не имеют способности к распространению).

По алгоритму строения вирусы подразделяются на:

а) «вульгарный вирус» (компьютерная программа, написанная единым блоком);

б) «раздробленный вирус» (компьютерная программа, разделенная на части, содержащие инструкции как, в какой последовательности, в какое время собрать их воедино).

Помимо вирусов, по характеру своего действия выделяют следующие вредоносные программы:

- «троянский конь», когда под известную программу вуалируется другая, которая, проникнув в информационно-вычислительные системы, внедряется в иные программы (иногда методом вставки операторов), начинающие работать неожиданно для законного пользователя по-новому;

- «троянская матрешка» (вредоносные команды формируются опосредованно через другие команды), «салями» и другие разновидности «троянского коня», «салями» применяется к программам, используемым в бухгалтерии. С помощью этой программы осуществляются компьютерные хищения. Принцип ее работы заключается в изъятии малых средств с каждого большого числа при совершении определенных операций, например, зачислении денег на счет или конвертации из одного вида валюты в другой. Программа названа так ввиду сходства с процессом отрезания тонких ломтиков одноименной колбасы. Программа эта весьма удобна для преступников, так как хищение оказывается высоко латентным ввиду того, что пропажу мизерных сумм выявить весьма сложно. Вместе с тем, учитывая скорость работы компьютера и частоту совершаемых операций (например, в пределах крупного банка), суммы, похищенные таким образом, оказываются в результате достаточно велики;

- «логическая бомба» - срабатывание определенных команд, неправомерно внесенных в какую-либо программу при определенных обстоятельствах, часто направленных на уничтожение данных. Иногда выделяют такой подвид, как «временная бомба», когда вредоносная программа или команда срабатывает по истечении определенного времени;

- компьютерные «черви». По характеру эта программа схожа с компьютерными вирусами. Отличие состоит в том, что «червь» - это самостоятельная программа.

Вредоносные программы могут сочетаться. Общественная опасность создания вредоносной программы определяется не столько способностью уничтожать, блокировать, модифицировать, копировать информацию, сколько способностью выполнять эти функции без получения санкции (согласия) собственника или законного владельца информации. Вредоносные программы содержат либо «вирусы», либо команды («троянский конь», «люк», «асинхронная атака», «логическая бомба» и т.п.), либо обладают свойствами, предназначенными для выполнения неправомерных действий.

Объемы и характеристики вредоносных программ разнообразны. Объединяющим является их разрушительное воздействие на информационные ресурсы, а в некоторых случаях и на сам компьютер.

Под программой для компьютера следует понимать объективную форму представления совокупности данных и команд, которые предназначены для функционирования компьютерной техники с целью получения определенного результата [90, с. 498]. Из определения следует, что создание программы следует считать оконченным с момента завершения процесса компилирования [91, с. 231]. Программой можно считать лишь реализованный алгоритм (совокупность данных и команд) в виде компилированного текста, декомпилированная, не переведенная на электронный язык программа, представляет собой обыкновенный текст. Законодатель устанавливает ответственность за создание таких вирусных программ, которые обладают способностью несанкционированного уничтожения, блокирования,

модификации, копировании информации либо нарушению работы компьютера, информационной системы или информационно-коммуникационной сети.

Внесение изменений в существующую программу или программный продукт для компьютера означает изменение теста программы путем исключения его отдельных фрагментов, замены их другими либо их дополнения новыми фрагментами посредством специального программного продукта или вручную. Внесение изменений в существующие программы - это комплекс операций с целью модификации ее во вредоносную. Причем «вирусной» программа становится именно в результате этих изменений.

Использование вредоносной программы для компьютера - это умышленное воспроизведение, распространение, установка или иные действия по введению программы в оборот в первоначальной или измененной форме. Под использованием понимается применение, запуск, вредоносной программы для осуществления функций, для которых она предназначена. Таким образом, использование вредоносной программы заключается во всяком ее употреблении по прямому назначению.

Распространение вредоносных программ для компьютера - это предоставление доступа к программе для компьютера в компилированном виде, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы либо создание условий для самораспространения программы.

Распространение вредоносных программ для компьютера возможно следующими способами:

- активным (посредством внедрения ее в компьютер, информационную систему или информационно-коммуникационной сеть);

- пассивным (не воспрепятствование самораспространении вредоносной программы или распространению ее третьими лицами).

К понятию распространение можно отнести и действия по сознательному представлению доступа другим пользователям к воспроизведенной вредоносной программе и программных продуктов или работа на чужом

компьютере с использованием дискеты с записью вредоносной программы. Распространение «вируса» может осуществляться посредством копирования вредоносной программы с диска на диск или через модем, компьютерную сеть, электронную почту.

Использование электронных носителей с вредоносными программами и продуктами заключается во всяком их употреблении с целью использования записанной программы для компьютера. При этом под электронным носителем понимаются устройства, позволяющие сохранять вне компьютера компьютерную информацию: дискеты, магнитные ленты, магнитооптические диски, флешки, жесткие диски.

Распространение электронных носителей с вредоносными программами и программными документами означает передачу электронных носителей третьим лицам как возмездно, так и безвозмездно либо предоставление им возможности пользования этими носителями. Распространение электронных носителей с вредоносными программами и программными документами представляет собой один из способов их распространения (к примеру, сетевой способ) и по сути дела является альтернативным распространению вредоносных программ и программных продуктов деянием.

Состав уголовного правонарушения является формальным, поэтому для уголовной ответственности не требуется наступления каких-либо общественно опасных последствий. На формальный характер конструкции состава указывает факт заведомости приведения к общественно опасным последствиям созданной вредоносной программы и программных продуктов, внесенных в программу и программные документы изменений, а также их использование и распространение. Такое построение состава связано с характером перечисленных в диспозиции статьи деяний.

Правонарушение признается оконченным в момент завершения создания компьютерной программы и программного документа или их использования, распространения, независимо от того, наступили общественно опасные последствия или нет.

Большинство ученых полагает, что психическое отношение к выполнению действий, образующих объективную сторону состава правонарушения, предусмотренного ч. 1 ст. 210 УК РК, характеризуется прямым умыслом. Виновное лицо сознает, что его действия по созданию, использованию или распространению соответствующих программ носят общественно опасный характер, предвидит неизбежность наступления несанкционированного уничтожения, блокирования, модификации, копировании информации, нарушения работы компьютера, информационной системы или информационно-коммуникационной сети и желает их наступления.

Единообразного определения признака заведомости в юридической литературе нет. Одни рассматривают «заведомость» в ряду с факультативными признаками субъективной стороны [92, с. 43], другие как обстоятельство, характеризующее интеллектуальный момент вины, третьи как признак волевого момента [93, с. 31]. Вместе с тем, учеными не уделяется достаточного внимания субъективному признаку «заведомости».

Признак «заведомости» характеризует осознание субъектом правонарушения социальной опасности и противоправности совершаемого им деяния в виде создания вредоносных программ для компьютера или внесения вредоносных изменений в существующие программы или программные продукты, а равно использования либо распространения таких программ или электронных носителей с такими программами. Для признания прямого умысла в действиях виновного лицо, необходимо установить, что степень осведомленности последнего вредоносности программы была исключительно велика. Лицо не обязательно должно быть достоверно уверено в наличии вредоносности компьютерной программы, достаточно того, что оно с высокой степенью вероятности это допускает.

Таким образом, интеллектуальный элемент прямого умысла при создании, внесении изменений, использовании и распространении вредоносной компьютерной программы определяется как такое состояние сознания

виновного лица, когда он знал (или допускал с высокой степенью вероятности), что данная программа может привести к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети. Волевой элемент прямого умысла характеризуется желанием совершить действия, образующие объективную стороны рассматриваемого формального состава правонарушения.

Ученые, считающие возможным признание косвенного умысла в рассматриваемом составе, признак сознательного допущения относят к характеристике волевого момента умысла. Нам представляется, что с учетом сложности технических процессов, протекающих в компьютерных системах, законодательно установленный признак «заведомости» осознания виновным лицом возможности наступления общественно опасных вредоносных последствий, указанных в диспозиции ч. 1 ст. 210 УК РК, является достаточным основанием расценивать поведение виновного лица как совершаемого с прямым умыслом.

Данный подход позволяет облегчить в значительной степени правильное применение рассматриваемой нормы права, т.к. не требует установления абсолютно четкого знания виновным свойств вредоносной программы и безусловного представления картины возможных общественно опасных последствий. При обращении с техникой столь высокого класса можно говорить только о высокой степени вероятности предположений, что идентично «желанию» в обычных материальных составах.

В последнее время исследователи поднимают вопрос о существовании «компьютерной» этики и «компьютерной» морали. Так, «хакеры» имеют собственную этику. Не видя жертву, они не осознают противоправность своего поведения, полагая, что нажатие кнопки на компьютере не образует преступления. Кроме того, для них характерно чувство безнаказанности. Они не устанавливают прямого контакта с жертвой, могут действовать из

собственной квартиры, способ совершения преступления позволяет не оставлять материальных следов криминальной деятельности, а для установления личности правонарушителя потребуется длительный промежуток времени, применение сложных технических устройств и привлечение специалистов.

Не менее важным обстоятельством, определяющим характер субъективной стороны, является то, что использование программного продукта и различные манипуляции с ним предполагает наличие у виновного лица большого аспекта разветвленных в: от узко операциональных (простая работа с клавиатурой) до ориентации в сетевом пространстве.

Цель данного правонарушения -неправомерное уничтожение, блокирование, модификация, копирование, использование информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, нарушение работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети.

Субъект данного правонарушения является общим: физическим вменяемым лицом, достигшим установленного законом возраста уголовной ответственности. Ответственность за незаконное обращение с вредоносными программами наступает с шестнадцати лет. Однако субъект данного правонарушения должен обладать и определенными профессиональными навыками и знаниями. Вредоносную программу создать или ее модифицировать может только человек, обладающий навыками в обращении с компьютерной техникой и в написании программы (профессиональные программисты, лица, освоившие основы программирования).

Законодатель в части 2 ст. 210 УК РК предусматривает повышенную уголовную ответственность за те же деяния, совершенные группой лиц по предварительному сговору, лицом с использованием своего служебного положения, в отношении национальных электронных информационных ресурсов или национальной информационной системы.

В части 3 вышеуказанной статьи установлена уголовная ответственность за те же деяния, совершенные преступной группой или повлекшие тяжкие последствия.

На основании вышесказанного необходимо сделать некоторые выводы:

1. Уголовные правонарушения в сфере информатизации и связи, особенно это касается взлома удаленных компьютеров, практически являются идеальной возможностью для правонарушителей совершать свои деяния без наказания. Практическая возможность доказательства этих правонарушений сводится к цифре очень приближенной к нулю. Конечно, особо громкие дела известны всему миру, но в связи с компьютерной и законодательной безграмотностью нашего населения дела, связанные с хищением информации, взломов компьютеров и тому подобное, почти никогда не заводятся, а если такое случается, то редко и сложно доказуемые.

2. Все компьютерные правонарушения условно можно подразделить на две большие категории - правонарушения, связанные с вмешательством в работу компьютеров и правонарушения, использующие компьютеры как необходимые технические средства.

## 4 Проблемы совершенствования мер противодействия компьютерным правонарушениям (преступлениям)

### 4.1 Взаимодействие государств в решении проблем, связанных с компьтерными преступлениями (правонарушениями)

Развитие научно-технического прогресса в XX в., обусловившее появление научно-технических достижений глобального значения, связано с новыми проблемами, затрагивающими интересы не только отдельных лиц и государств, но и международного сообщества в целом. Появление новых научно-технических объектов как результат извечного и постоянного стремления человечества к познанию окружающего мира относится, несомненно, к прогрессивным явлениям, но использование этих объектов может повлечь как позитивные, так и негативные последствия, так как неразрывно связано с рядом этических, политических и правовых проблем ответственности государств и индивидов.

С распространением производства компьютеров в 50-х гг. XX в. и появлением технологий электронных коммуникаций в 70-х гг. преодоление негативных последствий использования новых технических достижений постепенно трансформировалось из проблемы, разрешаемой в пределах отдельных государств, в проблему межгосударственного сотрудничества.

Для анализа проблем межгосударственного сотрудничества по борьбе с компьютерными преступлениями (в данном случае речь идет именно о преступлениях, так как сотрудничество на международном уровне возможно только по наиболее общественно опасным деяниям в вышеуказанной сфере) первостепенное значение имеет определение компьютерного преступления как международно-правовой категории.

В настоящее время термин «компьютерные преступления» используется в ряде международно-правовых документов.

Под международным преступлением понимается деяние, возникающее в результате нарушения государством международного обязательства, столь основополагающего для жизненно важных интересов международного

сообщества, что его нарушение международным сообществом рассматривается как преступление. При использовании глобальных компьютерных систем будут действовать положения ст. 4 Международной конвенции о ликвидации всех форм расовой дискриминации [94] от 07 марта 1966 года об осуждении государствами-участниками всякой пропаганды, основанной на идеях превосходства одной расы или группы лиц определенного цвета кожи или этнического происхождения, или пытающейся оправдать или поощрять расовую дискриминацию в какой бы то ни было форме. Кроме того, пункт «с» ст. 3 Конвенции о предупреждении преступления геноцида и наказании за него [95] от 09 декабря 1948 года содержит запрет на прямое и публичное подстрекательство к совершению геноцида, которое может быть осуществлено с использованием технологий электронных коммуникаций. Более того, компьютерные сети могут быть использованы для подготовки и координации совершения других международных преступлений, а компьютеры, управляющие военными объектами, могут непосредственно служить средством агрессии. Представляется вполне обоснованным отнесение международных преступлений, связанных с использованием компьютерной техники, к особой группе компьютерных преступлений.

С использованием компьютеров может быть совершен также и ряд преступлений международного характера - деяний, предусмотренных международными договорами и посягающих на нормальные отношения между государствами, наносящих ущерб мирному сотрудничеству в различных областях отношений, а также организациям и гражданам, наказуемых либо согласно нормам, установленным в международных договорах, либо нормам национального законодательства в соответствии с этими договорами. В частности, противоправным является распространение по компьютерным сетям порнографических предметов, анонсирование или оглашение каким бы то ни было путем (в целях поощрения оборота или торговли порнографическими предметами), что какое-либо лицо занимается их распространением или торговлей, а также способов их получения, что следует из положений ст. 1

Международной конвенции о пресечении обращения порнографических изданий и торговли ими от 12 сентября 1923 года [96].

Следует отметить, что в настоящее время глобальный характер приобрели различные способы мошенничества с использованием компьютеров, в частности в банковских сетях, распространение программного обеспечения и баз данных без получения необходимых лицензий от лица, обладающего правами на соответствующие объекты интеллектуальной собственности, и другие правонарушения, связанные с функционированием компьютеров. Не могут не вызывать опасений за состояние международного мира и безопасности периодически появляющиеся в печати сообщения о «взломе» хакерами баз данных и программного обеспечения Пентагона.

В целях эффективной борьбы с неправомерным использованием компьютерной техники компьютерные преступления не должны пониматься в узком смысле, как они понимаются в актах ОЭСР и Совета Европы, предусматривающих достаточно ограниченный перечень преступлений, непосредственно связанных с нарушением нормального функционирования компьютеров. Для определения понятия компьютерных преступлений в первую очередь следует учитывать способ их совершения.

Таким образом, к компьютерным следует отнести все преступления, совершаемые с использованием отдельных компьютеров либо технологий электронных коммуникаций.

Не исключено, что с развитием компьютерных сетей государства будут согласовывать новые нормы, содержащие меры по борьбе с преступлениями, связанными с использованием компьютеров и круг преступлений международного характера расширится.

Компьютерная преступность в условиях функционирования глобальных компьютерных сетей приобретает транснациональный характер, вследствие чего меры борьбы с ней должны предусматриваться не только в национальном законодательстве.

Информационная безопасность страны - это «состояние защищенности страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз» [97, с. 359].

Проблемы, возникающие в процессе сотрудничества государств в борьбе с компьютерными преступлениями, равно как и проблемы, связанные с сотрудничеством по пресечению и наказанию иных категорий преступлений, можно подразделить на следующие группы:

1) определение места совершения преступления;

2) выявление преступления и выдача преступников;

3) расследование преступления;

4) судебное преследование, в том числе передача судопроизводств;

5) определение места отбывания наказания за совершенное преступление.

В отношении компьютерных преступлений проблемы определения места совершения преступления, выявления преступления и его расследования являются наиболее сложными. Указанные преступления имеют высокую степень латентности, способы их совершения обусловливают значительные трудности в раскрытии, поскольку преступники, используя компьютер и коды доступа, остаются, по существу, анонимными. Более того, раскрытие таких преступлений возможно только вследствие привлечения высококвалифицированных специалистов в области компьютерной техники, обладающих не меньшим уровнем знаний, чем хакеры. Раскрытие преступлений усложняется и тем, что преступник, как правило, может находиться в одном государстве, а результаты преступной деятельности проявляются на территориях других государств.

Что касается определения места совершения преступления, то государства могли бы установить соответствующие правила путем заключения многостороннего договора. Представляется целесообразным предусмотреть в договоре положение, согласно которому местом совершения компьютерного преступления должна признаваться территория того государства, где наступили

последствия совершенного деяния. Но в случае, когда известно, с какого компьютера был произведен ввод данных и иные действия, представляющие собой преступное вмешательство в функционирование других компьютеров, в том числе и находящихся на территории иностранных государств, место нахождения такого компьютера должно признаваться местом совершения преступления. Место совершения преступления может быть определено отдельно для каждого деяния, даже если они совершались одним и тем же лицом.

Более сложной является проблема указания национальных органов, которые компетентны расследовать компьютерное преступление. В многостороннем договоре можно согласовать общее правило о расследовании компьютерных преступлений по месту их совершения с рядом исключений из общего правила. Во-первых, компьютерные преступления могут быть совершены на территории государства, которое не обладает необходимыми техническими приспособлениями, а также не имеет специалистов для их расследования. В таком случае возможна передача возбужденного уголовного дела для расследования органам другого государства после консультаций между компетентными представителями соответствующих государств. Во-вторых, если компьютерные преступления совершены одним и тем же лицом, возможна передача дела для расследования органам государства, где соответствующее лицо имеет место жительства, либо гражданином которого указанное лицо является. В-третьих, при совершении одним и тем же лицом компьютерных преступлений, последствия которых имели место в нескольких государствах, уголовные дела в отношении данного лица могут быть возбуждены в каждом из государств. Затем путем взаимных консультаций государства могут договориться о расследовании дела органами одного государства либо создании совместного органа по расследованию данного дела. В-четвертых, передача материалов уголовного дела, возбужденного по факту совершения компьютерного преступления, возможна и компетентным органам по месту жительства либо нахождения потерпевшего, если расследование дела

этими органами будет соответствовать интересам потерпевшего и целям быстрого и полного установления всех обстоятельств дела.

В.П. Талимончик считает, что наиболее полно интересы государств в борьбе с компьютерными преступлениями могут быть обеспечены вследствие создания системы международного контроля за передачей информации в компьютерных сетях и расследования правонарушений, связанных с использованием глобальных компьютерных сетей и отдельных компьютеров, имеющих трансграничные последствия [98, с. 17]. При этом должны соблюдаться специальные принципы международного обмена информацией, и в первую очередь принцип свободного, широкого и сбалансированного распространения информации. Система международного контроля и расследования может быть создана только при условии использования средств, которые не будут препятствовать свободному распространению правомерной информации и создавать условия для неправомерного доступа к информации, затрагивающей права человека.

Контроль за содержанием информации, расследование наиболее сложных либо затрагивающих интересы двух и более государств преступлений, координация деятельности национальных органов по расследованию компьютерных преступлений должны осуществляться в рамках международной организации.

Возможно, контроль за содержанием электронных данных и расследование будет входить в функции Интерпола. Но в таком случае нельзя не учитывать, что Интерпол координирует сотрудничество национальных органов уголовной полиции, борьба с международными преступлениями непосредственно в ее компетенцию не входит. Видимо, для координации сотрудничества государств в борьбе с международными компьютерными преступления и компьютерными преступлениями международного характера будет создана единая международная организация.

Создание международной организации по борьбе с компьютерными преступлениями будет способствовать эффективности межгосударственного

сотрудничества в данной области. В частности, государства, не обладающие высококвалифицированными кадрами и развитыми системами коммуникаций, смогут обращаться к ней за помощью. Даже государства, которые обладают всем необходимым для расследования компьютерных преступлений, нуждаются в информационном обеспечении своей деятельности, получении данных об опыте других государств. Для расследования в рамках такой организации могут быть переданы преступления, затрагивающие интересы множества государств и требующие совместных усилий по их раскрытию.

Таким образом, можно сделать вывод, что борьба с компьютерной преступностью связана как с использованием традиционных средств, применяемых государствами (в рамках существующих международных организаций, а также на основе двусторонних договоров о правовой помощи и многосторонних договоров по вопросам борьбы с отдельными видами правонарушений и оказанию правовой помощи по уголовным делам), так и с созданием новых, более эффективных средств.

## 4.2 Меры противодействия компьютерным преступлениям (правонарушениям)

Правоприменительная практика свидетельствует, что одним из главных направлений в борьбе с преступностью (правонарушениями) является её предупреждение. Идея о том, что предупреждение преступности (правонарушений) должно иметь приоритет перед карательной политикой государства, была высказана еще Платоном в IV в. до н.э. Суть кардинального подхода к вопросам борьбы с преступностью (правонарушениями) закрепилась в следующей формуле: «Мудрый законодатель предупредит преступление, чтобы не быть вынужденным наказывать за него».

Предупреждение преступлений (правонарушений) в «широком» смысле слова представляет собой систему экономических, социально-культурных, воспитательных и правовых мер, осуществляемых органами государственной

власти в процессе формирования правового государства и гражданского общества. Предупреждение преступности (правонарушений) выступает особым видом деятельности в области социального управления.

Предупреждение преступлений (правонарушений) в «узком» смысле - это комплекс специальных мер, предпринимаемых правоохранительными органами, по недопущению или пресечению криминальных посягательств и осуществляемый различными предусмотренными законом средствами [79, с. 234].

Криминология, разрабатывающая вопросы предупреждения преступности, выделяет несколько таких систем:

1. в зависимости от иерархии причин и условий преступности:

- общесоциальный уровень предупреждения,
- специально-криминологический уровень предупреждения;
- индивидуальный уровень предупреждения.

2. в зависимости от конкретного содержания:

- экономические меры предупреждения,
- социальные меры предупреждения,
- идеологические меры предупреждения,
- технические меры предупреждения,
- организационные меры предупреждения,
- правовые меры предупреждения.

Рядом ученых компьютерные системы рассматриваются как источник повышенной опасности, нарушающие отношения общественной безопасности, призванные удерживать указаны технические системы в безопасном, упорядоченном состоянии.

Поэтому предупредительные меры применительно к преступлениям (правонарушениями) в сфере информатизации и связи неразрывно связаны с таким более широким понятием как обеспечение информационной безопасности, которая предполагает наличие целостной системы отслеживания

обстановки в различных странах и своевременного обмена информацией внутри государства.

К основным источникам угроз информационной безопасности относятся:

1. Естественные, вызванные объективными природными явлениями, не зависящими от деятельности человека;

2. Искусственные, порожденные деятельностью человека, которые обусловлены:

а) непреднамеренной деятельностью человека (неумышленные ошибки в разработке компьютерных программ, в разработке программного продукта, в процессе эксплуатации компьютера и т.п.);

б) преднамеренная деятельность человека, сопряженная с умыслом, корыстными устремлениями, имеющая уголовно-правовую мотивацию и преследующая противоправные цели.

В условиях стремительного развития информационных технологий меры противодействия компьютерным правонарушениям должны являться составной частью всего комплекса экономических, политических, правовых, организационных мероприятий по обеспечению информационной безопасности общества и государства. Сущность противодействия компьютерным правонарушениям заключается в выработке комплексной системе мер, предопределенных особенностями компьютеров как технических сооружений и спецификой обрабатываемой и получаемой с сё помощью информации.

На этот процесс оказывают влияние такие объективные факторы как:

а) непотребляемость информационных ресурсов (они подвержены лишь моральному износу);

б) их нематериальность (они не сводимы только к электронным носителям, в которых воплощаются);

в) их высокий экономический потенциал (за счет сокращения людских, сырьевых, энергетических и т.п. ресурсов);

г) наличие мощного потенциала организационно-технических средств защиты;

д) варьирование информационной ценности и функционального значения программного продукта от детской игры до схем обслуживания военно-промышленного комплекса.

Почти все виды компьютерных правонарушений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих правонарушения и условий, способствующих их совершению.

Каких-то особых методов для борьбы с правонарушениями в сфере информатизации и связи в Казахстане нет. Используются те же методы, что и во всем мире. В мировой практике борьбы с компьютерной преступностью (компьютерными правонарушениями) применяются в совокупности правовые, организационные и технические методы [94, с. 19].

На основе данных, полученных в ходе анализа отечественной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с компьютерной преступностью (компьютерными правонарушениями), можно выделить три основные группы мер предупреждения:

1) правовые;

2) организационно-управленческие;

3) технические.

К правовым мерам предупреждения правонарушений в сфере информатизации и связи в первую очередь относятся нормы законодательства, устанавливающие уголовную ответственность за указанные выше противоправные деяния.

К правовым методам относятся разработка норм, устанавливающих ответственность за правонарушения в сфере информатизации и связи, защиту авторских прав программистов, совершенствование уголовного и гражданского

законодательства, а также судопроизводства, принятие международных договоров в данной сфере.

История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона уже в 1978 году. Принятый закон назывался «Computer crime act of 1978» и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства.

Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных правонарушений. Отечественное законодательство движется в этом направлении следующими шагами.

Первым из них по праву законодательным шагом можно считать принятие в июле 1997 года Уголовного Кодекса Республики Казахстан и выделяющего информацию в качестве объекта уголовно-правовой охраны.

Этим актом отечественное уголовное законодательство приводится в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран.

Вторым прогрессивным шагом является принятие Закона РК «О связи» в 1999 году и его переиздание в 2004 году [99].

Следующим важным шагом является принятие в 2007 году Закона РК «Об информатизации».

Данные нормативные акты дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны; устанавливают и закрепляют права и обязанности собственника на эти объекты; определяют правовой режим функционирования средств информационных технологий; определяют категории доступа определенных субъектов к

конкретным видам информации; устанавливают категории секретности данных и информации.

Между тем общеизвестно, что одними правовыми мерами не всегда удается достичь желаемого результата в деле предупреждения правонарушений.

Тогда следующим этапом становится применение мер организационно-управленческого характера для защиты средств компьютерной техники (далее – СКТ) от противоправных посягательств на них.

Организационно-управленческие мероприятия направлены на исключение (или по крайней мере затруднение) возникновения ситуаций, угрожающих безопасности. Они носят сугубо персональный характер и «лежат» в основании политики безопасности конкретного объекта. Данный аспект профилактики наиболее широкий и включает в себя как меры оперативного, так и факультативного характера. В 97 % случаях утечки информации причины происшедшего связаны с изъянами в организационно-управленческой сфере.

К ним относятся мероприятия:

а) регламентирующие процессы функционирования компьютерной системы;

б) осуществляемые при проектировании, строительстве и оборудовании объектов систем обработки информационных данных;

в) определяющие политику безопасности;

г) устанавливающие систему надежной охраны и действенного пропускного режима;

д) распределяющие реквизиты разграничения доступа;

е) направленные на осуществление явного и скрытого контроля за пользователями и т.п.

К организационно-управленческим мерам примыкают кадровые вопросы. Превентивная функция в этой части осуществляется опосредованно. В этих целях проводится тестирование кандидатов на работу; в заключаемых

контрактах отражаются условия конфиденциальности на весь период работы и на определенный срок после расторжения трудового соглашения; периодическое проведение ротации сотрудников; создание служб компьютерной безопасности; обучение персонала правилам защиты информации с учетом последних нововведений и т.п.

При этом различается несколько групп риска:

а) группа малого риска - ранее у сотрудника не отмечались случаи совершения правонарушения в работе с компьютером;

б) пограничная группа риска - у сотрудника в прошлом имелся единичный случай совершения правонарушения при работе с компьютером;

в) группа высокого риска - имеются сведения о неоднократном совершении сотрудником правонарушений при обращении с компьютерной информацией.

Организационные меры защиты СКТ включают в себя совокупность организационных мероприятий: по подбору, проверке и инструктажу персонала; разработке плана восстановления информационных объектов после входа их из строя; организации программно-технического обслуживания СКТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т.д.

Организационные меры являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных правонарушений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к клавиатуре компьютера, используемого как автономно, так и в качестве автоматизированной сети для

передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет правонарушителю свободно использовать компьютер в качестве орудия совершения правонарушения;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной безопасности от компьютерных правонарушений всего лишь необходимо:

1) просмотреть всю документацию в учреждении, организации;

2) ознакомиться с функциями и степенью ответственности каждого сотрудника;

3) определить возможные каналы утечки информации;

4) ликвидировать обнаруженные слабые звенья в защите.

Зарубежный опыт показывает, что наиболее эффективной мерой в этом направлении является введение в штатное расписание организации должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и

централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации снижает вероятность совершения компьютерных правонарушений вдвое.

Кроме этого, в обязательном порядке должны быть реализованы следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к СКТ, должны быть определены категории допуска;

2) определена административная ответственность для лиц за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

3) налажен периодический системный контроль за качеством защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

4) проведена классификация информации в соответствии с ее важностью;

5) организована физическая защита СКТ (физическая охрана).

Помимо организационно-управленческих мер, существенную общепрофилактическую роль в борьбе с компьютерными правонарушениями могут играть также меры технического характера.

Технические меры предназначены для защиты от нежелательного физического воздействия на аппаратные средства и средства связи компьютерной техники, а также для закрытия возможных каналов утечки конфиденциальной информации за счет применения лазерных, радиотехнических и других способов перехвата, а также средства визуального наблюдения, средства связи и охранной сигнализации.

Данный аспект профилактики (посредством технических или программно-аппаратурных мер) опирается на положения физической и интеллектуальной компьютерной безопасности.

Группа технических мер предназначена для закрытия возможных каналов утечки: а) конфиденциальной информации; б) данных, образующихся за счет побочных эдеюромагнитных излучений; в) вибрационных и акустических сигналов, образующихся на перегородках строительных конструкций, окон; в)

данных с помощью применения лазерных, радиотехнических и других способов перехвата.

Реализация этих методов осуществляется путем применения различных технических разработок, устройств и специального оборудования. Для защиты информации используется программное обеспечение антивирусного контроля; применяются различные методы шифрования данных; применение новейших технических мер, обеспечивающих реализацию организационно-управленческого уровня профилактики компьютерных правонарушений.

Различают следующие виды технических мер безопасности:

а) пассивные меры, которые предназначены для погашения или снижения уровня излучения от работающего компьютера (экранирование помещений, использование экранирующих средств, к примеру: металлических штор, специальных аэрозолей);

б) активные меры, которые включают применение специальных генераторов помех, охранной сигнализации, средств защиты портов компьютерной техники, устройств, обеспечивающих только санкционированный доступ идентифицированных пользователей к конфиденциальной информации, к компьютерным системам или сетям и др.

Наиболее важной и значимой в системе технических мер является защита программного обеспечения. В настоящее время к наиболее распространенным способам защиты относятся; дублирование файлов, применение паролей, кодирование, применение защитной оболочки вокруг файла, применение антивирусных программ. Последние являются в настоящее время одним из действенных способов борьбы с компьютерными вирусами, которые способны самопроизвольно присоединяться к другим программам, «заражая» их и вызывая различные нежелательные последствия в виде порчи файлов, искажение результатов вычислений, «засорение» ала стирание памяти и т.п. Современные антивирусные программы способны распознавать и уничтожать как известные, так и неизвестные вирусы и их модификации.

Как разновидность технических средств защиты выделяются физические меры, основанные на применении различных устройств и сооружений, препятствующих проникновению к защищаемой информации, компьютерным системам и сетям, а также технические средства связи, охранной и пожарной сигнализации. К таким мерам можно отнести найтование компьютеров, т.е. прикрепление компьютеров к столам, консолям при помощи специальных зажимов, освобождение от которых возможно с помощью специальных инструментов; использование «стальных рубашек», которые надеваются по окончании работы на компьютер; технические средства визуального наблюдения за компьютерными залами; применение аккумуляторных батарей, обеспечивающих бесперебойное электропитание в экстренных случаях и при авариях и т.п.

Условно технические меры можно подразделить на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно: аппаратные, программные и комплексные.

Аппаратные методы предназначены для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для закрытия возможных нежелательных каналов утечки конфиденциальной информации и данных, образующихся за счет побочных электромагнитных излучений и наводок, виброакустических сигналов, и т.п.

Практическая реализация данных методов обычно осуществляется с помощью применения различных технических устройств специального назначения. К ним, в частности, относятся:

1) источники бесперебойного питания, предохраняющие от скачкообразных перепадов напряжения;

2) устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находятся СКТ;

3) устройства комплексной защиты телефонии;

4) устройства, обеспечивающие только санкционированный физический доступ пользователя на охраняемые объекты СКТ (шифрозамки, устройства идентификации личности и т.п.);

5) устройства идентификации и фиксации терминалов и пользователей при попытках несанкционированного доступа к компьютерной сети;

6) средства охранно-пожарной сигнализации;

7) средства защиты портов компьютерной техники (наиболее эффективны для защиты компьютерных сетей от несанкционированного доступа) и т.д.

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям: а) аппаратуры; б) программного обеспечения; в) данных и управляющих команд.

Для защиты информации при ее передаче обычно используют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.

Все программы защиты, осуществляющие управление доступом к электронной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными.

Доступ может быть определен как:

- общий (безусловно предоставляемый каждому пользователю);

- отказ (безусловный отказ, например разрешение на удаление порции информации);

- зависимый от события (управляемый событием);

- зависимый от содержания данных;

- зависимый от состояния (динамического состояния компьютерной системы);

- частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз);

- по имени или другим признаком пользователя;

- зависимый от полномочий;

- по разрешению (например, по паролю);

- по процедуре.

Также к эффективным мерам противодействия попыткам несанкционированного доступа относятся средства регистрации. Для этих целей наиболее перспективными являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название мониторинга (автоматического наблюдения за возможной компьютерной угрозой).

Мониторинг осуществляется самой операционной системой (далее - ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения электронной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга).

В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия «логической бомбы».

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов особо надо подчеркнуть проблему защиты их от компьютерных вирусов.

Здесь необходимо активно использовать специальные программные антивирусные средства защиты (как зарубежного, так и отечественного производства). Антивирусные программы своевременно обнаруживают, распознают вирус в информационных ресурсах, а также «лечат» их.

Однако, наряду с использованием антивирусных программ, для уменьшения опасности вирусных посягательств на СКТ необходимо предпринять комплексные организационно-технические меры.

1. Информировать всех сотрудников учреждения, организации, использующих СКТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Запретить сотрудникам приносить на рабочее место программные средства (далее - ПС) «со стороны» для работы с ними на СКТ учреждения, организации по месту работы сотрудника.

3. Запретить сотрудникам использовать, хранить на носителях и в памяти компьютера компьютерные игры.

4. Предостеречь сотрудников организации от использования ПС и носителей электронной информации, имеющих происхождение из учебных заведений различного уровня и профиля.

5. Все файлы, которые поступают из внешней компьютерной сети должны обязательно тестироваться.

6. Создать архив копий ПС, используемых в непосредственной работе организации.

7. Регулярно просматривать хранимые в компьютерной системе ПС, создавать новые их архивные копии; где это возможно, использовать защиту типа «только чтение» для предупреждения несанкционированных манипуляций с ценными данными.

8. Периодически проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном.

9. Использовать для нужд электронной почты отдельный стендовый компьютер или ввести специальный отчет.

10. Установить системы защиты информации на особо важных компьютерах. Заактивировать на них специальные комплексные антивирусные ПС.

11. Постоянно контролировать исполнение установленных правил обеспечения безопасности СКТ и применять меры дисциплинарного воздействия к лицам, сознательно или неоднократно нарушавшим их и т.д.

В настоящее время идеальной всеохватывающей системы противодействия компьютерным правонарушениям не существует. Абсолютно надежные технические и физические средства защиты даже в сочетании со стойким персоналом сотрудников не могут обеспечить идеально надежную систему защиты. Только комплексный подход к рассматриваемой проблеме и сочетание различных мер противодействия позволять добиться такой степени защиты компьютерных систем и сетей от криминальных посягательств, которая позволить избежать общественно опасных последствий утечки защищаемой информации.

Комплексные меры защиты, с одной стороны, должны сочетать организационно-управленческие, физические и технические меры, а с другой - кадровые, правовые и морально-этические.

Таким образом, предупреждение преступности (правонарушений) в сфере обращения компьютерной информации рассматривается как средство регулирования информационных отношений; как взаимодействие мер социально-экономического, организационно-правового и воспитательного порядка; как сочетание различных уровней предупреждения компьютерной преступности (правонарушений), воплощенных в деятельности неоднородных субъектов, осуществляющих эту функцию.

Прогрессирование уголовных правонарушений в сфере информатизации и связи в Казахстане пока не имеет больших статистических показателей. На современном этапе развития общества проблема правонарушений в сфере информатизации и связи не грозит обрести те масштабы, которые она имеет в развитых странах. В государстве происходит процесс осваивания рынка локальных и межрегиональных информационных сетей, вхождения в международные сети; решение вопросов компьютерной оснащенности финансовых, управленческих и иных структур на периферии; невелик

кадровый потенциал специалистов по созданию современных информационных технологий.

Указанные факторы носят временный характер и в процессе интегрирования Казахстана в мировое информационное пространство будут изжиты. Увеличивающиеся темпы заполнения отечественного рынка средствами информационных технологий, внедрение в повседневную жизнь компьютерной техники, выявление отдельных фактов совершения компьютерных правонарушений свидетельствует о том, что в ближайшем будущем эта проблема может проявиться. Поэтому вопросы разработки и совершенствования эффективности мер предупреждения уголовных правонарушений в сфере информатизации и связи являются современными, призваны содействовать нейтрализации или минимизации криминогенных последствий от криминальной деятельности и упреждению процессов формирования компьютерных правонарушений.

### 4.3 Некоторые теоретические аспекты контроля над уголовными правонарушениями в сфере информатизации и связи

В условиях рыночных отношений и отсутствия стабильного правового и экономического механизмов защиты собственности (в том числе и интеллектуальной) предупреждение является одним из важнейших средств воздействия на уголовные правонарушения в сфере информатизации и связи. Предупредительный потенциал прежней административно-командной системы управления действовал на детерминанты преступлений, затрагивающих в основном интересы государства. Соответственно формировалась и вся уголовно-правовая политика. Формы и метод превенции основывались на использовании механизмов централизованного управления. В современных условиях, когда производство основывается на частной собственности, этот потенциал ориентирован на децентрализованное управление. В этих условиях

легче заранее предупредить правонарушения, нежели потом исправлять допущенные ошибки, издавая новые законодательные акты.

Превенция уголовных правонарушений в современных условиях должна быть направлена не столько на сокращение предусмотренных материальным правом правонарушений, сколько на нейтрализацию возможных негативно-криминальных последствий от позитивных социальных явлений, коим является процесс информатизации современного общества.

В философском понимании социальный контроль должен обеспечивать определенную организацию общественной жизни, адекватность поведения членов общества взаимным ожиданиям [100, с. 235]. Социальный контроль - это механизм, с помощью которого общество и его структуры (группы, организации) обеспечивают соблюдение системы ограничений (условий), нарушение которых наносит ущерб функционированию социальной системы.

Таким образом, социальный контроль представляет собой совокупность процессов в социальной системе, посредством которых обеспечивается соблюдение определенных ограничений в поведении членов социального консорциума, нарушение которых негативно сказывается на функционировании социальной системы в целом.

Социальный контроль не следует рассматривать как ограничение, лишение самостоятельности и принуждение. Социальный контроль является одной из важнейших функций социального управления и заключается в обеспечении достижения субъектом управления своих целей. На формирование и рост правонарушений в обществе оказывает влияние система негативных явлений, детерминирующих правонарушение как свое следствие. Философия называет около тридцати видов детерминаций. Поэтому и социальный контроль должен складываться из системы экономических, политических, идеологических, правовых и иных мер воздействия.

Основным инструментарием социального контроля являются правовые и моральные нормы, обычаи, традиции, административные предписания и т.п. Следовательно, целенаправленное влияние общества на поведение индивида

осуществляется в том числе и правовыми нормами. Выделение в рамках социального контроля правового имеет важное значение для реализации целей превенции компьютерных правонарушений.

Бесспорно, что правовой контроль должен осуществляться совокупностью методов и средств воздействия всех отраслей права при соблюдении законодателем «сторожевого контрольного фактора». В зависимости от средств и методов, функционально предопределяемых характером правоотношений, применительно к правонарушениям, связанным с использованием компьютерной техники, правовой контроль можно подразделить на два вида: позитивный и репрессивный [77, с. 20].

Позитивный правовой контроль представляет собой совокупность правовых норм, регламентирующих в соответствующей отрасли права информационные отношения, использование информационных ресурсов, а также порядок и условия применения информационного продукта в целях, не влекущих уголовно-правовую ответственность.

Практически во всем мире программы для компьютеров, базы данных, математическое обеспечение компьютеров признаются объектом авторского права. Программа для компьютера может быть объективирована на бумажном носителе или зафиксирована на техническом носителе. Будучи графически отображенной на бумаге компьютерная программа является объектом авторского права. При этом должно сохраняться единство содержания и формы. Авторское право запрещает копирование, размножение, распространение произведения (в данном случае программного продукта) без согласия автора. При реальном функционировании программа для компьютера используется в измененной (по сравнению с рукописью) форме, поэтому не всегда может быть защищена нормой позитивного авторского права.

Будучи зафиксированной на техническом носителе программа для компьютера может быть беспредельно репродуцируема: а) без оставления следов, позволяющих идентифицировать ее с первичной матрицей; б) с изменением формы, как юридического свидетельства нового объекта

авторского права; в) с внесением не концептуальных (не нарушающих первоначально заданных функций) изменений, свидетельствующих о так называемом «независимом (объективном)» совпадении; г) незаконным путем и пущена в торговый оборот; д) снабжена фальшивыми идентифицирующими знаками обозначения фирмы-производителя, фирмы-собственника, товарным знаком и т.п. В подобных ситуациях нормы авторского права не способны защитить интересы разработчиков программного продукта для компьютера и не могут обеспечить эффективный позитивный правовой контроль, Возникающий пробел компенсируется средствами репрессивного правового контроля.

Репрессивный правовой контроль прежде всего обеспечивается нормами уголовного права. И в этой связи УК РК предусматривает ответственность за нарушение прав интеллектуальной собственности (ст. 198 УК РК), незаконное использование товарного знака (ст. 222 УК РК), неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст. 205 УК РК), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК) и др.

На сегодняшний день случаи совершения компьютерных правонарушений носят единичный характер. Вместе с тем, многие государства, образованные на постсоветском пространстве к примеру Российская Федерация, прибалтийские государства, уже столкнулись с этим явлением. Поэтому вопросы совершенствования форм и методов репрессивного правового контроля над компьютерными правонарушениями имеют актуальное значение.

В целом эффективность правового контроля над компьютерными правонарушениями предполагает комплексный характер решения задач как позитивного, так и репрессивного контроля на фоне реализации комплекса государственных мер экономического, политического и организационного характера, обеспечивающих доминирующую роль права и законности в общественной жизни. Анализ научных трудов отечественных и зарубежных исследователей позволяет сформулировать задачи, подлежащие решению в

части установления правового контроля над компьютерными правонарушениями:

- дальнейшее развитие и углубление правовой регламентации отношений, возникающих по поводу и в связи с информацией, в том числе и компьютерной;

- определение роли и места уголовно-правовых норм в системе мер правового контроля над компьютерными правонарушениями;

- определение критериев разграничения деяний, влекущих административную или уголовно-правовую ответственность;

- принятие законопроектов, решающих проблемы информационной (в том числе и компьютерной) безопасности, определяющих круг субъектов данного вида криминальных посягательств;

- выработка и законодательное закрепление перечня охраняемой законом информации разного уровня, позволяющего дифференцировать санкционированный и несанкционированный доступы к компьютерам.

Приведенный перечень не является исчерпывающим и носит прогностический характер в части определения упреждающих мер правового контроля над правонарушениями, связанными с использованием средств компьютерной техники.

Национальная правовая база противодействия компьютерным правонарушениям включает действующий массив законодательных актов, регламентирующих правила обращения с информацией, в том числе и компьютерной и устанавливающих ответственность за их нарушение, постоянно расширяется.

Вместе с тем одними правовыми нормами достичь положительного результата нельзя. Необходимо сочетание правового запрета с морально-этическими мерами. К ним относятся нормы поведения и этики, которые складываются в информационной среде и которые призваны формировать по мере распространения компьютеров в обществе морально-нравственное сознание на базе общечеловеческих ценностей.

Этические нормы и принципы могут оказать положительное влияние на информационную культуру общества в целом и на уровень компьютерных правонарушений в частности. Неслучайно в разработанных ОЭСР руководящих принципах безопасности информационных систем назван принцип этики общения пользователей информационных технологий, который предполагает уважение прав и законных интересов всех субъектов, занятых в использовании и развитии информационных технологий.

Морально-этические нормы бывают как неписаные, так и оформленные в некий свод правил и предписаний (к примеру, Кодекс хакеров, опубликованный в сети Интернет). Эти нормы не носят обязательного характера, но со временем смогут заменить для законопослушных пользователей правовые нормы.

Сегодня формирование этических норм и принципов в информационной среде может существенно отразиться не только на состоянии компьютерных правонарушений, но и положительным образом повлиять на информационную культуру общества, так как эти нормы и принципы - естественное следствие понимание роли и значения современных информационных технологий в жизни государства, общества и каждого человека [17, с. 121].

Перспективные направления профилактической деятельности с правонарушениями в сфере информатизации и связи должны включать вопросы совершенствования законодательства, предусматривающего ответственность за данного рода правонарушения; совершенствование правоохранительными органами правоприменительной практики в отношении указанных уголовно-правовых норм и совершенствование организационных мер, направленных на предупреждение правонарушений в сфере информатизации и связи.

Итак, рассмотрев проблемы, возникающие в борьбе с компьютерными правонарушениями, можно сделать следующие выводы:

1. Правонарушения, совершаемые с использованием компьютерной техники и телекоммуникационных сетей связи, характеризуются высокой степенью латентности. Основной их отличительной чертой является то, что

злоумышленник может совершать противоправные действия, не покидая своей квартиры, дачи или офиса. Компьютерные правонарушения, в том числе хакерские «атаки» финансовых систем и крупных информационных порталов, давно приобрели уже не только организованный, но и трансграничный характер. Универсальные возможности сети Интернет позволяют нарушителям из разных стран договориться и координировать свои деструктивные действия.

2. Рост численности правонарушений, совершаемых в сфере информационного обмена, их многочисленные разновидности и изощренность, способность нарушителей оперативно устранять следы своего вмешательства в нормальное течение информационных процессов - все это обусловливает необходимость в постоянном повышении квалификации, уровня знаний и подготовки правоведов и других специалистов, которые вынуждены противостоять хакерам и другим компьютерным злоумышленникам.

3. Сомнений в необходимости существования уголовно-правовой защиты компьютерной информации нет. Уголовный закон достаточно строго преследует за совершение компьютерных правонарушений. Это связано с высокой степенью общественной опасности.

Также хотелось бы подчеркнуть, что абсолютную надежность и безопасность в компьютерных сетях не смогут гарантировать никакие аппаратные, программные и любые другие решения. В то же время свести риск потерь возможно лишь при комплексном подходе к вопросам безопасности.

## Заключение

Проведенное в настоящей работе исследование казахстанского уголовного законодательства, устанавливающего ответственность за правонарушения в сфере информатизации и связи, рассмотрение отдельных видов правонарушений, совершаемых с помощью компьютера, исследование проблем и способов защиты компьютерной информации от криминальных посягательств позволяет сделать следующие выводы:

1) В настоящее время в нашей стране накоплена научно-теоретическая база, которая свидетельствует о складывающемся устойчивом правовом механизме, нацеленном на защиту компьютерной информации. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стало появление в новом УК РК 2014 года специальной главы 7 «Уголовные правонарушения в сфере информатизации и связи», которая включает 9 статей.

2) Компьютерная преступность не знает границ, она выходит за пределы казахстанской действительности. Это международное понятие и бороться с ней надо согласованно и сообща. С внедрением в человеческую жизнь новых компьютерных технологий, когда обмен информацией стал быстрым, дешевым и эффективным, преступность в информационной сфере переросла за рамки уголовно-правовых норм, направленных для борьбы с ней. Компьютерные правонарушения условно можно подразделить на две большие категории - правонарушения, связанные с вмешательством в работу компьютеров и правонарушения, использующие компьютеры как необходимые технические средства.

3) Проблемы информационной безопасности постоянно усугубляется процессами незаконного несанкционированного проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего информационных систем. Неслучайно, поэтому защита компьютерной информации становится одной из самых острых проблем в

современной информатике. На сегодняшний день сформулировано четыре базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от несанкционированных сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;

- конфиденциальность (законность) информации;

- доступность для всех авторизованных зарегистрированных пользователей;

- защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка).

Анализ действующего казахстанского уголовного законодательства, устанавливающего ответственность за правонарушения в сфере информатизации и связи позволяет говорить о необходимости решения нескольких правовых проблем, которые могут быть рассмотрены в качестве составных частей правового механизма защиты компьютерной информации:

1) Установление контроля над несанкционируемым, противоправным доступом к компьютерным информационным данным системы.

2) Ответственность за выполнение технологических операций, связанных с противоправной деятельностью в отношении компьютерной информации.

Среди наиболее эффективным мер, направленных на предупреждение правонарушений в сфере компьютерной информации выделяются правовые, организационные и технические.

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные правонарушения, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

К правовым мерам относятся также вопросы государственного контроля за разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран.

К организационным мерам относится охрана информационного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания информационного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К техническим мерам следует отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию информационных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Подводя некоторые итоги, можно сделать выводы о том, что сложность компьютерной техники, латентность компьютерных правонарушений, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 205-213 главы 7 «Уголовные правонарушения в сфере информатизации и связи» УК Республики Казахстан.

К сожалению, даже обладая достаточно полным набором значащих элементов портрета компьютерного правонарушителя, мы лишь на 30-49% приближаемся к конкретному правонарушителю. Самое печальное, что дальнейшее продвижение по процентной шкале практически исключено – любое высокотехнично исполненное правонарушение не раскрываемо, если правонарушитель не допустил серьёзных ошибок или его не сдали подельщики. В целом, значительное обновление уголовного законодательства современного

Казахстана в сфере борьбы с киберпреступностью поможет более эффективно противодействовать современным угрозам безопасности личности, общества и государства за счет введения новых норм, направленных на борьбу с данными преступлениями. Конечно одними только уголовно-правовыми мерами невозможно полностью предотвратить эти деяния. Это в принципе относится к противодействию преступности. Определенный задел в виде нормативной основы (разработка уголовно-правового инструментария) создан, однако не стоит абсолютизировать или преувеличивать их значение.

В этой связи следует согласиться с мнением Н. А. Биекенова, о том, что Казахстан становится частью более широкого киберпространства и поэтому представляется необходимым разработать и принять свою государственную программу (концепцию, стратегию) киберзащиты информационного пространства, предусматривающей:

• создание системы постоянного мониторинга киберугроз;

• развитие национальных систем оперативного обнаружения кибератак и противодействия им;

• совершенствование системы взаимодействия государственных силовых структур, отвечающих за кибербезопасность и общественных организаций, работающих в области информационной безопасности;

• организацию программы научно-технических работ по проблемам кибербезопасности[5, с.29].

Думается в свете системного подхода первый шаг сделан: компьютерные правонарушения получили свое признание в качестве самостоятельной группы криминальных деяний.

Следующий шаг - формирование необходимой концептуальной и институциональной базы, наработка правоприменительного опыта. И этому должно быть уделено самое серьезное внимание, иначе шансы на реальные успехи в противодействии с компьютерными правонарушениями будут не высоки, в то время как социальные риски и колоссальные экономические потери от них станут возрастать в геометрической прогрессии.

## Список использованных источников


1. Конституция Республики Казахстан от 30 августа 1995 года, введена в действие 05 сентября 1995 года // Сайт законодательства РК. – http://www.zakon.kz.
2. Бертран де ла Шапель Управление Интернетом. Свобода и регулирование в регионе ОБСЕ. С. 21
3. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Диссер. к.ю.н. -2007. -160 с.
4. Цит: Жатканбаева А. Е. Функциональные компоненты информационной безопасности// Право и государство. 2013. № 4 (61) - С.73
5. Биекенов Н.А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан// Право и государство. -2013. № 4 (61). -С.29
6. Комментарий к Уголовному кодексу Республики Казахстан/ под ред. И.И. Рогова, С.М. Рахметова. Алматы, Баспа. -1999. -С.496.
7. Закон Республики Казахстан "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам деятельности органов внутренних дел" 23 апреля 2014 года № 200-V ЗРК
8. Уголовный кодекс Республики Казахстан от 03 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 02.08.2015 г.) // Сайт законодательства РК. – http://www.zakon.kz.
9. Козаченко И.Я. Уголовный кодекс Республики Казахстан как базисная социальная ценность государства. Модернизация уголовного законодательства: Коллективная монография/ Ответственный редактор А.Е. Мизанбаев. - Костанай. -2014.- С.37-38.
10. Бекмагамбетов А.Б., Ревин В.П. Уголовное право Республики Казахстан. Учебник./Под ред.В.П.Ревина.-Алматы: "Жеты Жаргы",2015.-С.5
11. Исмагулова А.Т.Уголовные правонарушения в сфере информатизации и связи: законодательные новеллы Казахстана / Уголовно-правовая охрана информационного пространства в условиях глобализации: коллективная

монография по материалам XII Международной научно-практической конференции, посвященной памяти М.И. Ковалева (Екатеринбург, 20-21 февраля 2015 г.)/ Под ред. И.Я. Козаченко. Екатеринбург: Издательский дом Уральского государственного юридического университета, 2016. -148 с.

12. Досье на проект Уголовного кодекса Республики Казахстан// http://online.zakon.kz/
13. Закон Республики Казахстан от 06 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» // Сайт законодательства РК. – http://www.zakon.kz.
14. Закон Республики Казахстан № 217-III «Об информатизации» от 11 января 2007 года // Сайт законодательства РК. – http://www.zakon.kz.
15. Компьютерные преступления и обеспечение безопасности ЭВМ. Проблемы преступности в капиталистических странах. - М.: Винити, 1983. -№6. -С.3
16. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 11.
17. Сеитов Т.Е. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане. Учебное пособие. – Алматы: Данекер, 2004. – С. 328.
18. Назмышев Р.А. Криминально-правовая сущность преступлений в сфере компьютерной информации как критерий оценки понятия «компьютерные преступления» // Фемида. – 2003. – № 4. – С. 74.
19. Оспанов Е.Т. Орудие преступления – компьютер // Бюллетень ГСУ и ЭКУ МВД РК. – Алматы: МВД РК, 2005. – №1-2(1-5). – С.35-41.
20. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs. – http://www.Gazeta.Ru.
21. Толеубекова Б.Х. Компьютерная преступность. Монография. – Караганда, 2005. – С. 295.

22. Конвенция о преступности в сфере компьютерной информации. – http://www.oprave.ru.
23. Информация о борьбе с преступлениями в сфере высоких технологий // Департамент криминальной полиции МВД Республики Казахстан. – http://www.crime-research.org.kz.
24. Информация о борьбе с преступлениями в сфере высоких технологий за 2015 г.// Департамент криминальной полиции МВД Республики Казахстан. –http:// http://mvd.gov.kz/
25. Уголовное право. Особенная часть: Учебник для ВУЗов / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М.: Новый юрист, 2008. – 768 с.
26. Крылов В.В. Информация как элемент криминальной деятельности // Вестник Моск. ун-та. Сер. 11. Право. – М., 2008. – № 4. – С. 50-64.
27. Кутузов В., Гуцалюк М., Цимбалюк В. Преступления в сфере высоких технологий. – Минск, 2002. – 268 с.
28. Кутузов В., Гуцалюк М., Цимбалюк В. Преступления в сфере высоких технологий. – Минск, 2002. – 268 с.
29. Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: Сб. матер. межд. конф. 01 – 02 марта 2001 г. – Алматы: Интернет трейнинг центр, 2006. – С. 14.
30. Скородумов Е.И. Безопасность информационных технологий – человеческий фактор // Экономика и производство, 2006. – № 3. – С. 32.
31. Айков Д., Сейгер К.. Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с английского. - М.: Мир, 2004. – 167 с.
32. Лунеев В.В. Преступность 21 века. Мировой криминологический анализ. – М.: Норма, 2007. – 470 с.
33. Комитет по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан. – http://www.kz.

34. Катаев С.Л. Социальные аспекты компьютерной преступности // Центр исследования проблем компьютерной преступности. – Киев, 2008. – С. 43.
35. Ладный В. Проблема распространения в сети информации порнографического характера // Комсомольская правда. – 2004. – 26 января. – №14 (22479).
36. Уголовный кодекс Российской Федерации от 13 июня 1996 г. – № 63-ФЗ. – http://www. consultant.ru.
37. Сальников В.П. Компьютерная преступность: уголовно-правовые и криминологические проблемы. Материалы Международной научно-практической конференции // Государство и право. – 2005. – № 9. – С. 101.
38. Беспалова Е.В., Широков В.А. Компьютерные преступления: основные тенденции развития// Юрист. -2006. -№10. -С.19
39. Полякова Т.А. Вопросы ответственности за использование информационно-телекоммуникационных систем в террористических и экстремистских целях//Российский следователь. 2008. №1.
40. Даровских Ю.В., Григорьев Д.А. Предупреждение экстремизма в сети Интернет (постановка проблемы)//Конституция Российской Федерации как гарант прав и свобод человека и гражданина при расследовании преступлений: материалы Международной научно-практической конференции (Москва, 14 ноября 2013 г.) В 3-х частях. Часть 3 (перспективы совершенствования). М.: Институт повышения квалификации Следственного комитета Российской Федерации, 2013. -81 с. 250 с.
41. Глушков В.М. Основы безбумажной информатики. – М.: Наука, 2007. – 159 с.
42. Воздействие организованной преступности на общество в целом // Материалы Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена. 13 - 23 апреля 1993. – http://www. consultant.ru.

43. Тихомиров В.П. Зачем рынку информационные технологии? // Новин-тех. – 2001. – № 1. – С.17.
44. Анин Б. Защита компьютерной информации. – СПб.: BHV, 2006. – 187 с.
45. Черкасов В. Информация защищена - нет проблем ? // Мир безопасности. – 2007. – № 11. – С.4.
46. Медведовский И.Д. Атака через Internet / Под науч. ред. проф. Зегжды П.Д. - СПб.: Мир и Семья - 95, 2007. – 214 с.
47. Фролов Д.Б., Старостина Е.В. Новая система страха - кибертерроризм // Безопасность информационных технологий. – 2004. – № 2. – С. 38.
48. Голубев В.А. Проблемы борьбы с кибертерроризмом в современных условиях. – http://www.crime-research.ru.
49. Мониторинг состояния сети Интернет и нарушений прав ее пользователей в Казахстане в августе 2008 года. – http://www.info@adilsoz.kz.
50. Закон Республики Казахстан «О средствах массовой информации» № 451-I от 23 июля 1999 года. // Сайт законодательства РК. – http://www.zakon.kz.
51. Бельгибаев С. Интеллектуальный взлом. - http://www.iim.kz.
52. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юрид. лит., 2004. – 372 с.
53. Модельный уголовный кодекс для стран-участников СНГ от 17 февраля 1996 года. – http://www.iacis.ru.
54. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 года. – http://www.pavlodar.com.
55. Расследование компьютерных преступлений // Проблемы преступности в капиталистических странах. – 2002. – № 6. – С.8.
56. Борьба с компьютерной преступностью за рубежом. – М.: Академия МВД РФ, 2005. – 129 с.

57. Gary S. Morris. Основы компьютерного законодательства США // Системы безопасности связи и телекоммуникаций. – 1996. – № 1. – С. 18-19.
58. Карпец И.И. Международная преступность. – М., 1998. – С. 197.
59. Международный обзор уголовной политики ООН. Нью-Йорк. – 2004. – http://www.iacis.ru.
60. Курушин В.Д., Шопин А.В. Предупреждение и раскрытие преступлений, совершаемых с использованием компьютерной техники. – М., 2004. – 249 с.
61. Волеводз А.Г. Противодействие компьютерным преступлениям: Правовые основы международного сотрудничества. – М.: Юрлитформ, 2002. – 496 с.
62. Хакеры угрожают Казахстану. – http://www.crime-research.org.kz.
63. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом (по материалам зарубежной печати): Ежем. информ. бюл. ВИНИТИ. – М., 2006. – № 4. – С. 3-5.
64. Соглашение «О сотрудничестве государств-участников Содружества Независимых государств в борьбе с преступлениями в сфере компьютерной информации» от 01 июня 2001 года. – http://www.bestpravo.ru.
65. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. – М.: Палеотип; Логос, 2009. – 148 с.
66. Комментарий к Уголовному кодексу Республики Казахстан / Под ред. Борчашвили И.Ш.– А., 2007. – 692 с.
67. Крылов В.Б. Информационные компьютерные преступления. – М.: ИНФРА-М-НОРМА, 2007. – 274 с.
68. Курушин В.Д., Шопин А.В. Предупреждение и раскрытие преступлений, совершаемых с использованием компьютерной техники. – М., 2004. – 249 с.

69. Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» // Науч. редактор проф. Волженкин Б.В. – СПб., 2008. – 193 с.
70. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 2007. – № 10. – С. 25.
71. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 2006. – № 1. – С. 14.
72. Лопатина Т.М. Проблемы компьютерной преступности. Учебное пособие. – Петропавловск: Северо-Казахстанская юридическая академия, 2003. – 175 с.
73. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. – М: Право и закон, 2006. – 247 с.
74. Гражданский кодекс Республики Казахстан (Общая часть) № 269-XII от 27 декабря 1994 года. // Сайт законодательства РК. – http://www.zakon.kz.
75. Всеобщая декларация прав человека (принята на 3-ей сессии Генеральной Ассамблеи ООН) от 10 декабря 1948 года // Российская газета. – 1995. - 5 апреля. - http://www.iacis.ru.
76. Исаев А.А. Применение специальных познаний для квалификации преступлений. – Алматы: Мектеп, 2007. – 159 с.
77. Першиков В., Савинков В. Толковый словарь по информатики. – М.: Финансы и статистика, 2003. – 400 с.
78. Зуев К.А. Компьютерная преступность и компьютер против преступности. – М., 2000. – 395 с.
79. Ожегов С.П. Словарь русского языка: Ок. 57000 слов / Под ред. докт. филол. наук, проф. Шведовой Н.Ю. 20-е изд., стереотипное. – М.: Русский язык, 1988. – 750 с.
80. Уголовное право Республики Казахстан. Особенная часть. Учебник для ВУЗов / Под ред. И.Ш. Борчашвили, С.М. Рахметова, в 2-х частях. Часть 2. – Алматы: Данекер, 2006. – 456 с.
81. Толковый словарь по вычислительным системам. – М., 1999. – 281 с.

82. Толеубекова Б.Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники / Автореферат дисс. … докт. юрид. наук. – Астана, 1998. – 190 с.
83. Криминология. Учебник для юридических ВУЗов / Под ред. В.Н. Бурлакова, В.П. Сальникова, С.В. Степашина. – СПб.: Санкт-Петербургский университет МВД России, 1999. – 319 с.
84. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики / Автореферат дисс. … канд. юрид. наук. – Иркутск, 2006. - С. 59.
85. Хакеры: компьютерная преступность. Можно ли ей противостоять? // Мир безопасности. – № 11. – 2007. – С.12.
86. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Телеком, 2002. – 236 с.
87. Бессонов В.А. Виктимологическне аспекты предупреждения преступлений в сфере компьютерной информации. Автореферат дисс...к-та наук. – Н. Новгород, 2000. – С. 10.
88. Мосин О.В. Компьютерная преступность в Казахстане. Как с ней бороться? 2008 г. – Юридический портал «Правопорядок» – http://www.oprave.ru.
89. Kaspersky CRYSTAL 2011 года. Известных вирусов 5405850. – http://support.kaspersky.ru.
90. Комментарий к Уголовному кодексу Республики Казахстан. – Алматы: Баспа, 1999. – 589 с.
91. Воройский Ф.С. Систематизированный толковый словарь по информатике. – М.: Либерия, 1998. – 431 с.
92. Дагель П.С., Котов Д.П. Субъективная сторона преступления и ее установление. – Воронеж, 2004. – 215 с.
93. Якушин В.А. Ошибка и ее уголовно-правовое значение. – Казань, 2008. – 186 с.

94. Международная конвенция о ликвидации всех форм расовой дискриминации (Принята 21 декабря 1965 г. Резолюцией 2106 (XX) Генеральной Ассамблеи ООН) // Ведомости ВС СССР. – 1969. – № 25. – Ст. 219. – http://www.medialaw.ru.
95. Конвенция о предупреждении преступления геноцида и наказании за него (Заключена 09 декабря 1948 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. XVI. – М., 1957. – http://www.medialaw.ru
96. Международная конвенция о пресечении обращения порнографических изданий и торговли ими (заключена в г. Женеве 12 сентября 1923 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. IX. – М., 1938. – http://www.medialaw.ru.
97. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. Б.Н. Топорнина. – СПб., 2001. – 477 с.
98. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств // Законодательство и экономика. – 2005. – № 5. – С. 17.
99. Закон Республики Казахстан «О связи» № 567 от 05 июля 2004 года. –// Сайт законодательства РК. - http://www.zakon.kz.
100. Философский энциклопедический словарь. – М, 2003. – 639 с.

Подписано в печать 04.04.2016
Заказ № 9
Формат 60 х 84 1/16
Бумага офисная.
Печать офсетная.
Объем 10 усл. п. л.
Тираж 100 экз.

Отпечатано
в ТОО «New Line Media»
г. Костанай, пр. Аль-Фараби, 115, оф. 512
тел.: 8 (7142) 53-11-47, 53-06-71
nlmedia.kz, geosprint@mail.ru