Министерство внутренних дел Республики Казахстан
Карагандинская академия имени Баримбека Бейсенова

ИСКАКОВ КУАНЫШ ДУМАНОВИЧ

# Уголовные правонарушения в сфере информатизации и связи: понятие, виды и проблемы квалификации

Шифр и наименование специальности «6М030300-Правоохранительная деятельность»

Диссертация/проект на соискание степени магистр юридических наук (для научной и педагогической магистратуры) по специальности 6М030300 «Правоохранительная деятельность».

Научный руководитель:
Доцент кафедры
уголовного права и криминологии
подполковник полиции,
к.ю.н., Кощегулов Б.Б.

Караганда 2020

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИТ – информационные технологии
г. – год
п. – пункт
ч. – часть
ст. – статья
УК – Уголовный кодекс
РК – Республики Казахстан
ЭВМ – Электронно-вычислительная машина
СНГ - Содружество Независимых Государств
ГК – Гражданский кодекс
США – Соединенные Штаты Америки
РФ – Российская Федерация
МВД – Министерство Внутренних Дел
ООН – Организация Объединенных Наций
СССР – Союз Советских Социалистических Республик
ПК – Персональный компьютер
ЭВТ – Электронно-вычислительная техника
ЗРК – Закон Республики Казахстан
СМИ – Средства массовой информации
КНБ – Комитет национальной безопасности
ДКП – Департамент криминальной полиции
ИКТ – Информационно компьютерные технологии
ОЗУ - Оперативно запоминающее устройство
KZ-CERT - Казахстанская Служба реагирования на компьютерные инциденты
РГП – Республиканское государственное предприятие
ПХВ – Право хозяйственного ведения

# ВВЕДЕНИЕ

Защита национальных интересов Республики Казахстан в информационной сфере от угроз внешнего и внутреннего характера составляют основное содержание деятельности по обеспечению информационной безопасности Республики Казахстан

В последние годы проблема преступности в сфере информатизации и связи приобрела особую остроту и актуальность. Эта проблема, заявившая о себе в развитых странах Запада во второй половине 60-х годов, а в нашей стране – на рубеже 70 – 80-х годов XX века, в настоящее время все больше проявляет тенденцию к росту, распространенности и повышенной опасности. К причинам возникновения преступности в сфере информатизации и связи можно отнести, информационно-технологическое переоборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных; а также реальную возможность получения значительной экономической выгоды от противоправных деяний с использованием компьютерных технологий.

Елбасы Республики Казахстан Нурсултан Абишевич Назарбаев в своем Послании «Казахстанский путь - 2050: единая цель, единые интересы, единое будущее» говорил об укреплении информационной безопасности, обращая особое внимание на информационную безопасность, которая является одним из главных элементов Стратегии развития нашей страны до 2050 года и одной из актуальных проблем современного общества[1].

В своем Послании народу Казахстана «Третья модернизация Казахстана: глобальная конкурентоспособность» от 31 января 2017 г. Елбасы Республики Казахстан Н.Назарбаев отметил что «все большую актуальность приобретает борьба с киберпреступностью. Поручаю Правительству и Комитету национальной безопасности принять меры по созданию системы «Киберщит Казахстана» [2].

В связи с этим была принята Концепция кибербезопасности «Киберщит Казахстана» утвержденная постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407[3], которая определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.

В соответствии с рассуждениями о развитии обеспечения информационной безопасности, указанными в упомянутой Концепции, технологическая эволюция становится источником принципиально новых угроз, предоставляя недоступные ранее возможности негативного влияния на личность, общество и государство.

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. Первоначально общение (обмен

сведениями) осуществлялось жестами, знаками, мимикой и нечленораздельными звуками, затем появились человеческая речь, письменность, книгопечатание. В XX столетии получили развитие такие средства коммуникации, как телеграф, телефон, радио, кино, телевидение, компьютер. Параллельно проходил и иной процесс: по мере появления различных достижений науки и техники многие из них принимались на вооружение преступного мира. Однако внедрение во все сферы деятельности компьютерной техники сыграло наиболее существенную роль в деле технического вооружения преступности. «Невидимость» компьютерного преступника и одновременно «удлинение его рук» путем доступа к любым охраняемым секретам – военным, финансовым, иным – делают компьютерную технику весьма привлекательной для представителей преступного мира.

Опасность подобного рода деяний определяется еще и тем, что компьютер постепенно во всем мире заполняет все сферы жизнедеятельности человека, что позволяет преступникам значительно расширить свою экспансию. Спектр преступного использования компьютеров практически равен спектру его применения по прямому назначению, а это означает, что преступное вторжение через компьютерные сети может быть произведено в сферу космической и оборонной индустрии, политики и международных отношений и т.п..

Теория и практика не выработали единого определения компьютерных уголовных правонарушений. Объясняется это, в первую очередь, различием отечественного и зарубежного законодательства о уголовных правонарушениях в сфере информатизации и связи. В соответствии с действующим уголовным законодательством Республики Казахстан под уголовными правонарушениями в сфере информатизации и связи понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

В последние годы с ростом ИТ-технологий резко выросло количество уголовных правонарушений, связанных с хищением безналичных и даже наличных средств. Ущерб от уголовных правонарушений в сфере информатизации и связи и во всем мире за прошлый год составил $113 млрд. При этом средний ущерб на душу потерпевшего составил $87.

С 2008-2019 гг. в Казахстане было зафиксировано 874 уголовных правонарушений в сфере информатизации и связи.

С переходом на интернет-рельсы оплаты покупок и сервисов, в геометрической прогрессией растет и количество уголовных правонарушений в сфере информатизации и связи. По данным Генпрокуратуры республики Казахстан, в этом году количество правонарушений в ИТ-сфере выросло на 25%[4].

Как показывает практика, квалификация уголовных правонарушений, совершаемых в сфере в сфере информатизации и связи, представляет определенные трудности. Особенно при оценке неправомерного доступа к компьютерной информации как самого распространенного общественно опасного деяния в рассматриваемой сфере. Указанные обстоятельства и обусловливают актуальность выбранной темы диссертационного исследования.

Уголовные правонарушения в сфере информатизации и связи представляют собой проблему, которая в науке отечественного уголовного права представляется довольно плохо изученной. Причиной этого, несомненно, является относительно небольшая доля уголовных правонарушении в сфере информатизации и связи в структуре преступности, а также слабое внимание законодателя к нормам об уголовной ответственности за совершение уголовных правонарушении в сфере информатизации и связи.

Степень научной разработанности темы исследования. Проблеме уголовных правонарушений в сфере информатизации и связи уделено значительное внимание в юридической литературе такими учеными, как Ж.К. Аманов, Ю.М. Батурин, И.Ш. Борчашвили, В.Б. Вехов, М.Ю. Дворецкий, Д.В. Добровольский, А.М. Жодзишский, С.В. Кисилев, В.В. Крылов, Ю.И. Ляпунов, С.В. Максимов, Р.А. Назмышев, А.Т. Нугманова, Е.Т. Оспанов, Н.С. Полевой, В.Ю. Рогозин, Е.Р. Россинская, Н.А. Селиванов, Т.Г. Смирнова, С.Г. Спирина, А.В. Сырбу, Б.Х. Толеубекова, А.И. Усов.

**Объектом данного исследования** является совокупность общественных отношений, связанных с привлечением виновного лица к уголовной ответственности за совершение уголовных правонарушений в сфере информатизации и связи.

Предметом же выступают нормы уголовного законодательства как Казахстана, так и зарубежных стран, статистические и справочные материалы, материалы судебной практики, учебная и научная литература.

**Целью данного исследования** является комплексный анализ системы уголовных правонарушении в сфере информатизации и связи по Уголовному кодексу Республики Казахстан.

**К задачам данного исследования** можно отнести:

- рассмотрение истории развития законодательства Казахстана об уголовной ответственности за уголовные правонарушения в сфере информатизации и связи;
- анализ норм уголовного законодательства зарубежных стран об уголовной ответственности за совершение уголовных правонарушении в сфере информатизации и связи;
- общая характеристика уголовных правонарушении в сфере информатизации и связи, предусмотренных УК РК (ст. 205-213), а также анализ отдельных признаков составов данных уголовных правонарушении.

**Основные положения, выносимые на защиту.**

1. На основе анализа существующих точек зрения ученых-юристов автор дает определения понятия уголовных правонарушений в сфере информатизации и связи, под которым следует понимать запрещенное уголовным законом умышленное деяние, причиняющее вред общественным отношениям в сфере информатизации и связи, безопасности компьютерных систем или создающее угрозу причинения такого вреда.

1.1. Под безопасностью компьютерных систем предлагается понимать совокупность общественных отношений, обеспечивающих правомерное использование компьютерных технологий и компьютерной информации.

1.2. Уголовные правонарушения, совершаемые с использованием компьютерных технологий, понимается как совокупность общественно - опасных деяний, характеризующейся особым объектом - безопасностью информационных систем. Выделение этого объекта обусловлено требованиями объективной действительности и его особенностями.

2. Автор раскрывает понятие «компьютерная система» как неотъемлемого признака уголовных правонарушений в сфере информатизации и связи, совершаемых с использованием компьютерных технологий. Компьютерная система определяется как совокупность компьютерных технологий и содержащейся в них компьютерной информации.

3. Основываясь на результатах анализа статистических данных, судебной практики, а также специализированной литературы, автор выделяет основные детерминанты преступности в сфере информатизации и связи: 1) ненадлежащее отношение к вопросу обеспечения информационной безопасности; 2) низкий уровень программно-технических средств защиты информации; 3) небрежность в обеспечении конфиденциальности информации; 4) низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности.

4. Назрела необходимость принятия Пленумом Верховного Суда Республики Казахстан нормативного постановления, в котором будут разъяснены вопросы касающиеся уголовной ответственности за совершение уголовных правонарушений в сфере информатизации и связи.

**Методологическую основу данного исследования** составляют как общенаучные (анализ, синтез, индукция, дедукция, классификация и т.д.), так и частнонаучные (формально-юридический, исторический, системный и т.д.) методы юридического исследования. Особое внимание уделено использованию метода сравнительного правоведения, который предполагает сопоставление норм недействующего законодательства с нормами действующего законодательства или сравнение норм законодательства разных стран с целью выявления недостатков и достоинств тех или иных правовых норм.

**Теоретическая и практическая значимость** работы проявляются в том, что имеющиеся в диссертации выводы и положения могут быть использованы при совершенствовании действующего уголовного законодательства и других нормативных актов в сфере информатизации и связи, а также при разработке учебных программ, отдельных тем и вопросов по различным предметам, касающимся темы исследования, так и в правоприменительной деятельности судебно-следственных органов.

**Структура и объем диссертации** отвечают основной цели и предмету исследования. Работа состоит из введения, трех разделов, включающие восемь подразделов, заключения, списка использованной литературы, оформленных в соответствии с требованиями предъявляемые к данному виду работ

# 1 СОЦИАЛЬНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА УГОЛОВНЫХ ПРАВОНАРУШЕНИИ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

## 1.1 История развития законодательства об уголовной ответственности за уголовные правонарушения в сфере информатизации и связи

Защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать: целостность данных — защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных; конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Развитие государства и общества как политико-правовых явлений осуществляется всегда в четко определенных исторических и территориальных факторах, которые обусловливают это развитие. При этом угрозы для государства, общества и человека также находятся в постоянном изменении, адекватном развитию общества и государства. Современные мировые тенденции сегодня сигнализируют о возникновении новых форматов угроз для национальной безопасности Казахстана в XXI в. Во многом катализатором этих процессов стала стремительная рецессия в мировой финансово-экономической системе, начавшаяся в 2008 г. Претерпевающая серьезные потрясения западная модель финансово-экономической системы показывает, что меркантилизм, сконцентрированный на погоне за безграничной прибылью и не имеющий в своей основе гуманистических ценностей, является тупиковым. На этом фоне большому испытанию на прочность подвергаются западные ценности глобализма, либерализма, мультикультурализма, космополитизма и др. То, что мировое сообщество, в какой-то мере по инерции, продолжает с оглядкой смотреть на Запад, в надежде получить какие-то новые рецепты решения этих проблем, свидетельствует о неполном осознании растущего кризисного содержания современного мирового порядка. В то же время индикаторов, указывающих на это, очень много. Мультикультурализм в Европе перешел границу критической отметки невозврата, и норвежские теракты это доказали. По социологическим замерам, проведенным в Германии еще в 2010 г., стало ясно, что наметились тенденции роста радикального национализма и,

возможно, фашизма. Безграничные свободы либерализма сегодня привели к крепчающему социальному разложению в Европе. Свобода употребления наркотических веществ в Нидерландах, процветание однополых браков во многих странах Европы, распространение порнографической и поп-культуры снижают социальный капитал, потребительская культура, затягивающая молодое поколение в долговые кабальные условия, и многие другие социокультурные проблемы сегодня говорят о серьезном системном кризисе западных ценностей. Таким образом, финансово-экономический кризис является производной от духовного кризиса, который стал сегодня очевидным. В условиях, когда процессы глобализации показали, что современные ценности не имеют будущего, а на замену им еще не придумано ничего нового и более универсального, то в перспективе следует ожидать в мировом масштабе массового возврата к духовным, культурно-цивилизационным истокам, которые в условиях идеологической опустошенности, скорее всего, станут единственной точкой опоры. Культурно-цивилизационный ренессанс уже сегодня закладывает новый формат международных отношений. И если ранее человечество прошло эпохи геополитики и геоэкономики, то в новых условиях огромную роль уже будет играть геокультура. Формирование нового мирового порядка, скорее всего, будет сопровождаться стремительным ростом поисков идентичности. В этом отношении возрастающие национальные и религиозные идентичности станут важными факторами, вокруг которых будут формироваться геокультурные механизмы и технологии[5, с. 35].

Соответственно безопасность в целом, и информационная безопасность в частности, призвана, в первую очередь, обеспечить состояние защищенности национальной идентичности, которая выражается, как правило, в культурных ценностях, определяющих систему социальных взаимосвязей в том или ином обществе.

Человечеству потребовалось немало времени, чтобы от первых, примитивных счетных устройств XVII века перейти к использованию сверхбыстродействующих, с огромным объемом памяти (по нынешним меркам) электронно-вычислительных машин (ЭВМ), способных собирать, хранить, перерабатывать, передавать и выдавать любую информацию. Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини - и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными. Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным

мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты[6, с. 87].

Адекватными должны быть и меры по предотвращению таких последствий. Эффективно противостоять информационным угрозам в современных условиях может лишь хорошо организованная государственная система обеспечения информационной безопасности, которая должна осуществляться при полном взаимодействии всех государственных органов, негосударственных структур и граждан Республики Казахстан[7].

Одним из основных приоритетных задач в программе «Казахстан - 2030» были названы укрепление национальной безопасности, одной из составляющих которой является информационная безопасность, и борьба с преступностью[8].

Защита национальных интересов Республики Казахстан в информационной сфере от угроз внешнего и внутреннего характера составляют основное содержание деятельности по обеспечению информационной безопасности Республики Казахстан[9, с. 78].

В свое время XIX век назвали веком производства, XX - веком управления, а XXI век по праву именуется веком информации. Сегодня все являются очевидцами повышения значимости информации как для личности, так для государства и общества в целом. Возрастание роли информации практически во всех сферах жизнедеятельности обусловлено многими факторами и прежде всего - формированием информационного сектора экономики, равного по значимости, а порой превосходящего по ресурсному потенциалу такие традиционные ее подразделения, как промышленность, сельское хозяйство и услуги. Экономисты рассматривают информацию как товар, объект рыночных отношений, а юристы решают вопрос о правовом обеспечении информационной безопасности.

В этой связи в Республике Казахстан были приняты ряд правовых, организационных и практических мер, которые реализуются государственными органами Республики Казахстан. Кроме того, был принят комплекс законодательных мер, направленных на дальнейшее совершенствование уголовного, уголовно-процессуального и иных законодательств, приводящих их в соответствие с международно-правовыми стандартами, в том числе и в вопросах информационной безопасности[10, с. 112].

К международным договорам в сфере информационной безопасности относятся: Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности одобренной Постановлением Правительства Республики Казахстан от 28 мая 2012 г. № 692; Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности одобренное постановлением Правительства

Республики Казахстан от 12 июня 2009 г. № 902, Соглашение между Правительством Республики Казахстан и Правительством Республики Беларусь о сотрудничестве в области защиты информации, утвержденное постановление Правительства Республики Казахстан от 6 января 2006 г. N 10, Соглашение между Правительством Республики Казахстан и Правительством Российской Федерации о взаимной защите секретной информации, утвержденное постановлением Правительства Республики Казахстан от 9 сентября 2004 г. № 947 и т.д.[11, 12, 13, 14].

Правовой основой обеспечения информационной безопасности выступает, прежде всего, Конституция Республики Казахстан от 30 августа 1995 г. В ней закреплена обязанность государственных органов, общественных объединений, должностных лиц и средств массовой информации обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации. В Конституции Республики Казахстан указывается, что каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом[15].

Отношения в сфере информационной безопасности регулируется и такими кодифицированными нормативными актами как Гражданский кодекс Республики Казахстан, Гражданский кодекс Республики Казахстан (Особенная часть), Трудовой кодекс Республики Казахстан, кодекс Республики Казахстан об административных правонарушениях, Уголовный кодекс Республики Казахстан, кодекс Республики Казахстан о таможенном регулировании в Республике Казахстан [16, 17, 18, 19, 20].

В Гражданском кодексе Республики Казахстан содержаться нормы, касающиеся служебной и коммерческой тайны, электронной цифровой подписи. В гражданском кодексе Республики Казахстан (Особенная часть) закрепляется такой вид услуг как информационные.

Уголовный кодекс Республики Казахстан 2014 г. выделил следующее преступное деяние в сфере информационной безопасности, которые были собраны в главе 7 «Уголовные правонарушения в сфере информатизации и связи» - «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций» ст. 205 УК РК, «Неправомерные уничтожение или модификация информации» ст. 206 УК РК, «Нарушение работы информационной системы или сетей телекоммуникаций» ст. 207 УК РК, «Неправомерное завладение информацией» ст. 208 УК РК, «Принуждение к передаче информации» ст. 209 УК РК, «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» ст. 210 УК РК, «Неправомерное распространение электронных информационных ресурсов ограниченного доступа» ст. 211 УК РК, «Предоставление услуг для размещения интернет-ресурсов, преследующих

противоправные цели» ст. 212 УК РК, «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства» ст. 213 УК РК.

В Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V содержатся такие составы правонарушений в данной сфере как ст. 636 «Незаконное подключение оконечных устройств (оборудования) к сетям электросвязи», ст. 637 «Нарушение законодательства Республики Казахстан в области связи», ст. 638 «Использование средств связи, подлежащих обязательному подтверждению соответствия, но не прошедших его», ст. 639 «Нарушение требований по эксплуатации средств защиты электронных информационных ресурсов», ст. 640 «Нарушение законодательства Республики Казахстан об электронном документе и электронной цифровой подписи», ст. 641 «Нарушение законодательства Республики Казахстан об информатизации» которые собраны в главе 31 «Административные правонарушения в сфере информатизации и связи».

В Трудовом кодексе Республики Казахстан 2015г. определяется, что гражданский служащий не вправе использовать в неслужебных целях средства материально-технического, финансового и информационного обеспечения, другое государственное имущество и служебную информацию. В данном кодексе содержится также норма о том, что работник обязан не разглашать сведений, составляющих государственные секреты, служебную, коммерческую или иную охраняемую законом тайну, ставших ему известными в связи с выполнением трудовых обязанностей.

Кодекс Республики Казахстан от 26 декабря 2017 года № 123-VI «О таможенном регулировании в Республике Казахстан» содержит в себе целую главу 49, посвященную «Информационным системам и информационно-коммуникационным технологиям, используемые таможенными органами» которая включает в себя ст. 438 «Информационные системы и информационно-коммуникационные технологии, используемые таможенными органами», ст. 439 «Программные продукты, находящиеся в собственности декларантов и лиц, осуществляющих деятельность в сфере таможенного дела», ст. 440 «Информационные ресурсы таможенных органов», ст. 441 «Защита информации и прав лиц, участвующих в информационных процессах и информатизации».

Правовую базу обеспечения информационной безопасности составляют также следующие законы Республики Казахстан: от 10 июня 1996 г. № 6 «Об авторском праве и смежных правах», от 15 марта 1999 г. N 349-1 «О государственных секретах», от 23 июля 1999 г. № 451-I «О средствах массовой информации», от 7 января 2003 г. N 370 «Об электронном документе и электронной цифровой подписи», от 5 июля 2004 года «О

связи», от 9 ноября 2004 года № 603-II «О техническом регулировании», от 11 января 2007 г. № 217 «Об информатизации», от 6 января 2012 г. № 527-IV «О национальной безопасности Республики Казахстан», от 16 мая 2014 года № 202-V «О разрешениях и уведомлениях», от 16 ноября 2015 года № 401-V «О доступе к информации», от 24 ноября 2015 года № 418-V «Об информатизации» и т.д.

Особое место призван занять закон Республики Казахстан от 10 июля 2009 г. № 178-IV «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей»[21].

Данный закон сокращенно именуют «Законом о регулировании Интернета». Изменения коснулись всего пятнадцати законов. Интернет-ресурсы приравнены к средству массовой информации со всеми вытекающими последствиями об ограничении на распространении запрещенной законом информации и возможных неприятных последствиях для нарушителей. Решение о наложении санкций, в том числе крайних - о приостановлении или о прекращении выпуска средства массовой информации - вправе принимать только суд.

Особое место в обеспечении информационной безопасности Республики Казахстан являются Концепции информационной безопасности Республики Казахстан. Первая «Концепция информационной безопасности Республики Казахстан» была принята указом Президента Республики Казахстан от 10 октября 2006 года № 199[22], вторая «Концепция информационной безопасности Республики Казахстан до 2016 года» была принята указом Президента Республики Казахстан от 14 ноября 2011 г. N 174[23], третья «Концепция «Киберщит Казахстана» принята постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407[3], данные концепции определяют государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности.

Концепция выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативных правовых актов, регулирующих данную сферу.

Концепция основана на оценке текущей ситуации в Республики Казахстан и определяет государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности.

При разработке Концепции также был учтен имеющийся международный опыт в области обеспечения информационной безопасности, в частности США, Великобритании, Канады, Российской Федерации, Индии, Эстонии. В Концепции выдержан соответствующий международному опыту комплексный подход к реализации вопросов обеспечения информационной безопасности, включающий законодательное, нормативно-методическое, организационное, технологическое и кадровое обеспечение.

Концепция выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативных правовых актов, регулирующих данную сферу[3].

Структура правового регулирования отношений в области информационной безопасности акцентирует внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности.

В законодательстве об информационной безопасности можно выделить три основных направлений правовой защиты объектов в информационной сфере:

- защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации;

- защита информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и

телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц;

- защита информационных прав и свобод (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; право собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в условиях информатизации.

Нормы информационного права не всегда находятся в нормативных актах, которые с известной степенью условности можно отнести к так называемому информационному законодательству. Они разбросаны по многочисленным правовым актам, регулирующим такие отрасли, как конституционное, гражданское, административное, финансовое и уголовное право. Это еще раз подтверждает тот факт, что регламентация правил поведения в связи с деятельностью по информации является необходимой практически во всех сферах жизни человека[10, с. 113].

Основным средством борьбы с преступными нарушениями нормального функционирования компьютерной техники должно стать уголовное законодательство[24, с. 42].

В уголовном кодексе Республики Казахстан 2014г. ориентируясь на сходные представления об объекте уголовно-правовой охраны, объединили компьютерные посягательства в одну из глав «Уголовные правонарушения в сфере информатизации и связи», где нашли место почти все деяния, вмешательству в работу компьютера[20].

Подводя итог вышесказанному в Республике Казахстан основным политико-правовым актом, определяющим принципы и основные направления развития информационной безопасности, является Концепция кибербезопасности «Киберщит Казахстана» от 30 июня 2017 года.

Концепция кибербезопасности «Киберщит Казахстана» разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира, в которых обеспечение информационной безопасности как составляющей национальной безопасности определено одним из основных долгосрочных приоритетов. Концепция основана на оценке текущей ситуации и определяет государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности. Концепция разработана в соответствии с Конституцией Республики Казахстан, Уголовным кодексом Республики Казахстан, Кодексом Республики Казахстан Об административных правонарушениях, Предпринимательским кодексом Республики Казахстан и Законами Республики Казахстан «Об оперативно-розыскной деятельности», «О банках и банковской деятельности в Республике Казахстан», «Об электронном документе и электронной

цифровой подписи», «О связи», «Об образовании», «О науке», «О национальной безопасности Республики Казахстан», «О персональных данных и их защите», «О гражданской защите», «О разрешениях и уведомлениях», «Об информатизации», «О государственных закупках».

При разработке Концепции учитывался имеющийся международный опыт в области обеспечения информационной безопасности, в частности, США, Великобритании, Канады, Российской Федерации, Индии, Эстонии. В Концепции выдержан соответствующий международному опыту комплексный подход к реализации вопросов обеспечения информационной безопасности, включающий законодательное, нормативно-методическое, организационное, технологическое и кадровое обеспечение. В положения Концепции включены основные направления Концепции сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, подписанной в г. Бишкеке 10 октября 2008 г., Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, ратифицированного Законом Республики Казахстан от 1 июня 2010 г. «О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности».

В настоящее время в Казахстане приняты законы об охране правоотношений в сфере информатизации и связи, которые в целом соответствуют международным требованиям. При этом основная задача состоит во внедрении в настоящее время существующих законодательных актов, поскольку, несмотря на принятие целого блока отвечающих современным требованиям законов, в нашей стране наблюдается значительный рост уголовных правонарушений в сфере информатизации и связи

## 1.2 Понятие и виды уголовных правонарушений в сфере информатизации и связи.

Защита информации в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать: целостность данных — защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных; конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

По мере осознания большинством населения страны роли информационных правоотношений в жизни общества в целом, произошли в различных отраслях права позитивные сдвиги в области придания самостоятельного статуса нормам, охраняющим указанный вид правоотношений в соответствующих законодательных актах республики.

В Казахстане вопрос о законодательном закреплении компьютерных преступлений в качестве самостоятельного уголовно-наказуемого деяния впервые был поставлен при подготовке проекта Уголовного кодекса в конце 1995 г. и закреплен в новом уголовном законодательстве, принятом 16 июля 1997 г. в ст. 227 «Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ».

Уголовный кодекс Республики Казахстан от 3 июля 2014 года посвятил целую главу 7 «Уголовные правонарушения в сфере информатизации и связи», предусмотрев в ней 9 статей.

Необходимость закрепления данной главы в УК РК продиктована развитием технического прогресса, широким использованием компьютерной техники и возможностью появления новых криминализированных проявлений, посягающих на законные правоотношения в сфере обращения и использования компьютерной информации.

Анализ ряда научной и специальной литературы показывает, что компьютерные преступления в современных условиях имеют тенденции к росту. Проблема преступности как негативного социального явления в последнее время приобрела международную значимость.

Так, если в период с 1980 по 1984 гг., компьютерными преступлениями в США в целом нанесен ущерб в 5 млн. долларов, то в 1995 г. по одному только делу хакера В. Левина ущерб, нанесенный «Ситибанку», составил около 10 млн. долларов. А уже на начало нового столетия около 10 млрд. долларов.

В январе 1995 г. ГСУ МВД Республики Казахстан было закончено расследование уголовного дела о попытке хищения 6 млн. тенге путем использования компьютерной техники операторами Алатауского филиала Крамдсбанка и ВЦ Нацбанка РК [25].

XXI в. — век стремительного прогресса информационных технологий. Так, в 2003 г. на Интернет-экономику в мире уже приходилось около 5 % валового продукта. По данным специалистов в 2012г. число пользователей интернета составляло 2,08 млрд. человек, а в 2019 их уже составило 4,39

млрд. пользователей подключенных к сети Интернет, где на данный момент размещено несколько миллионов сайтов и изображений. Объем передаваемых данных через Интернет удваивается, что, на наш взгляд, указывает на появление реальной зависимости развитых стран мира от международной информационной инфраструктуры. Несомненно, это затронуло и Казахстан.

Однако на сегодняшний день Интернет выступает не только как кладезь информации, но и как угроза в виде информационных войн и компьютерной преступности. При этом выделяется пять основных направлений правового регулирования Интернет-отношений:

1) защита личных данных и частной жизни в сети Интернет;

2) регулирование электронной коммерции и иных сделок и обеспечение их безопасности;

3) защита интеллектуальной собственности;

4) борьба против противоправного содержания информации и противоправного поведения в сети;

5) правовое регулирование электронных сообщений.

Для того чтобы сформулировать понятие компьютерной преступности необходимо дать определение понятию компьютерного преступления.

Первое научное обсуждение компьютерной преступности было осуществлено в 1993 г. на семинаре «Криминалистика и компьютерная преступность» научно-исследовательского института проблем укрепления законности и правопорядка Генеральной прокуратуры РФ и ЭКЦ МВД России, где под компьютерными преступлениями стали понимать «предусмотренные законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства»[26, с. 37]. При этом указанное понятие не содержало упоминания о виновном характере посягательств, а также последствий или на возможности их наступления в результате совершения общественно опасного деяния.

В юридической литературе на данный счет мнения ученых были разделены.

Так, по мнению В.Б. Вехова, «под компьютерными преступлениями нужно понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства» [27, с. 23].

А.К. Караханьян считает, что к компьютерным преступлениям относится «внесение изменений в информацию на различных этапах ее обработки в программное обеспечение, а также овладение информацией» [28, с. 244].

К.С. Скоромников, говоря о частом использовании термина «компьютерные преступления» в правоприменительной практике в отношении общественно опасных деяний с применением средств

вычислительной техники и об отсутствии данного термина в уголовном законодательстве, предлагает ввести его в официальную судебную статистику как условное наименование компьютерных преступлений [29, с. 168]. Мы не согласны с таким предложением, так как в рассматриваемой сфере появляются новые деяния, которые осуществляются не только посредством ЭВМ, системы ЭВМ или их сети, но и с помощью телекоммуникационного оборудования.

При этом в уголовно-правовой литературе существовало две позиции, это когда одни ученые предлагали именовать рассматриваемые деяния компьютерными преступлениями, другие — преступлениями в сфере компьютерной информации.

Например, С.В.Бородин рассматривает преступления в сфере компьютерной информации как общественно опасные деяния, которые «конкретно направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации» [30, с. 662]. При этом он не указывает на последствия, на форму вины рассматриваемых преступлений, а объектом выступают интересы личности, общества, государства, охраняемые уголовным законом в области безопасности изготовления, использования и распространения компьютерной информации, информационных ресурсов, систем и технологий.

Т.Г. Смирнова рассматривает преступления в сфере компьютерной информации как «запрещенные уголовным законом общественно опасные деяния, которые, будучи направленными на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей, причиняют либо сохраняют угрозу причинения вреда жизни и здоровью личности, права и свободам человека и гражданина, государственной и общественной безопасности» [31, с. 14].

При этом необходимо делать различия между машинной информацией, то есть информацией, являющейся продуктом, произведенным с помощью или для компьютерной техники (например, программа для управления устройствами ЭВМ) и информацией, имеющей «некомпьютерный» характер (например, электронный документ) [32, с. 17].

Под машинной информацией понимается информация, циркулирующая в вычислительной среде, зафиксированная на физическом носителе в форме, доступной восприятию ЭВМ, или передающаяся по телекоммуникационным каналам, сформированная в вычислительной среде и пересылаемая посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство либо на управляющий датчик оборудования.

Также необходимо учитывать, что компьютер в преступлениях может выступать как предметом, так и орудием совершения преступления. Данное свойство определяется технологической спецификой его строения.

На X Конгрессе ООН по предупреждению преступности и обращению с правонарушителями, компьютерные преступления были подразделены на две категории:

1) любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных (в узком смысле);

2) любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей (в широком смысле, как преступление, связанное с компьютерами).

В США используются, например, такие понятия как «High tech crime» или «Cyber crime», означающие «преступления в сфере высоких технологий» и «киберпреступления». В действующем уголовном законодательстве Республики Казахстан данный вид преступных деяний определен как преступления в сфере компьютерной информации. На наш взгляд, указанное название не дает возможности четко определить конкретный вид преступлений, что приводит к неоднозначности, потому что необходимо учитывать тот факт, что компьютеры используются практически во всех сферах жизнедеятельности общества и являются лишь одной из разновидностей информационного оборудования. Поэтому, по нашему мнению, целесообразно обозначить данные преступления как преступления, совершенные в сфере информационных технологий — предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы ЭВМ, системы ЭВМ или их сети, причиняющие вред законным интересам собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина, национальной безопасности, где предметом выступает компьютерная информация.

В СССР первые компьютерные преступления были зафиксированы в 1979 г. в г. Вильнюсе и в 1982г. в г. Горьком. Появление первых компьютерных преступлений в начале 80-х годов прошлого столетия было обусловлено переходом на автоматизированные системы документооборота. Этот переход и создал благоприятные условия для возникновения и роста компьютерной преступности. Первые хищения посредством незаконной манипуляции с компьютерной информацией совершались во время перехода отделений связи СССР на новую централизованную автоматическую систему обработки (получения и отправки) денежных переводов клиентов, функционирующую на базе компьютерного комплекса «Онега». Вместе с этой системой применялся обычный ручной способ приема и отправления

платежей. Параллельное использование автоматизированных и неавтоматизированных операций с денежными средствами и позволило преступникам совершать хищения [27, с. 70-71].

Автоматизация банковской деятельности определила качественно новый этап роста компьютерной преступности. Так, в 1991 г. сотрудником вычислительного центра Внешэкономбанка было совершено хищение в крупном размере (125,5 тысяч долларов США). В начале 90-х годов (1991-1997 гг.) в процессе становления банковской системы страны отмечалась большая активность со стороны компьютерных преступников. Только в 1995 г. ущерб от компьютерных преступлений в сфере экономики составил 250 млрд. руб. [33, с. 89].

Это было обусловлено рядом причин.

Во-первых, большинство организаций не принимало достаточных мер по обеспечению безопасности ЭВМ, а также систем и их сетей. Это было вызвано нежеланием дополнительных материальных затрат.

Во-вторых, в этот период времени советское уголовное законодательство не предусматривало уголовной ответственности за компьютерные преступления.

В-третьих, в правоохранительных органах не было специальных подразделений, осуществляющих борьбу с компьютерной преступностью, не хватало квалифицированных специалистов.

В результате с 1 января 1997 г. в уголовное законодательство была введена уголовная ответственность за преступления в сфере компьютерной информации, а для осуществления борьбы с данными видами преступлений в правоохранительных органах созданы специальные подразделения.

В настоящее время данный вид преступной деятельности является и остается, если можно так выразиться, одним из самых «молодых», в ее выделение из всей структуры преступности позволяет детально изучить ее особенности, специфику, и при этом выработать дифференцированные меры борьбы с ней.

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название «компьютерная преступность». Поэтому, что на сегодняшний день остается неясным, что следует понимать под компьютерной преступностью.

Так, в юридическом словаре преступность означает «совокупность всех фактически совершенных противоправных деяний, массовое негативное социально-правовое явление, обладающее определенными закономерностями, количественными и качественными характеристиками» [34, с. 368].

Понятие «преступность» употребляется в тех случаях, когда речь идет о множестве преступлений, об их определенной статистической совокупности. Признавая структурный характер преступности, практически все криминологи выделяют отдельные ее составляющие. В юридической

литературе структура преступности определяется как «удельный вес и соотношение различных видов преступлений в общем их числе за определенный период времени на определенной территории» [35, с. 156].

Таким образом, сформулировав определение понятия преступлений в сфере информационных технологий, представляется возможным определить термин «компьютерная преступность», где подразумевается совокупность преступлений в сфере компьютерной информации и опосредованных общественно опасных деяний. Сосуществование этих общественно опасных деяний способно причинить значительный вред интересам личности, общества и государства, они посягают на безопасность компьютерной информации.

Подпадая под определение преступности вообще, компьютерная преступность является профессиональной по следующим признакам:

1. Наличие у преступника определенных познаний и навыков во владении компьютерной техникой.

2. Устойчивый вид преступного занятия.

3. Совершение данного вида преступления — как источник средств существования или получения выгоды.

4. Наличие устойчивых связей с антисоциальной средой.

5. Совокупность профессиональных преступников — что свидетельствует о масштабности преступной деятельности в сфере информационных технологий.

Таким образом, компьютерная преступность представляет собой естественный и необходимый результат эволюции общества, основанный на информационных технологиях, выступает как дополнительная комфортная форма жизнедеятельности, не поддающаяся ликвидации либо преодолению и требующая адекватных способов и методов регулирования и управления в целях минимизации причиняемого вреда интересам личности, общества и государства, обладающее признаками профессиональной преступности и представляющее собой виновное нарушение уголовно-правовых запретов и совокупность всех фактически совершенных преступлений в сфере информационных технологий.

На наш взгляд, к компьютерной преступности примыкают и некоторые действия, направленные на поддержание условий для ее существования и развития (например, создание сайтов, направленных на распространение криминальной идеологии, а также обмен криминальным опытом и специальными познаниями). В сети Интернет насчитывается более 30 тысяч ориентированных на взлом сайтов, где любое лицо может приобрести за небольшую сумму книгу, обучающую элементарным приемам атаки на информационные системы [36].

По нашему мнению, следует различать компьютерную преступность как правовую категорию и компьютерную преступность как социальное явление, которое включает в себя не только совокупность всех

компьютерных преступлений, но и различные формы тесто связанной с ними организационной деятельности.

При этом компьютерные преступления условно можно подразделить на две большие категории — преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

Несанкционированный доступ к информации, хранящейся в компьютере, который 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 людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая на удачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может неспеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению «брешей».

Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что некто 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 приема. Самый простейший путь его осуществления — получить коды и другие идентифицирующие шифры законных пользователей.

Это может делаться:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;
– 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 получить некоторую информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособлений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа — мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ может осуществляться в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к непринадлежащим ему частям банка данных. Все происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

«Временная бомба» — разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени.

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

С помощью «троянского коня» преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность «троянского коня». Ее особенность состоит в том, что в безобидно выглядящей кусок программы вставляются не команды, собственно, выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т. д. (сколь угодно большое число раз), создающие «троянского коня».

В США получила распространение форма компьютерного вандализма, при которой «троянский конь» разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась «временная бомба», которая «взрывается» в самый неожиданный момент, разрушая всю библиотеку данных. При этом не следует думать, что «логические бомбы» — это экзотика, несвойственная нашему обществу.

Разработка и распространение компьютерных вирусов.

«Троянский конь» типа «сотри все данные этой программы, перейди в следующую и сделай тоже самое» обладает свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер «заболевает».

Экспертами собрано досье писем от шантажистов, требующих перечисления крупных сумм денег в одно из отделений американской фирмы «ПК Сиборг»; в случае отказа преступники грозятся вывести компьютеры из строя. По данным журнала «Business world», дискеты-вирусоносители получены десятью тысячами организаций, использующих в своей работе компьютеры. Для поиска и выявления злоумышленников созданы специальные отряды английских детективов.

По оценке специалистов в «обращении» находится более 100 типов вирусов.

Но все их можно разделить на две разновидности, обнаружение которых различно по сложности: «вульгарный вирус» и «раздробленный вирус». Программа «вульгарного вируса» написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить ее в самом начале эпидемии (размножения). Эта операция требует, однако, крайне тщательного анализа всей совокупности операционной системы ЭВМ. Программа «раздробленного вируса» разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в «распределенном» состоянии, лишь на короткое время своей работы, собираясь в единое целое. Как правило, создатели вируса указывают ему число репродукций, после достижения которого он становится агрессивным.

Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер.

Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея (так называемый «итальянский попрыгунчик»). Признаки могут быть эволютивными, и «болезнь» будет обостряться по мере своего течения. Так, по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения.

По-видимому, в будущем будут появляться принципиально новые виды вирусов. Например, можно себе представить (пока подобных сообщений не было) своего рода «троянского коня» вирусного типа в электронных цепях. В самом деле, пока речь идет только о заражении компьютеров. А почему бы — не микросхем? Ведь они становятся все более мощными и превращаются в подобие ЭВМ. И их необходимо программировать. Конечно, ничто не может непосредственно «заразить» микросхему. Но ведь можно заразить компьютер, используемый как программатор для тысячи микросхем.

Каковы способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве средства передвижения. То есть с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И

наоборот, когда «здоровая» дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения — это копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы.

Специалисты предостерегают от копирования ворованных программ. Иногда, однако, и официально поставляемые программы могут быть источником заражения.

В печати часто проводится параллель между компьютерным вирусом и вирусом «AIDS». Только упорядоченная жизнь с одним или несколькими партнерами способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражению.

Естественно, что против вирусов были приняты чрезвычайные меры, приведшие к созданию текстовых программ-антивирусов. Защитные программы подразделяются на три вида: фильтрующие (препятствующие проникновению вируса), противоинфекционные (постоянно контролирующие процессы в системе) и противовирусные (настроенные на выявление отдельных вирусов).

Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

Заметим, что пожелание ограничить использование непроверенного программного обеспечения скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные программы на «стерильных» носителях стоят немалых денег в валюте. Поэтому избежать их неконтролируемого копирования почти невозможно.

Справедливости ради следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т. п.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в

любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее «свежих». Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

Хищение компьютерной информации.

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

На основе анализа вышеперечисленных существующих точек зрения ученых-юристов мы считаем, что под уголовными правонарушениями в сфере информатизации и связи, следует понимать запрещенное уголовным законом умышленное деяние, причиняющее вред общественным отношениям в сфере информатизации и связи, безопасности компьютерных систем или создающее угрозу причинения такого вреда. Под безопасностью компьютерных систем следует считать совокупность общественных отношений, обеспечивающих правомерное использование компьютерных технологий и компьютерной информации. Уголовными правонарушениями, совершаемые с использованием компьютерных технологий, следует

понимать совокупность общественно опасных деяний, характеризующейся особым объектом - безопасностью информационных систем.

## 1.3 Уголовная ответственность за уголовные правонарушения в сфере информатизации и связи по законодательству зарубежных стран

Принятие УК РК поставило ряд проблем перед теоретиками уголовно-правовой науки: определить объект преступлений в сфере информатизации и связи, сформулировать их понятие и систему; установить критерии выделения близких по содержанию видов преступных посягательств, отграничение от других составов уголовных правонарушений; решить вопрос квалификации, а также ответственности и наказания за них. Бланкетный характер диспозиций соответствующих уголовно-правовых норм требует обращения к различным правовым актам, регулирующим возникающие правоотношения, и знания терминологии.

Анализ специальной литературы показывает, что вопросам терминологии, используемой законодателем для формулирования норм о преступлениях в сфере компьютерной информации, не было уделено надлежащего внимания, что диктует исследование зарубежного опыта борьбы с этими преступлениями[37, с. 37].

В параметрах построения миропорядка на основе верховенства права важное место занимает борьба с международной преступностью. В рамках общепризнанного понимания в национальной и зарубежной науке международного уголовного права установлено деление международных преступных деяний на международные преступления и преступления международного характера[38, с. 123; 39, с. 50-90; 40, с. 134-137].

Для эффективной борьбы с преступлениями в сфере компьютерной информации необходимо учитывать опыт борьбы других стран[41, с. 12].

По мнению многих исследователей, проблема обеспечения безопасности компьютерных информации и технологий, в том числе и уголовно-правовыми средствами, является на сегодня одной из самых актуальных в большинстве развитых стран мира[42, с. 5-28].

Уголовно-правовое регулирование зарубежным законодательством вопросов уголовной ответственности за так называемые компьютерные преступления существенно отличается друг от друга. Не во всех государствах законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием информатизации и связи.

Определенный опыт законодательного регулирования в уголовном праве вопросов ответственности за совершение преступлений в сфере

информатизации и связи накоплен государствами, входившими ранее в состав СССР и вошедших в состав Содружества Независимых Государств.

«Информационная революция» застала Россию в сложный экономический и политический период. Необходимость досрочной разработки правовых основ охраны информационных отношений, еще слабая развитость электронно-вычислительных систем, незначительное количество выявленных общественно опасных посягательств на эти отношения, отсутствие необходимого опыта привело к тому, что во вновь принятом в 1996 года Уголовном кодексе РФ в гл. 28 «Преступления в сфере компьютерной информации» содержалось три статьи, предусматривающие ответственность за «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274). Названные в ст. 272 и 274 УК РФ деяния относятся к преступлениям небольшой тяжести, а эти же преступления, совершенные при отягчающих обстоятельствах, – к преступлениям средней тяжести.

В Уголовном кодексе Республики Беларусь[43].имеется семь статей, устанавливающих ответственность за следующие деяния: несанкционированный доступ к компьютерной информации (ст. 349), модификацию компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработку, использование либо распространение вредоносных программ (ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355)[44, с. 64-74].

Таким же образом урегулированы вопросы уголовной ответственности за преступления против информационной безопасности в Уголовном кодексе Республики Таджикистан(ст. ст. 298–304)[45].

С 1 сентября 2001 года вступил в действие Уголовный кодекс Украины[46], которым установлена ответственность за ряд преступлений, родовым объектом посягательств которых согласно заглавию раздела XVI обозначена сфера использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей. В данный раздел включены: ст. 361 «Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей»[47]; ст. 362 «Хищение, присвоение, вымогательство компьютерной информации либо завладение ею путем мошенничества или злоупотребления служебным положением»; ст. 363 «Нарушение правил эксплуатации автоматических электронно-вычислительных систем».

Кроме того, в ст. 301 УК Украины, устанавливающей ответственность за ввоз, изготовление, сбыт и распространение порнографических предметов,

включен квалифицирующий признак совершения данных преступлений (ч. ч. 2 и 3): изготовление или использование компьютерных программ, что влечет за собой усиление наказания.

В конце 2004 года Верховная Рада Украины внесла изменения в Уголовный кодекс Украины относительно ответственности за преступления в сфере использования компьютеров. В частности, в новой редакции представлена ст. 361 УК Украины, в соответствии с которой уголовная ответственность будет наступать за несанкционированное вмешательство в работу ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, что привело к утечке; потере; подделке; блокированию информации; искажению процесса обработки информации; нарушению установленного порядка ее маршрутизации.

В то же время УК Украины дополняется новыми статьями, которые устанавливают уголовную ответственность за: создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт (ст. 361-1 УК Украины); несанкционированный сбыт или распространение информации с ограниченным доступом, которая хранится в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361-2 УК Украины); препятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи (ст. 363-3 УК Украины).

В новой редакции излагаются ст. ст. 362 и 363 УК Украины, которые устанавливают ответственность за: несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, содеянные лицом, которое имеет право доступа к ней (ст. 362 УК Украины); нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты информации, которая в них обрабатывается (ст. 363 УК Украины).

Уголовный кодекс Республики Узбекистан[48] предусматривает такие составы преступлений, как: хищение путем присвоения и растраты с использованием средств компьютерной техники (п. «г» ч. 3 ст. 167); мошенничество с использованием средств компьютерной техники (п. «в» ч. 3 ст. 168); кража, совершенная с несанкционированным проникновением в компьютерную систему (п. «в» ч. 3 ст. 169); нарушение правил информатизации (ст. 174); незаконное собирание, разглашение или использование информации (ст. 191); дискредитация конкурента (ст. 192).

Аналогичным образом подходит к регулированию борьбы с преступлениями в сфере компьютерной информации Уголовный кодекс

Республики Кыргызстан[49]. Кроме того, законодатель отразил особенности их совершения с использованием компьютерных информации и технологий, предусмотрев ответственность за: нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 136); аналогичное деяние, совершенное с использованием специальных технических средств, предназначенных для негласного получения информации (ч. 2 ст. 136); незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (ч. 3 ст. 136); нарушение авторских, смежных прав и прав патентообладателей путем выпуска под своим именем чужой программы для ЭВМ либо базы данных, либо иное присвоение авторства на такое произведение, а равно принуждение к соавторству (ч. 1 ст. 150); незаконное использование программы для ЭВМ или базы данных (ч. 2 ст. 150); незаконное получение сведений, составляющих коммерческую или банковскую тайну, путем перехвата информации в средствах связи, незаконного проникновения в компьютерную систему или сеть (ст. 193).

Уголовный кодекс Республики Туркменистан[50] содержит гл. 33 «Преступления в сфере компьютерной информации», в которую включены: ст. 333 «Нарушение законодательства о правовой охране алгоритмов, программ для электронных вычислительных машин (ЭВМ), баз данных и топологий интегральных микросхем»; ст. 334 «Неправомерный доступ к компьютерной информации» и ст. 335 «Создание, использование и распространение вредоносных программ для ЭВМ», положения которых аналогичны ст. 272 и ст. 273 УК РФ.

Фактически соответствуют положениям ст. ст. 272 – 274 УК РФ нормы об уголовной ответственности за преступления в сфере компьютерной информации, содержащиеся в УК Азербайджанской Республики (ст. ст. 271 – 273)[51] и УК Грузии(ст. ст. 284 – 286)[52].

Уголовным кодексом Республики Молдова, [53] принятым 18 апреля 2002 года, преступления рассматриваемого вида сгруппированы в гл. XI «Преступления в сфере информатики», например ст. 259 «Несанкционированный доступ к компьютерной информации», то есть к информации, хранящейся в компьютерах, на машинных носителях, в компьютерной системе или сети, сопряженный с уничтожением, повреждением, модификацией, блокированием или копированием информации, нарушением работы компьютеров, компьютерных систем или сетей.

Кроме того, в соответствии со ст. 260 УК Республики Молдова предусмотрена уголовная ответственность за: «внесение или распространение вредоносных компьютерных программ», которое законодатель определил как заведомое внесение в компьютерные программы вирусных модификаций либо распространение компьютерных программ или информации, выводящих из строя машинные носители информации,

технические средства обработки данных или нарушающих систему защиты. А ст. 261 УК Республики Молдова предусмотрена уголовная ответственность за нарушение ответственным лицом правил сбора, обработки, хранения, распространения, распределения информации или правил защиты информационных систем, предусмотренных в соответствии с видом информации или степенью ее защиты, если это действие способствовало хищению, искажению, уничтожению информации или повлекло иные тяжкие последствия.

В соответствии с Уголовным кодексом Республики Армения[54] (УК РА), принятом в апреле 2003 года, в гл. 24 «Преступление против безопасности компьютерной информации», размещенной в разделе 9 «Преступления против общественной безопасности, безопасности компьютерной информации, общественного порядка, общественной нравственности и здоровья населения», предусмотрено семь составов.

Так, в ст. 251 УК РА предусмотрена уголовная ответственность за несанкционированный доступ (проникновение) к системе компьютерной информации.

Кроме того, установлена уголовная ответственность за: изменение информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях, либо внесение в них ложной информации при отсутствии признаков хищения чужого имущества, либо причинение имущественного ущерба путем обмана или злоупотребления доверием, повлекшие значительный ущерб; компьютерный саботаж – уничтожение, блокирование либо приведение в негодность компьютерной информации или программы, выведение из строя компьютерного оборудования либо повреждение компьютера, компьютерной системы, сети или машинных носителей; неправомерное завладение компьютерной информацией; за изготовление в целях сбыта или сбыт специальных программных или аппаратных средств для неправомерного доступа (проникновения) к защищенной информации; за разработку, использование и распространение вредоносных программ; за нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ (право на проникновение) к компьютеру, компьютерной системе или сети, если это деяние повлекло по неосторожности уничтожение, блокирование, изменение охраняемой законом компьютерной информации, нарушение работы компьютерного оборудования либо повлекло иной значительный ущерб.

Кроме того, в разделе 8 УК РА «Преступления против собственности, экономики и экономической деятельности» предусмотрено два состава, имеющих отношение к рассматриваемой проблеме. Так, в гл. 21 УК РА «Преступления против собственности», в соответствии со ст. 181 уголовно наказуемым является: хищение чужого имущества в значительных размерах, совершенное с использованием компьютерной техники.

В гл. 22 УК РА «Преступления против экономической деятельности» предусмотрена уголовная ответственность за собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз в отношении лиц, владеющих коммерческой или банковской тайной, их близких, прослушивания средств связи, незаконного проникновения в компьютерную или программную систему или сеть, использования специальных технических средств, а также иными незаконными способами в целях разглашения или использования этих сведений (ст. 199 УК РА).

В ст. 307 гл. 28 УК РА «Преступления против основ конституционного строя и безопасности государства» раздела 11 «Преступления против государственной власти» установлена уголовная ответственность за нарушение правил обращения с документами или компьютерной информацией, содержащими государственную тайну, а также с иными предметами, содержащими сведения о государственной тайне, лицом, обязанным соблюдать эти правила, если это повлекло по неосторожности утрату этих документов, или предметов, или компьютерной информации.

Как видно, родовой объект «компьютерных преступлений» в уголовном законодательстве стран СНГ различен. Так, в соответствии с УК Азербайджана, Армении, Кыргызстана, Российской Федерации, Туркменистана, где составы преступлений охватываются главой «Преступления в сфере компьютерной информации», родовым объектом являются отношения в области компьютерной информации. Более того, уголовное законодательство стран СНГ по-разному оценивает степень общественной опасности преступлений в сфере компьютерной информации.

В Республике Беларусь и Таджикистане, где общественно опасные деяния объединены в главу «Преступления против информационной безопасности», законодатель установил в качестве родового объекта информационную безопасность, хотя преступления, посягающие на состояние защищенности жизненно важных интересов физических и юридических лиц в информационной сфере, содержатся и в других разделах и главах УК. В УК Украины родовой объект определен как отношения в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей и соответствующая глава называется «Преступления в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей».

В УК Грузии (глава «Компьютерные преступления») и Молдовы (глава «Преступления в сфере информатики») законодатель четко не определил родовой объект группы общественных отношений, подлежащих уголовно-правовой охране.

В УК Узбекистана (глава «Хищение чужого имущества») состав преступления «Нарушение правил информатизации» отнесен к преступлениям против собственности, а в УК Казахстана преступление в

соответствии со ст. 227 относится к преступлениям в сфере экономической деятельности.

Проблема борьбы с компьютерными (информационными) преступлениями в настоящее время стоит перед многими государствами.

Многие европейские государства повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества.

Так, в 1993 году в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий Уголовный кодекс[55] новыми составами: несанкционированный доступ в компьютерные сети (ст. 138a (1)); несанкционированное копирование данных (ст. 138 (2)); компьютерный саботаж (ст. 350a (1), 350b (1)); распространение вирусов (ст. 350a (3), 350b); компьютерный шпионаж (ст. 273 (2)).

В ряд статей, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст.ст. 317, 318); запись (прослушивание, копирование) информационных коммуникаций; кража путем обмана служб (ст. 362c)), были внесены дополнения, в редакции других (саботаж (ст.ст. 161, 351); подлог банковских карточек (ст. 232)) даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст.ст. 98, 98a); вмешательство в коммуникации (ст. 139a, 139b); порнография (ст. 240b).

Таким образом, уголовное законодательство Нидерландов предоставляет широкие возможности для борьбы с различными видами компьютерных преступлений.

В ФРГ с 1 января 1975 года действует новая редакция Уголовного кодекса 1871 года. С этого же времени началась дискуссия о целесообразности разработки уголовного законодательства, предусматривающего ответственность за действия, связанные с компьютерами.

В 1986 году в Уголовный кодекс было введено несколько новых поправок, содержащих описание компьютерных преступлений. В настоящее время УК ФРГ имеет 7 составов компьютерных преступлений. Предусмотрена уголовная ответственность для лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (ст. 202a).

Ответственности за компьютерное мошенничество (ст. 263a) подлежит лицо, оказавшее влияние на результаты процесса обработки информации путем неправильного оформления программ (манипуляцией с программным обеспечением), использования неправильных или неполных данных, а также посредством незаконного использования данных или воздействия на процесс обработки информации. Уголовно наказуемо изменение данных, имеющих доказательственное значение (ст. 269), а также фальсифицированное

использование результатов переработки данных в правоприменительной деятельности (ст. 270).

УК ФРГ предусматривает наказание за уничтожение, повреждение технических записей, не принадлежащих виновному вообще или исключительно (ст. 274). Подлежит ответственности тот, кто неправомерно аннулирует, уничтожает, делает непригодными или изменяет данные (ст. 303a). Установлена уголовная ответственность за компьютерный саботаж (ст. 303b).

Среди уголовных кодексов европейских зарубежных государств особое внимание привлекают кодексы Испании[56] и Франции[57], недавно вступившие в силу Кодекс Франции вступил в действие с весны 1994 года, а Испании в 1996 года.

Кодекс Франции включает составы большого числа компьютерных преступлений. Среди них посягательства на деятельность ЭВМ. Так, в главе 3 устанавливается ответственность за преступления, посягающие на системы автоматизированной обработки данных, такие как незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1); воспрепятствование работе или нарушение работы системы (ст. 323-2); ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3).

В УК Франции предусмотрена ответственность за посягательства, связанные с использованием картотек и обработкой данных на ЭВМ: осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16); осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17); сбор и обработка данных незаконным способом (ст. 226-18); ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19); хранение определенных данных сверх установленного законом срока (ст. 226-20); использование данных с иной целью, чем это было предусмотрено (ст. 226-21); разглашение данных, могущее привести к указанным в законе последствиям (ст. 226-22).

Кроме того, Кодекс Франции предусматривает ответственность за действия, совершаемые с компьютерной информацией в ущерб интересам государства. Перечень данных составов преступлений также достаточно велик: сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних (ст.ст. 411-7, 411-8, 413-9, 413-10, 413-11).

В УК Испании, в отличие от УК Франции, нет специальных норм, предусматривающих ответственность за посягательство на компьютерную информацию, но она установлена за преступления, совершаемые с использованием информационных технологий: раскрытие и распространение тайных сведений (ст. 197); посягательство на интеллектуальную собственность (ст. 270) и коммерческую тайну (ст.278); подделка документов (ст. 394); изготовление и владение средствами (инструмент, материал, орудие, вещество, машина, компьютерная программа, аппарат), специально предназначенными для совершения преступлений, предусмотренных в предыдущих статьях (ст. 400); раскрытие и выдача тайны и информации, связанных с национальной обороной (ст.ст. 598, 599).

В Соединенных Штатах Америки компьютерная преступность появилась на рубеже 70-х годов. Именно с этого времени возник вопрос о том, в какой мере действующее уголовное законодательство обеспечивает потребности борьбы с компьютерными преступлениями. Американские исследователи пришли к выводу, что законодательство нуждается в новых законах, ориентированных на противодействие не известным ранее явлениям[58, с. 11].

В частности, в США возникла проблема уголовно-правовой оценки действий человека, который делает копию записи информации, а затем продает ее заинтересованным лицам. За что привлекать к ответственности в данном случае? Ведь кражи имущества в традиционном значении этого слова не происходило. Можно ли компьютерную программу считать «имуществом»? Как оценивать действия человека, который продает машинное время, стоимость которого представляется достаточно высокой? Поэтому не случайно в 1977 года в США появился законопроект о защите федеральных компьютерных систем.

Он предусматривал уголовную ответственность за следующие категории компьютерных преступлений: введение ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; кража денег, ценных бумаг, имущества, услуг, ценной информации, совершенная электронными или иными средствами. На основе данного законопроекта в 1984 году был принят соответствующий федеральный закон, который затем был дополнен в 1986 году.

В настоящее время в Соединенных Штатах преступления с использованием компьютера становятся все более обычным явлением вследствие всеобщей компьютеризации страны, хотя никто в точности не знает, сколько их совершается в действительности.

По приблизительным оценкам американских исследователей, ущерб от такого рода преступлений составляет миллиарды долларов ежегодно.

Общепринятого определения того, что надо понимать под компьютерным преступлением, в США нет. Каждый штат имеет свой закон,

специально рассматривающий преступления, связанные с использованием компьютера. Причем некоторые штаты ограничиваются модификацией традиционных законов, например, предусматривая ответственность за хищения компьютерного времени или данных.

Американские исследователи, основываясь на анализе действующего законодательства, выделяют пять основных форм неправомерного поведения, связанного с использованием компьютеров, которые в той или иной формулировке представлены в законах штатов: неразрешенный доступ; неразрешенное использование; нечестная манипуляция или изменение данных; компьютерный саботаж; хищение информации[58, с. 18].

Данная классификация не лишена недостатков, которые отмечают и сами американские ученые. В частности, она не включает хищение элементов компьютерного оборудования, не предусматривает ситуации, когда компьютеры используются при совершении других преступлений и т.д.

Анализируя все изложенное в первой главе, можно сделать ряд выводов.

В конце восьмидесятых и начале девяностых годов прошлого столетия ответственность за компьютерные преступления была предусмотрена во многих государствах мира.

Несмотря на новизну компьютерных преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает.

Проведенный анализ показал, что законодательство об уголовной ответственности за уголовные правонарушения в сфере информатизации и связи отличается определенным своеобразием; не во всех государствах бывшего СССР законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных информации и технологий. Многие европейские государства и США провели решительную борьбу с уголовными правонарушениями в сфере информатизации и связи с момента их появления в жизни общества, следовательно, правовая регламентация уголовной ответственности за совершение уголовных правонарушений в сфере информатизации и связи отличается очень высокой степенью детализации и высоким уровнем юридической техники.

Очевидно, что национальному законодателю следует оценить опыт зарубежных государств и выяснить пригодность вышеупомянутых правовых инструментов для защиты в сфере информатизации и связи

# 2 ХАРАКТЕРИСТИКА СОСТАВОВ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

## 2.2 Характеристика общих объективных и субъективных признаков уголовных правонарушений в сфере информатизации и связи

Информационные и коммуникационные технологии в процессе своего развития занимают все более значимое место в жизни общества. Они широко внедряются в деятельность государственных органов, финансово-экономических институтов. Все большие объемы информации, денежных средств, производственных процессов переносятся в электронную форму.

Одновременно с этим становятся актуальными вопросы защиты информационных ресурсов, информационных систем и инфраструктуры связи от противоправных посягательств, предупреждения использования возможностей этих технологий в преступных целях.

Общественная опасность уголовных правонарушений в сфере информатизации и связи заключается, прежде всего, в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи.

Опасность компьютерных преступлений помимо того, что преступник, оставаясь «невидимым», может принести значительный ущерб, определяется еще и тем, что компьютер постепенно во всем мире заполняет все сферы жизнедеятельности человека, что позволяет преступникам значительно расширить свою экспансию. «Спектр преступного использования компьютеров практически равен спектру его применения по прямому назначению, а это означает, что преступное вторжение через ЭВТ может быть произведено в сферу космической и оборонной индустрии, политики и международных отношений и т.п.»[59, с. 35].

Теория и практика не выработали единого определения компьютерных преступлений. Объясняется это, в первую очередь, различием отечественного и зарубежного законодательства о преступлениях с использованием компьютера. Так, на заседании постоянно действующего межведомственного семинара «Криминалистика и компьютерная преступность» в 1993 году компьютерные преступления определялись как «предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства»[27, с. 24]. Такого понятия в основном придерживаются зарубежное законодательство и практика.

Наиболее распространенными преступлениями 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. До 95% программного продукта, реализуемого в Казахстане, является пиратским [60, с. 13]. 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.

Комплекс причин и условий компьютерной преступности составляют, по мнению большинства авторов, следующие обстоятельства: высвобождение и сложности трудоустройства высокоинтеллектуальной и профессиональной части населения, связанной с наукой, тонкими технологиями, обороной и т.п.; безработица интеллектуальной элиты общества; возможность быстрого обогащения путем компьютерных хищений с незначительной вероятностью разоблачения ввиду высокой латентности компьютерных преступлений; недостаточная защищенность автоматизированных систем обработки данных; отставание технической оснащенности, профессионализма сотрудников правоохранительных органов от действий профессиональных компьютерных преступников; отсутствие обобщенной следственной и судебной практики расследования компьютерных преступлений; лояльное отношение общества к такого рода преступлениям ввиду использования лицами, их совершающими, интеллектуального способа обогащения и т.п.[61, 447]. Начиная с 80-х годов, когда появились первые отечественные публикации о необходимости противостояния компьютерной преступности, их авторы указывали еще и на такое условие, как отсутствие законодательной базы подобной борьбы[62, с. 12]. В настоящее время подобное законодательство существует, но оно не вполне совершенно.

Большинство уголовных правонарушений в сфере информатизации и связи – 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»)[63, с. 146].

Родовым объектом уголовных правонарушений в сфере информатизации и связи является общественная безопасность в сфере получения информации и связи.

В ст. 1 Закона РК от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан»[64] дается понятие национальной безопасности Республики Казахстан (далее – национальная безопасность) – состояние защищенности национальных интересов Республики Казахстан от реальных и потенциальных угроз, обеспечивающее динамическое развитие человека и гражданина, общества и государства.

в соответствии со ст. 3 Закона «О национальной безопасности Республики Казахстан» к основным принципами обеспечения национальной безопасности являются: 1) соблюдение законности при осуществлении деятельности по обеспечению национальной безопасности; 2) приоритет прав и свобод человека и гражданина; 3) оперативное взаимное информирование и согласованность действий сил обеспечения национальной безопасности; 4) единство, взаимосвязь и сбалансированность всех видов национальной безопасности, оперативное изменение их приоритетности в зависимости от развития ситуации; 5) приоритетность предупредительно-профилактических мер при обеспечении национальной безопасности; 6) своевременность и адекватность мер обеспечения национальной безопасности масштабам и характеру нанесенного и (или) потенциального ущерба национальной безопасности; 7) соблюдение баланса интересов человека и гражданина, общества и государства, их взаимная ответственность; 8) контролируемость реализации всей совокупности действий по защите национальной безопасности; 9) интеграция системы обеспечения национальной безопасности с международными системами безопасности; 10) четкое разграничение полномочий государственных органов.

К основным объектам безопасности Закон относит: человека, его жизнь, права и свободы; общество, его материальные и духовные ценности; государство, его конституционный строй. Выделяют различные виды безопасности: общественную, военную, политическую, экономическую, информационную и экологическую безопасность.

В круг этих объектов Закон включает и информационную безопасность. В соответствии со ст. 4 данного Закона к информационной безопасности относится – 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.

Уголовно-правовая охрана таких объектов общественной безопасности, как основы конституционного строя и безопасность государства, а также мир и безопасность человечества, от внешних и внутренних угроз, относится к иным разделам УК. В рассматриваемом же разделе УК берет под охрану

человека (жизнь, здоровье, собственность, иные права и свободы); общество (его материальные и духовные ценности) от внешних угроз.

Безопасность как условие функционирования и развития общества имеет две составляющие, которые оцениваются по объективным и субъективным критериям. Объективный критерий – это уровень реальной защищенности системой законодательного регулирования, организационными мерами по использованию материальных средств, реализацией этих мер правоохранительными и другими органами. Субъективный критерий общественной безопасности как объекта уголовно-правовой охраны – часть общественной психологии, то есть общественное спокойствие, ощущение состояния защищенности, своей безопасности и безопасности других, неприкосновенности собственности, уверенность в нормальной работе государственных и общественных институтов.

Информационная безопасность представляет собой состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению до заданного уровня, предотвращению или исключению негативных последствий от воздействия (или отсутствия такового) на элементы информационной сферы[65, с. 187].

В Концепции кибербезопасности Республики Казахстан «Киберщит Казахстана» утвержденной Постановлением Правительства Республики Казахстан от 30 июня 2017 года[3], понятие информационная безопасность рассматривается с двух взаимосвязанных аспектов: технического и социально-политического.

Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации.

Социально-политический аспект заключается в защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан.

«Современное общество использует четыре основных ресурса: природные богатства, труд, капитал и информацию»[66, с. 6].

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина, принятая Генеральной Ассамблеей ООН 10 декабря 1948 года[67, с. 131-159], 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 РК в ч. 2 ст. 20 подтвердила и гарантировала это право граждан, ограничив его сведениями, составляющих

государственные секреты Республики Казахстан. Вместе с тем Конституция РК содержит ряд иных ограничений, связанных с распространением информации. В частности, ст. 18 закрепляет право граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Комплексное законодательство об охране информации в Республике Казахстан появилось только в середине 90-х годов, до этого времени существовали лишь отдельные законы, содержавшие некоторые нормы об охраняемой информации.

На сегодняшний день новейшие информационные технологии, СМИ, многократно усилили возможности информационного воздействия на человека, население государства в целом. В результате информация превратилась в важнейший ресурс государства наряду с его другими основными ресурсами (природными, экономическими, трудовыми, материальными и т.д.).

Некоторые психологи утверждают, что человек разумный постепенно превращается в человека информационного. Наряду с традиционными методами управления обществом (административно-организационными, экономическими, социально-психологическими, правовыми) и отдельными личностями все большее распространение получает специальный метод централизованного воздействия на широкие слои населения – метод информационного управления. В основе метода информационного управления лежит теория Антонио Грамши о том, что для достижения стратегических целей изменения общественного строя надо действовать, меняя не базис общества, а через надстройку – силами интеллигенции, совершая молекулярную агрессию в сознание общества и разрушая его культурное ядро. Так, один из постулатов теории управления гласит, что эволюции в человеческом сознании достичь проще, чем совершить в нем революционные изменения[68, с. 6].

Информация в переводе с латинского information означает «ознакомление, разъяснение, изложение».

В философской литературе сложилась устойчивая традиция рассмотрения информации на основе философских категорий отражения и различия (разнообразия). Информация не существует без отражения, как и отражение без информации. Свойство отражения заключается в способности любого объекта воспроизводить некоторые особенности воздействующих на него объектов. Однако для определения понятия информации одной категории отражения недостаточно. Информация имеет место только там, где среди некоторого тождества существует определенное различие. Единицей измерения информации может считаться элементарное различие, то есть различие между двумя объектами в каком-либо одном фиксированном свойстве. Чем больше в совокупности отличных друг от друга элементов, тем

больше эта совокупность содержит информации. Таким образом, информация в философии определяется как отраженное разнообразие, а именно разнообразие, которое отражающий объект содержит об отражаемом[69, с. 401].

Как отмечает Юрченко И. А., особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее. Даже тогда, когда информация отражается сознанием человека, она существует лишь в единстве с определенными нейрофизиологическими процессами, то есть имеет свой материальный носитель[70, с. 15].

В конце 50-х годов один из основоположников кибернетики, Н. Виннер определил информацию как: «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде»[71, с. 31]. В данном определении ученый впервые затрагивает проблему неполноты получаемой индивидом информации, с одной стороны, а с другой, необходимость защиты сведений от «случайностей внешней среды».

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводит в юридическую сферу понятия, ранее применявшиеся в кибернетике и информатике.

Правовое понятие информации несколько уже, чем философское. В контексте Закона Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации»[72] термин «информация» становится универсальным, он обозначает любые сведения о лицах, предметах, фактах, событиях, явлениях и процессах, полученные или созданные обладателем информации, зафиксированные на любом носителе и имеющие реквизиты, позволяющие ее идентифицировать. В данном определении сведения понимаются как реальные объекты социальной жизни: лица, предметы, факты, события, явления, процессы. Эти сведения могут служить и объектом познания, и ресурсом пополнения информационной базы: с одной стороны, сведения могут быть получены в результате исследования окружающей действительности и приобщены к уже существующей объективной системе знаний о мире, а с другой, быть объектом поиска, производимого конкретным потребителем для достижения его целей.

Вся информация, объединенная в информационные ресурсы (отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах), подразделяется на открытую (общедоступную) и информацию с ограниченным доступом. Последняя, в свою очередь, делится на информацию, отнесенную к государственной тайне, и конфиденциальную. Именно информация с

ограниченным доступом (а отнесенной к таковой она может быть только на основании закона) является предметом компьютерных преступлений.

Государственная, служебная, коммерческая тайна, а также многие иные виды информации нуждаются в обязательной государственной правовой охране. В некоторых случаях важность тайны информации настолько велика, что ее охрану государство осуществляет мерами уголовного законодательства. Вместе с тем правовая охрана информации не может ущемлять права граждан. Так, в соответствии с ч. 1 ст. 6 Закона «О доступе к информации» не могут относиться к информации с ограниченным доступом, в частности, сведения о чрезвычайных ситуациях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствия.

Компьютерная информация – это информация в оперативной памяти ЭВМ, информация на иных машинных носителях как подключенных к ЭВМ, так и на съемных устройствах, включая дискеты, лазерные и иные диски. Цена дискеты не имеет никакого отношения к ценности информации, на ней записанной. Хищение дискеты (кроме грабежа и разбоя) влечет административную ответственность за мелкое хищение, что не исключает ответственности за неправомерный доступ к информации, на ней записанной, если виновный при этом умышленно приобретает доступ к информации на дискете.

Компьютерная информация в системе или сети ЭВМ не может существовать иначе как на конкретных ЭВМ, в эту систему или сеть объединенных. Поэтому, например, перехват информации при ее передаче по каналам связи будет неправомерным доступом к информации в ЭВМ, с которой она передается. Компьютерная информация в ЭВМ, в свою очередь, существует только в виде записей на машинных носителях.

Определяя слово «компьютер» следует исходить из употребления слов «ЭВМ», «компьютер» в естественном русском языке. Так, очевидно, не может рассматриваться в качестве компьютера калькулятор, и использование чужого калькулятора без разрешения его хозяина не является преступлением. Не будет компьютером и кассовый аппарат, в том числе и оборудованный электронным запоминающим устройством. В русском языке слова «ЭВМ», «компьютер» употребляются для обозначения «карманных компьютеров» (например, компьютеров для Windows CE, «ньютонов»), персональных компьютеров и компьютеров более высокого уровня. Компьютерами будут и электронные машины, являющиеся неотъемлемой частью какой-либо технической системы (бортовые компьютеры, компьютеры в автоматизированных производствах и т.п.).

Специалисты прибегают к разным критериям отграничения «компьютеров» от иных вычислительных устройств. Так, например, одни используют идеальную модель «машины Тьюринга» (минимальный набор функций – по этому критерию к компьютерам можно отнести и

программируемый калькулятор), другие большее внимание уделяют интерфейсу и операционной системе, третьи вовсе отрицают принципиальное отличие компьютера от иных вычислительных устройств. В уголовном праве приемлем лишь лингвистический критерий.

Большей частью преступления в сфере компьютерной информации могут совершаться только путем действия – неправомерный доступ к компьютерной информации или создание либо использование вредоносных программ для ЭВМ. Однако нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети возможно и путем бездействия – в виде невыполнения обязательных предписаний таких правил.

Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть сформулированы как преступления с материальным составом, а создание, использование или распространение вредоносных программ и программных продуктов – с формальным.

Временем совершения компьютерного преступления (временем совершения общественно опасного деяния независимо от времени наступления последствий – ст. 5 УК РК) является момент нажатия клавиши клавиатуры компьютера или кнопки «мыши», отсылающей последнюю компьютерную команду, независимо от того, в какое время наступили опасные последствия. Время, отделяющее последствия от деяния, может быть минимальным и составлять несколько секунд, необходимых для прохождения информации по каналам и выполнения компьютером команды. Однако в некоторых случаях этот промежуток времени может быть весьма продолжительным. В основном это относится к ст. 205 и 210 УК РК. Некоторые вредоносные программы могут начать свое разрушительное действие не сразу, а по истечении длительного времени. Вирус может, выражаясь терминологией программистов, «спать» в компьютере и начать работу после совершения пользователем определенных действий, например, после обращения к тем или иным программам, использования определенных терминов или просто по прохождении некоторого времени.

На основе анализа вышеперечисленных существующих точек зрения ученых-юристов мы считаем, что под уголовными правонарушениями в сфере информатизации и связи, следует понимать запрещенное уголовным законом умышленное деяние, причиняющее вред общественным отношениям в сфере информатизации и связи, безопасности компьютерных систем или создающее угрозу причинения такого вреда. Под безопасностью компьютерных систем следует считать совокупность общественных отношений, обеспечивающих правомерное использование компьютерных технологий и компьютерной информации. Уголовными правонарушениями, совершаемые с использованием компьютерных технологий, следует понимать совокупность общественно опасных деяний, характеризующейся особым объектом - безопасностью информационных систем.

Значительно сложнее обстоит дело с определением места совершения преступления. Поскольку большое количество компьютерных преступлений совершается в компьютерных сетях, объединяющих несколько регионов или стран, лидирующее место среди которых занимает всемирная компьютерная сеть Интернет, постольку место совершения деяния и место наступления последствий могут отделять многие километры, таможенные и государственные границы. Так, недавно один суд рассмотрел уголовное дело по факту хищения средств с использованием компьютерной сети Интернет. Гражданин Казахстана Г., используя домашний компьютер, в одном из сайтов Интернета обнаружил программу, производящую безналичные расчеты с кредитных карт. Г. скопировал программу на свой компьютер. После этого Г., входя в виртуальный магазин, реальный аналог которого располагался в Канаде, производил заказ и предварительную оплату товаров с чужих кредитных карточек, используя вышеупомянутую программу. После этой трансакции Г. незамедлительно отказывался от приобретения товара, однако для возврата денег указывал уже иные номера кредитных карт – собственных или своих сообщников. При этом последние были как гражданами Казахстана, так и России. Деньги либо немедленно обналичивались через банкоматы, либо с помощью кредитных карт производилась покупка товаров в тех магазинах, где расчеты возможны также с помощью кредитных карт[73]. На первый взгляд, в данном деянии затронуты три страны. Однако на самом деле их значительно больше, так как пострадавшие лица, с банковских карточек которых незаконно списывались денежные средства якобы в оплату товаров, являлись гражданами различных стран.

Уголовный кодекс РК не содержит нормы, определяющей место совершения преступления, поэтому им может быть место как совершения деяния, так и наступления последствий, либо то место, в котором деяние окончено либо пресечено.

Транснациональный характер компьютерных преступлений обусловливает повышение роли международного сообщества при принятии решения по этому вопросу. Определенные шаги в данном направлении уже сделаны. Так, в п. 18 Венской декларации 2000 года говорится о необходимости разработки программных рекомендаций в отношении преступлений, связанных с использованием компьютеров, и предлагается Комиссии по предупреждению преступности и уголовному правосудию приступить к работе в этом направлении.

Проблема унификации международно-правового уголовного регулирования квалификации компьютерных преступлений чрезвычайно важна. Государство, на территории которого наступили общественно опасные последствия, чьи граждане или организации стали потерпевшими, справедливо может претендовать на то, чтобы под местом совершения преступления признавалось именно данное государство. Однако это может

повлечь новые проблемы при решении вопроса о привлечении казахстанского гражданина к уголовной ответственности. В соответствии с ч. 1 ст. 7 УК РК такое деяние должно одновременно признаваться преступлением на территории другого государства. Если в отношении общеуголовных преступлений законодательство более или менее единообразно, то законодательство о уголовных правонарушений в сфере информатизации и связи и практика его применения весьма различаются.

О важности определения места совершения преступления красноречиво говорит следующий пример. С июня по сентябрь 1994 года российским программистом Л. и его сообщниками, являющимися гражданами других государств, с использованием компьютера, расположенного в Санкт-Петербурге, через электронную компьютерную систему телекоммуникационной связи Интернет вводились ложные сведения в систему управления наличными фондами «City Bank of America», расположенного в Нью-Йорке. В результате такой деятельности было похищено более 10 млн. долларов США со счетов клиентов банка. В организованную преступную группу входили граждане США, Великобритании, Израиля, Швейцарии, ФРГ и России. Однако при привлечении Л. к уголовной ответственности в Лондоне судебная инстанция в августе 1995 года отложила принятие решения по этому делу на неопределенный срок ввиду того, что подсудимый использовал компьютер, находящийся на территории Российской Федерации, а не на территории США, как того требовало законодательство Великобритании. В результате просьба правоохранительных органов США и России о выдаче Л. была отклонена[27, с. 17-18].

## 2.2 Особенности уголовно-правовой характеристики неправомерного доступ к информации, в информационную систему или сеть телекоммуникации

Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст. 205 УК РК). Общественная опасность уголовного правонарушения заключается, прежде всего, в том, что они нарушают права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в информационной сфере, наносят вред конфиденциальности, целостности, сохранности и доступности информационных ресурсов, информационных систем и инфраструктуры связи.

Информационная безопасность характеризуется как состояние защищенности прав и интересов человека, общества и государства в информационной сфере и отнесена Законом Республики Казахстан от 6

января 2012 г. «О национальной безопасности Республики Казахстан» к одному из видов национальной безопасности.

Общественная опасность комментируемого уголовного правонарушения (ч.ч. 1 и 2 - проступки, ч. 3 - преступление) заключается в нарушении права на конфиденциальность информации, ущемлении законных интересов собственников информационных систем и информационно-коммуникационных сетей по ограничению их доступности.

Объектом комментируемого уголовного правонарушения являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и информационно-коммуникационных сетей.

Предметом рассматриваемого уголовного правонарушения выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе национальная информационная система; информационно-коммуникационная сеть; национальные электронные информационные ресурсы.

Под информацией в комментируемой статье следует понимать информацию, хранимую в электронном виде на электронном носителе, представляющую собой такую последовательность состояний элементов электронной вычислительной техники или иных электронных средств обработки, хранения и передачи информации, которая несет определенные сведения, сообщения, данные. Информация может быть представлена в виде цифр, текста, изображения, аудио-, видео-, программного кода или их комбинации. Набор символов, не имеющих смысла и не предназначенных для чего-либо, к информации не относится[73].

К охраняемой законом информации относятся государственные секреты, личная, семейная, служебная, коммерческая, банковская, налоговая, адвокатская, врачебная и иные охраняемые законом тайны, другие конфиденциальные сведения.

Исходя из Нормативного постановления Конституционного Совета Республики Казахстан от 20 августа 2009 г., к охраняемой законом тайне следует относить сведения, не являющиеся общедоступными на равных условиях для неограниченного круга лиц, изначально неизвестные третьим лицам[74].

Конституционное право каждого на тайну подразумевает, что только само лицо, которому принадлежит эта тайна, может распоряжаться ею по своему усмотрению, в том числе передавать эти сведения третьим лицам.

Каждый имеет право отнести любые неизвестные третьим лицам сведения к конфиденциальным, если законом прямо не указывается, что эти сведения являются общедоступными либо могут быть преданы огласке или изъяты в предусмотренном законом порядке.

Очевидно, что высшую степень защиты от утечки из информационных компьютерных систем должны иметь сведения, отнесенные к государственной тайне

Согласно Закону Республики Казахстан от 15 марта 1999 г. «О государственных секретах» к государственным секретам относятся защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права[75].

Государственная тайна - это сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.

Служебная тайна - это сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

Электронными носителями называются любые виды материальных носителей, которые позволяют записывать, хранить и воспроизводить информацию в форматах данных, предназначенных для обработки средствами вычислительной техники. Формат данных может быть цифровым, как правило, бинарным и аналоговым. К электронным носителям следует относить не только постоянные запоминающие устройства - к примеру, магнитные и оптические диски, магнитные и полупроводниковые карты, но и оперативные запоминающие устройства - к примеру, оперативная память компьютера или иного электронного устройства. Информация, как правило, хранится на электронных носителях в виде файлов.

Информация, хранимая в электронном виде в информационных системах, называется электронным информационным ресурсом, или иначе - информационной базой данных. Для электронных информационных ресурсов характерен значительный объем и структурированность данных, их определенное функциональное предназначение.

Информация, хранимая в электронном виде в информационных системах, функционирующих в открытой информационно-коммуникационной сети, относится к интернет-ресурсам.

Информационная система представляет собой систему, предназначенную для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса.

Согласно статье 15 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» по критериям права собственности и категории доступа информационные системы подразделяются на государственные и негосударственные, общедоступные и ограниченного доступа.

Государственными являются информационные системы, создаваемые или приобретаемые за счет бюджетных средств либо полученные ими иным предусмотренными законом способом (дарение, конфискация и другие).

Общедоступными являются информационные системы, содержащие электронные информационные ресурсы, которые предоставляются или распространяются их собственником или владельцем без указания условий их использования, а также электронные информационные ресурсы, доступ к которым является свободным и не зависит от формы их предоставления и способа распространения. Общедоступные информационные системы не являются предметом рассматриваемого уголовного правонарушения.

Все государственные электронные информационные ресурсы являются общедоступными, за исключением отнесенных к государственным секретам и конфиденциальных информационных ресурсов. К категории конфиденциальных электронных информационных ресурсов относятся электронные информационные ресурсы, содержащие персональные данные или охраняемую законом тайну.

К информационным системам ограниченного доступа относятся информационные системы, содержащие электронные информационные ресурсы, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем в случаях, установленных законодательством Республики Казахстан.

Следовательно, к информационным системам, выступающим предметом рассматриваемого уголовного правонарушения, следует относить:

- информационные системы, содержащие государственные электронные информационные ресурсы, отнесенные к государственным секретам;

- информационные системы, содержащие конфиденциальные электронные информационные ресурсы, в том числе содержащие персональные данные, охраняемую законом тайну;

- иные информационные системы, доступ к которым ограничен их собственником или владельцем.

Информационно-коммуникационная сеть представляет собой совокупность технических и аппаратно-программных средств обеспечения взаимодействия между информационными системами или между их составляющими, а также передачи информационных ресурсов.

Объективная сторона рассматриваемого уголовного правонарушения выражается в неправомерном доступе к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или

информационно-коммуникационную сеть, в результате которого существенно нарушаются права и законные интересы граждан или организаций либо охраняемые законом интересы общества или государства[76, с. 282].

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. 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 использованием информации понимается субъект, обращающийся к информационной системе за получением необходимой информации с целью ее использования.

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. ОЗУ устройств связи, сетевые устройства и каналы связи относятся к информационно-коммуникационной сети компьютера, в которых также может находиться охраняемая законом информация[77, с. 100]..

Неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, выражается в получении возможности непосредственного завладения этой информацией и может быть осуществлен как с преодолением мер защиты, установленных собственником (владельцем) электронного носителя, так и без такового.

Неправомерный доступ к информационной системе выражается в получении возможности непосредственного использования хотя бы одной из функций этой системы: хранения, обработки, поиска, распространения, передачи и предоставления информации. Неправомерный доступ к информационной системе, как правило, осуществляется путем преодоления мер ее защиты.

Неправомерный доступ к информационно-коммуникационной сети выражается в получении возможности непосредственного взаимодействия с

входящими в нее информационными системами и их составляющими и также осуществляется, как правило, с преодолением мер защиты.

Выше уже упоминалось, что ст. 205 УК РК устанавливает наказание за неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть при условии, если это деяние повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства. Такой перечень обязательных последствий вполне обоснован. На практике ему соответствует достаточно широкий круг противоправных деяний, направленных на нарушение целостности, доступности и конфиденциальности информации. Прежде всего, среди специалистов распространено мнение, что «сам по себе факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. Необходимо, по крайней мере, установить факт переноса указанной информации на другой машинный носитель». Действительно, если полученные следствием материалы не подтверждают факта уничтожения, блокирования, модификации или копирования компьютерной информации, то несанкционированное обладателем ознакомление с ней не может служить достаточным основанием к применению ст. 205 УК. Однако совершенно понятно, что на практике в большинстве случаев существенный ущерб обладателю конфиденциальной информации наносит уже само ознакомление с ней постороннего лица.

В рассматриваемом аспекте проблема юридической оценки мысленного восприятия информации лицом, осуществляющим неправомерный доступ к ней без ее копирования на машинные носители, является достаточно сложной. По замечанию В. В. Крылова, «если придерживаться понимания термина копирования только как процесса изготовления копии документированной информации в виде физически осязаемого объекта, то все случаи, не связанные с копированием, но приводящие к ознакомлению с информацией независимо от того, какой режим использования информации установил ее собственник, не являются противоправными»[78, с. 84].

При этом не учитывается позиция некоторых исследователей о «существовании исключительного специфического носителя охраняемых информационных ресурсов – человека, его памяти»[79, с. 24] и то обстоятельство, что в ряде случаев с запечатленной в памяти информации может быть впоследствии изготовлена копия, в том числе и на машинном носителе.

Доступ осуществляется только программно-техническими средствами.

Выделяются три вида мер защиты: правовые, организационные и технические (программно-технические).

Технические (программно-технические) меры защиты информации, хранящейся на электронном носителе, электронных информационных

ресурсов и информационных систем от несанкционированного доступа состоят в установлении технических (программно-технических) средств, реализующих функции контроля доступа (в том числе регистрации фактов доступа, блокирования несанкционированного доступа), шифрования информации.

Преодоление технических или программно-технических мер защиты следует рассматривать как действие, непосредственно направленное на совершение данного уголовного правонарушения, и также осуществляется только программно-техническими средствами.

Правовые меры защиты выражаются в договорных обязательствах между собственником (владельцем) электронных информационных ресурсов и их пользователями, устанавливающих условия доступа и использования этими ресурсами.

Организационные меры защиты могут выражаться в разграничении прав доступа к информации по кругу лиц и характеру информации.

Преодоление правовых и организационных мер защиты следует рассматривать как создание условий для совершения неправомерного доступа.

Ознакомление с охраняемой законом информацией, содержащейся на электронном носителе, в момент получения неправомерного доступа к ней либо в любой другой момент для квалификации данного уголовного правонарушения значения не имеет. Виновный может не знакомиться с полученными сведениями, а передать их третьим лицам.

Неправомерный доступ к информационной системе и информационно-коммуникационной сети может осуществляться непосредственно через компьютер (сервер), на котором функционирует информационная система, или компьютер (рабочую станцию), ранее подключенный к информационно-коммуникационной сети.

Неправомерный доступ без преодоления защиты может быть осуществлен через компьютер, на котором открыт доступ (сеанс) лицом, имеющим право на это (администратор, пользователь системы или сети).

Неправомерный доступ может осуществляться удаленно, в том числе через Интернет.

Рассматриваемое уголовное правонарушение по конструкции относится к материальному составу. Оно признается оконченным с момента наступления вредных последствий.

Вредные последствия выражаются в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства (ч.1 ст.205 УК) либо тяжких последствий (ч.3 ст.205 УК).

Вредные последствия выражаются в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, под которым, с учетом

положений п. 14 ст. 3 УК РК, раскрывающих понятие существенного вреда, следует понимать, в частности:

- нарушение конституционных прав и свобод человека и гражданина, прав и законных интересов организаций, охраняемых законом интересов общества и государства;

- причинение значительного ущерба (то есть ущерба на сумму, в сто раз превышающую месячный расчетный показатель);

- нарушение нормальной работы организаций или государственных органов.

Из признаков, перечисленных в п.14 ст.3 УК, для данного случая следует под существенным вредом понимать: нарушение конституционных прав и свобод человека и гражданина, прав и законных интересов организаций, охраняемых законом интересов общества и государства; причинение значительного ущерба; нарушение нормальной работы организаций или государственных органов. Таким же образом, из признаков п.4 ст.3 УК к тяжким последствиям необходимо относить: самоубийство потерпевшего (потерпевшей) или его (ее) близкого (близких); причинение крупного или особо крупного ущерба.

Между неправомерным доступом и наступившими общественно опасными последствиями должна быть установлена причинная связь.

В случаях, когда неправомерный доступ к информационной системе или информационно-коммуникационной сети привел к нарушению их работы и эти последствия не охватывались умыслом лица, деяние необходимо квалифицировать, исходя из причиненного ущерба, только по ст.205 УК.

С субъективной стороны рассматриваемое уголовное правонарушение может быть совершено только умышленно (прямой или косвенный умысел): виновный сознает, что он совершает неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления.

По отношению к причинению существенного вреда в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства возможен косвенный умысел, когда виновное лицо сознательно допускает эти последствия либо относится к их наступлению безразлично.

Мотивы и цели данного уголовного правонарушения разнообразны и на квалификацию не влияют, но они должны учитываться при индивидуализации наказания. В большинстве случаев это корыстный мотив.

В случае совершения незаконного доступа к охраняемой законом информации, хранящейся на электронном носителе, с целью незаконного собирания сведений о частной жизни лица, составляющих его личную или

семейную тайну, без его согласия, деяние образует совокупность и квалифицируется по ст. 205 УК РК и соответствующей части ст. 147 УК РК.

В случае совершения незаконного доступа в информационную систему или информационно-коммуникационную сеть с целью незаконного собирания сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия или незаконного нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений физических лиц, деяние квалифицируется по ч. 3 соответственно ст. 147 или ст. 148 УК РК. Дополнительной квалификации по ст. 205 УК РК не требуется.

В случае совершения незаконного доступа к охраняемой законом информации, хранящейся на электронном носителе, в информационную систему или информационно коммуникационную сеть с целью незаконного собирания сведений, составляющих государственные секреты, деяние образует совокупность и квалифицируется по ст. 205 и соответствующей части ст. 185 УК РК.

Не требуется дополнительной квалификации по ст. 205 УК РК в случаях совершения деяния, предусмотренного ст. 223 УК РК «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну».

Субъектом уголовного правонарушения является физическое вменяемое лицо, достигшее 16-летнего 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 правонарушениями «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 компьютеру, 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.)[77, с. 104].

В ч. 2 ст. 205 УК РК установлена ответственность за неправомерный доступ к государственному электронному информационному ресурсу или информационной системе государственных органов.

Государственными признаются информационные системы, состоящие из государственных электронных информационных ресурсов, имеющих важное стратегическое значение для экономики и безопасности государства.

Перечень национальных электронных информационных ресурсов и национальных информационных систем определен постановлением Правительства Республики Казахстан от 1 октября 2007 года № 863 «Об утверждении Перечня национальных электронных информационных ресурсов и национальных информационных систем»

К национальным электронным информационным ресурсам и национальным информационным системам относятся: информационная система «Государственная база данных «Адресный регистр»; информационная система «Государственная база данных «Физические лица»; информационная система «Государственная база данных «Юридические лица»; информационная система «Государственная база данных «Регистр недвижимости»; информационная система «Государственная база данных «е-лицензирование»; Веб-портал «электронное правительство»; Шлюз «электронного правительства»; информационная система «Платежный шлюз «электронного правительства»; Национальный удостоверяющий центр Республики Казахстан; Удостоверяющий центр государственных органов Республики Казахстан; Единая система электронного документооборота государственных органов Республики Казахстан; информационная система «Государственный регистр электронных информационных ресурсов и информационных систем»; информационная система «Депозитарий информационных систем, программных продуктов, программных кодов и нормативно-технической документации»; информационная система «Система мониторинга доменных имен KZ»; интегрированная информационная система казначейства; информационная система «Интегрированная налоговая информационная система»; информационная система «Сервисы обработки налоговой отчетности»; информационная система «Web-приложение «Кабинет налогоплательщика»; автоматизированная информационная система «Электронные

государственные закупки»; Система электронных архивов государственных органов; Единая транспортная среда государственных органов; автоматизированная информационная система «Государственные стандарты»; «Портал государственного языка» Республики Казахстан; автоматизированная информационная система государственного земельного кадастра; система электронного обучения «e-learning»; интранет-портал государственных органов; информационная система «Интегрированная информационная система для центров обслуживания населения»; информационная система «Единая электронная почтовая система государственных органов Республики Казахстан».

Доступ к национальным электронным информационным ресурсам и национальным информационным системам является ограниченным в части сведений, относящихся к третьим лицам. Пользователь этих систем вправе получать только сведения, касающиеся его лично либо доверителя или иного представляемого на основании договора или закона лица, либо сведения о третьих лицах в пределах служебных полномочий.

В ч. 3 ст. 205 УК РК предусмотрен особо квалифицирующий признак - тяжкие последствия.

С учетом положений п. 4) ст. 3 УК РК к тяжким последствиям необходимо относить, в частности: самоубийство потерпевшего (потерпевшей) или его (ее) близкого (близких); причинение крупного или особо крупного ущерба. Эти последствия должны находиться в причинной связи с умышленным неправомерным доступом.

Законодатель в ч. 3 ст. 205 УК РК специально указал, что тяжкие последствия должны наступить по неосторожности. Следовательно, по отношению к причинению тяжких последствий возможна только неосторожная форма вины, в виде преступной самонадеянности или преступной небрежности. Совершая умышленный неправомерный доступ, лицо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит, но должно и может предвидеть возможность их наступления. При этом в соответствии со ст. 22 УК РК в целом преступление, предусмотренное ч. 3 ст. 205 УК РК, признается совершенным умышленно.

Деяния, предусмотренные ч.ч. 1 и 2 ст. 205 УК РК, относятся к уголовным проступкам.

Деяние, предусмотренное ч. 3 ст. 205 УК РК, относится к преступлениям небольшой тяжести.

## 2.3 Особенности уголовно-правовой характеристики создание, использование или распространение вредоносных компьютерных программ и программных продуктов

Ст. 210 УК РК предусматривает ответственность за создание, компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт 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, а равно умышленные использование и (или) распространение такой программы или программного продукта.

Общественная опасность анализируемого уголовного правонарушения определяется масштабностью и значительностью ущерба, который может причинить программа, созданная с деструктивными возможностями, а также возможностью использования таких программ для совершения иных уголовных правонарушений[76, с. 292].

Компьютерная программа – это объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютера, с целью получения определенного результата. Программа реализует алгоритм решения какой-либо задачи. Создание компьютерной программы – это написание ее алгоритма, то есть последовательности логических команд, с дальнейшими преобразованиями его в машинном языке.

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 в наем, предоставление 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-коммуникационную 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 носителе 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 представляют собой один из способов их распространения (к примеру, сетевой способ) и по сути дела является альтернативным распространению вредоносных программ и программных продуктов деянием.

Под уничтожением информации следует понимать приведение ее либо полностью, либо в существенной части в состояние, делающее ее непригодной для использования по назначению.

Блокирование информации – это невозможность ее использования при сохранности такой информации.

Под модификацией понимается изменение первоначальной информации без согласия ее собственника или иного законного лица.

Копирование информации – это снятие копии с оригинальной информации с сохранением ее неповрежденности и возможности использования по назначению.

Нарушение работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети может выразиться в их произвольном отключении, в

отказе выдать информацию, в выдаче искаженной информации при сохранении целости этих устройств или их сети.

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 указанных в диспозиции статьи деяний.

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

В случае если действие вредоносной программы было условием совершения лицом другого уголовного правонарушения, деяния должны быть квалифицированны по совокупности вне зависимости от степени тяжести другого уголовного правонарушения.

Программу-вирус называют так потому, что ее функционирование внешне схоже с существованием биологического вируса, который использует здоровые клетки, инфицируя их и заставляя воспроизводить вирус. Компьютерный вирус не существует сам по себе, он использует иные программы, которые модифицируются и, выполняя определенные функции, воспроизводят вирус[80, с. 120].

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.

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);

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. Активизируются 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 дня 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 счёт 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.

Вопрос о том, как определить, является ли программа вредоносной, очень сложный, особенно для неспециалиста. Вредоносных для ЭВМ программ существует очень много.

Как ранее было отмечено к вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

«Сетевые черви»

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т.д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ– и IRC-сообщениях, файл в каталоге обмена P2P и т.д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, то есть имеют свойство троянской программы и/или компьютерного вируса.

«Классические компьютерные вирусы»

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удаленные компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съемный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

«Троянские программы». В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

«Хакерские утилиты и прочие вредоносные программы»

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного программного обеспечения;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам[81, с. 14-22].

Цели использования компьютерных вредоносных программ

«Мелкое воровство». С появлением и популяризацией платных Интернет-сервисов (почта, WWW, хостинг) компьютерный андеграунд начинает проявлять повышенный интерес к получению доступа в сеть за чужой счет, то есть посредством кражи чьего-либо логина и пароля (или нескольких логинов/паролей с различных пораженных компьютеров) путем применения специально разработанных троянских программ.

В начале 1997 года зафиксированы первые случаи создания и распространения троянских программ, ворующих пароли доступа к системе AOL.

В 1998 году, с распространением Интернет-услуг в Европе и России, аналогичные троянские программы появляются и для других Интернет-сервисов. До сих пор троянцы, ворующие пароли к dial-up, пароли к AOL, коды доступа к другим сервисам, составляют заметную часть ежедневных «поступлений» в лаборатории антивирусных компаний всего мира.

Троянские программы данного типа, как и вирусы, обычно создаются молодыми людьми, у которых нет средств для оплаты Интернет-услуг. Характерен тот факт, что по мере удешевления Интернет-сервисов уменьшается и удельное количество таких троянских программ.

«Мелкими воришками» также создаются троянские программы других типов: ворующие регистрационные данные и ключевые файлы различных программных продуктов (часто – сетевых игр), использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т.п.

«Криминальный бизнес»

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно или неосознанно создают вредоносные программы с единственной целью: получить чужие деньги (рекламируя что-либо или просто воруя их), ресурсы зараженного компьютера (опять-таки, ради денег – для обслуживания спам-бизнеса или организации DoS-атак с целью дальнейшего шантажа).

Обслуживание рекламного и спам-бизнеса – один из основных видов деятельности таких хакеров. Для рассылки спама ими создаются специализированные троянские proxy-сервера, которые затем внедряются в десятки тысяч компьютеров. Затем такая сеть «зомби-машин» поступает на черный Интернет-рынок, где приобретается спамерами. Для внедрения в операционную систему и дальнейшего обновления принудительной рекламы создаются утилиты, использующие откровенно хакерские методы: незаметную инсталляцию в систему, разнообразные маскировки (чтобы затруднить удаление рекламного софта), противодействие антивирусным программам.

Вторым видом деятельности подобных вирусописателей является создание, распространение и обслуживание троянских программ-шпионов, направленных на воровство денежных средств с персональных (а если повезет – то и с корпоративных) «электронных кошельков» или с обслуживаемых через Интернет банковских счетов.

Троянские программы данного типа собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину».

Третьим видом криминальной деятельности этой группы является Интернет-рэкет, то есть организация массированной DoS-атаки на один или несколько Интернет-ресурсов с последующим требованием денежного вознаграждения за прекращение атаки. Обычно под удар попадают Интернет-магазины, букмекерские конторы – то есть компании, бизнес которых напрямую зависит от работоспособности веб-сайта компании.

Вирусы, созданные этой категорией «писателей», становятся причиной многочисленных вирусных эпидемий, инициированных для массового распространения и установки описанных выше троянских компонент.

«Нежелательное программное обеспечение»

Системы навязывания электронной рекламы, различные «звонилки» на платные телефонные номера, утилиты, периодически предлагающие пользователю посетить те или иные платные веб-ресурсы, прочие типы нежелательного программного обеспечения – они также требуют технической поддержки со стороны программистов-хакеров. Данная поддержка требуется для реализации механизмов скрытного внедрения в систему, периодического обновления своих компонент и противодействия антивирусным программам.

Очевидно, что для решения данных задач в большинстве случаев также используется труд хакеров, поскольку перечисленные задачи практически совпадают с функционалом троянских программ различных типов.

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

Выполнение объективной стороны данного преступления возможно только путем совершения активных действий. Создание, использование и

распространение вредоносных программ для ЭВМ будет выполнено с момента создания такой программы, внесения изменений в существующие программы, использования либо распространения подобной программы. Наступление определенных последствий не предусмотрено объективной стороной состава. Однако такие программы должны содержать в себе потенциальную угрозу уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Для признания деяния оконченным достаточно совершения одного из действий, предусмотренных диспозицией статьи, даже если программа реально не причинила вреда информационным ресурсам либо аппаратным средствам. К таким действиям относятся:

- создание вредоносной компьютерной программы, программного продукта;
- внесение вредоносных изменений в существующую компьютерную программу или программный продукт;
- использование и (или) распространение вредоносной компьютерной программы или программного продукта.

Использование вредоносных программ в глобальных сетях

Глобализация общественных процессов, характерная для современного этапа развития общества и тесно связанная с совершенствованием информационных технологий, привела к глобализации коммуникационных систем. Единое мировое информационное пространство стало вполне ощутимой реальностью. В последние годы происходит стремительный рост числа пользователей глобальными сетями, прежде всего Интернетом. В настоящее время также можно отметить интенсивное увеличение российского сегмента глобальной информационной сети Интернет как в количественном (число операторов и пользователей), так и в качественном (расширение круга оказываемых услуг) отношении.

Сегодня стало совершенно очевидным, что расширение всемирной паутины и возрастание объема и качества доступных ресурсов сопровождаются соответствующим ростом различных злоупотреблений. В условиях широкого распространения интернет-технологий в экономической и иной деятельности преступность в виртуальной сфере представляет достаточно серьезную угрозу.

Интернет все более активно используется преступниками для незаконного проникновения в корпоративные и личные базы данных, а также в качестве пособий по приготовлению к террористическим акциям, рекомендаций относительно того, как уйти от уголовного преследования, для пропаганды национальной вражды и призывов к развязыванию войны.

Одним из наиболее распространенных сетевых преступлений, Вредоносные программы (троянские программы, компьютерные вирусы, компьютерные черви, программные закладки) получили в глобальных компьютерных сетях очень широкое распространение. Некоторые из них,

выходя из-под контроля создателей, могут неуправляемо наносить существенный вред. Здесь можно вспомнить нашумевший в свое время случай с вирусом, созданным Робертом Т. Морисом, студентом первого курса университета в Корнелле. Проверяя возможность копирования программ с компьютера на компьютер в сети ARPANET, студент вывел из строя 6200 компьютеров США, так как из-за сбоя в алгоритме скорость размножения вируса стала гигантской. При этом вирус поразил компьютеры секретной военной сети MILNET, хотя эксперимент проводился в ARPANET. Соединение этих двух сетей держалось в секрете и потому стало полной неожиданностью для американского студента[82, с. 276]. А, например, вирус «Мелисса» в 1999 году независимо от воли создателя инфицировал программы более 1 млн. компьютеров, подключенных к Интернету[83, с. 86].

Особое место среди вредоносных программ занимают компьютерные вирусы, вредоносные программы для ЭВМ, способные к самораспространению путем включения своего программного кода или некоторой его части в программный код файлов, системные области или иное рабочее пространство машинных носителей информации с сохранением всех первоначальных свойств или некоторой их части[84, с. 29].

Цели, с которыми распространяются в глобальных сетях компьютерные вирусы, могут быть самыми различными – от хулиганских до политических. В последнее время довольно часто подобные действия совершаются по идеологическим мотивам. Для обозначения этого явления в западных средствах массовой информации применяется такое понятие, как «хактивизм». В качестве примера можно привести случай, когда во время Косовского конфликта коммерческие структуры, общественные организации, академические институты получали из некоторых европейских стран электронную почту с вирусами. Эти сообщения политической направленности, написанные на плохом английском, содержали обвинения НАТО в несправедливой агрессии и призывы к защите прав сербов, а также пропагандистские мультфильмы. Ущерб адресату таких писем причинялся несколькими вирусами, содержащимися во вложении (например, в антинатовском мультфильме).

Сегодня количество известных вирусов не поддается строгому учету и постоянно увеличивается. По приблизительным оценкам специалистов, ведущих борьбу с вредоносными программами, в среднем ежедневно появляется около 30 новых вирусов. Еще в 1987 году специалисты доказали невозможность разработки алгоритма, способного обнаружить все возможные вирусы. Исследования компании IBM показали, что возможно создание вирусов, выявление которых будет затруднено даже при наличии образца вируса[83, с. 85-86].

Еще одной проблемой являются сложности, возникающие при оценке ущерба, наносимого вирусами. Это связано с необходимостью анализа большого количества показателей, трудно поддающихся учету. Основные

издержки связаны с простоями вычислительной техники, очисткой ее от зараженных файлов, восстановлением информации, внедрением нового защитного программного обеспечения, ухудшением репутации пострадавших фирм.

Один из наиболее известных производителей антивирусного программного обеспечения компания McAfee в своем отчете пришла к выводу, что ситуация с вирусами будет ухудшаться в связи с постоянным увеличением их числа, усложнением применяемых при их создании алгоритмов, изменением механизмов распространения, расширением глубины проникновения в системы и, как следствие, нарастанием масштабов причиняемого вреда[83, с. 87].

Некоторые авторы относятся к таким программам как к информационному оружию, для которого характерны универсальность, радикальность воздействия, доступность, широкие возможности места и времени применения, высокая эффективность на значительных расстояниях, скрытность использования[85, с. 82-89].

Субъектом может быть лицо, достигшее 16-летнего возраста. 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.

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 лица, 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 сторону 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 деяния, 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 предполагают наличие у виновного лица большого аспекта разветвленных видов: от узко операциональных (простая работа клавиатурой) до ориентации в сетевом пространстве

Цель данного правонарушения является 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.

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).

В ч. 2 ст. 210 УК РК предусмотрены квалифицирующие признаки, к которым относятся совершение деяния: группой лиц по предварительному сговору; лицом с использованием своего служебного положения; в отношении государственных электронных информационных ресурсов или информационных систем государственных органов.

Квалифицирующие признаки «группа лиц по предварительному сговору», «государственные электронные информационные ресурсы», «информационные системы государственных органов», рассмотрены при анализе уголовных правонарушений, предусмотренных ч. 2 ст. 205.

В ч. 3 ст. 210 УК РК предусмотрены особо квалифицирующие признаки, к которым относятся: совершение деяния преступной группой; тяжкие последствия.

Деяние, предусмотренное ч. 1 ст. 210 УК РК, относится к преступлениям средней тяжести.

Деяния, предусмотренные ч.ч. 2 и 3 ст. 210 УК РК, относятся к тяжким преступлениям.

На основании вышесказанного необходимо сделать некоторые выводы:

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.

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.

Субъективная сторона характеризуется только прямым умыслом. Виновный сознает общественно опасный характер своих действий, предвидит возможность наступления указанных в законе последствий и

желает их наступления. Мотивами преступления могут быть корыстные или хулиганские побуждения, месть, зависть и другие.

Лицо, создавшее, использовавшее вредоносную программу, распространившее ее через третьих лиц, отвечает за возникшие тяжкие последствия, если оно предвидело возможность наступления этих последствий. Преступная небрежность не вменяется в вину в случае, если между созданием, использованием и распространением вредоносной программы и соответствующими тяжкими последствиями такое количество промежуточных звеньев, что субъект явно не мог предвидеть столь опасный результат.

# 3 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

## 3.1 Причины и условия совершения преступлений в сфере информатизации и связи

В связи с развитием информационных технологий в Казахстане, как и во всем мире, ежедневно увеличивается количество используемой электронно-вычислительной техники и число пользователей в сети Интернет. Одновременно растет и количество преступлений в этой области.

В Республике Казахстан за период с 2010 по 2016 год плотность пользователей Интернета увеличилась с 36,1% до 75%, а количество пользователей мобильного Интернета с 3 миллионов 694 тысяч практически утроилось и достигло 10 миллионов 567 тысяч. Такое экспоненциальное увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов или вредоносного воздействия на технические средства[3].

Распространенность вредоносных программ для персональных компьютеров и мобильных устройств растет вместе с числом их пользователей. При этом подавляющее большинство пользователей не используют специализированное программное обеспечение для защиты своих персональных компьютеров, смартфонов, планшетов.

Этот фактор эксплуатируется «хакерами», что каждый день приводит к увеличению количества атак, нацеленных на заражение абонентских устройств вредоносным программным обеспечением.

В то время, как количество абонентских устройств, подключенных к Интернету, увеличивается и большинство пользователей продолжает игнорировать меры «цифровой гигиены» в отношении себя и принадлежащих им устройств, концепция «Интернета вещей» только усиливает проблему их безопасного использования.

Проблема причин преступности является одной из центральных в криминологии[86, с. 85]. Причинный комплекс преступности включает ее причины и условия, которые в совокупности составляют факторы преступности. Причины — это социально-психологические детерминанты, которые непосредственно порождают, воспроизводят преступность и преступления как свое закономерное следствие; условия — это такие социальные явления, которые сами не порождают преступность и преступления, а способствуют, облегчают, интенсифицируют формирование и действие причины[87, с. 167-168].

По мнению А. И. Долговой, изменения социальной среды, связанные с компьютеризацией общества, характеризуются следующими криминологический значимыми обстоятельствами[88, с. 684-685].

1. Повсеместное и всестороннее внедрение новых технологий привело к техническому оснащению отдельных преступников и организованных преступных групп;

2. Появились новые технологии совершения преступлений. Многие «традиционные» преступления стало невозможно совершать или масштабно, или без риска быстрого разоблачения, если не использовать высокие технологии. Поэтому, например, все большее распространение получают мошеннические действия, связанные с системой электронного безналичного денежного обращения;

3. Формирование информационного пространства, основанного на использовании ЭВМ, систем ЭВМ и сетей ЭВМ, а также взаимосвязанные с этим процессы зарождения и развития общественных отношений в сфере компьютерной информации стали основой возникновения новых видов преступной деятельности.

Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в ее повышении у населения, работников сферы ИКТ и руководителей организаций создают питательную почву для развития правонарушений и преступлений в информационной сфере.

Отсутствие знаний о правовых ограничениях создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и смежных прав на программное обеспечение и влияющих на функционирование информационных ресурсов.

Таким образом, низкий уровень цифровой грамотности конечных пользователей в вопросах защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов (особенно «фишинговые» страницы поддельных интернет-магазинов и банков, распространение вирусных и «троянских» программ через «взломанные» сайты, скачивание нелицензионного («пиратского») программного обеспечения) приводят к тысячам случаев, когда граждане Республики Казахстан становятся жертвами, а принадлежащие им технические средства орудиями противоправного использования ИКТ.

Недостаточная осведомленность в методах защиты информации и низкая обеспеченность в системах информационной безопасности предприятий малого и среднего бизнеса, в том числе занятых в сфере оказания информационно-коммуникационных услуг, которые зачастую даже не могут оценить состояние принадлежащей информационно-коммуникационной инфраструктуры, приводят к большому количеству не анализируемых событий и инцидентов информационной безопасности, затрудняющих как профилактику технологических уязвимостей, так и борьбу с преступниками, использующими ИКТ как средство для совершения преступлений.

Принято выделять два типа причинного комплекса компьютерной преступности[88, с. 683-684]. К первому типу относится причинный комплекс, не имеющий особенностей по сравнению с другими, «некомпьютерными» видами преступности. Отличие заключается только в том, что преступники дополнительно используют компьютерные технологии. В результате несколько изменяются условия преступной деятельности, ее формы, масштабы и последствия. Вопросу общей детерминации преступности посвящено большое количество работ ученых-криминологов[88, с. 229-376; 89, с. 85-124; 90, с. 240].

Второй тип определяет специфический (особый) комплекс причин. Он заключается в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений, связанных с появлением автоматизированных систем обработки информации. Взаимосвязь и взаимообусловленность новой социальной среды, соответствующих личностных характеристик субъекта и условий социального контроля образуют специфику причинного комплекса детерминации компьютерной преступности.

В. Д. Курушин и В. А. Минаев выделяют следующие причины компьютерной преступности[41, с. 18-21].

1. Уязвимость и взаимозависимость компьютерных систем.

2. Несовершенство социальных, юридических и политических структур, уровень развития которых значительно отстает от уровня развития компьютерных и телекоммуникационных технологий.

3. Возрастающая зависимость современных технологий от компьютерных систем и средств телесвязи.

Важность проблемы для развитых и развивающихся стран. В целях ликвидации технологического отставания развивающимся странам следует сосредоточить свои усилия на внедрении высоких технологий в свою экономику, хотя такое внедрение неизбежно связано с огромными материальными затратами на первоначальном этапе и потенциальной уязвимостью.

4. Отсутствие ответственности. Многие аспекты компьютерной преступности в большей степени являются следствием слабого обеспечения безопасности информации, чем результатом действий злоумышленников. Отсюда появляется необходимость расширения осведомленности общества об уязвимости компьютерных систем и необходимость осуществления действенных мер безопасности.

5. Несовершенство уголовного законодательства, связанное либо с отсутствием соответствующих составов преступлений, либо со сложностью толкования и применения норм, что ограничивает действия правоохранительных органов.

6. Несогласованность существующих законов как на международном, так и на национальном уровнях.

7. Отсутствие международных соглашений по процедурным вопросам, что самым серьезным образом влияет на нормальное функционирование органов уголовной юстиции.

8. Неэффективность гражданского законодательства, которое должно дополнять уголовные санкции.

9. Обслуживающие организации, поставщики и персонал в компьютерной и телекоммуникационной промышленности далеко не всегда проникнуты чувством ответственности перед покупателями и пользователями.

10. Система международных стандартов в области компьютерной техники, связи и информационной безопасности не успевает за требованиями времени.

11. Пользователи систем передачи и обработки данных как в частном, так и в государственном секторах не проявляют должной бдительности при обеспечении информационной безопасности.

12. При реализации новых технологических достижений не всегда соблюдаются права личности, допускаются нарушения этических и правовых концепций.

Т. П. Кесареева объединяет причины компьютерной преступности в следующие группы: политические, экономические, правовые, нравственно-психологические, неподготовленность правоохранительных органов к борьбе с новыми видами преступлений, самодетерминация, недостатки социального контроля[91, с. 122].

По результатам опроса, проведенного В. Ю. Максимовым среди сотрудников органов внутренних дел, в числе причин, более всего влияющих на данный вид преступности, экономические факторы назвали 87 % респондентов, социальные — 35 %, правовые — 30 %.. Среди секторов экономики, наиболее подверженных таким посягательствам, 81 % опрошенных назвали банковский и 53 % — финансовый сектора[92, с. 19-20].

Признавая криминогенность перечисленных факторов, отметим, что они не могут являться непосредственными причинами преступного поведения. Действительно, указанные обстоятельства в равной мере воздействуют на значительные социальные группы, однако далеко не все их представители совершают преступления. Автор придерживается концепции деформации сознания, вызываемой индивидуальным для каждого субъекта комплексом факторов, которая, в свою очередь, и детерминирует преступное поведение[90, с. 94-97]

Еще Ч. Беккариа отмечал, что «одно из самых действенных средств, сдерживающих преступления, заключается не в жестокости наказаний, а в их неизбежности и, следовательно, в бдительности властей»[93, с. 123-124]. Однако сверхвысокий уровень латентности умышленных преступлений в сфере компьютерной информации — явное подтверждение безнаказанности лиц, их совершивших.

Низкий уровень специальной подготовки сотрудников правоохранительных органов, их недостаточная активность в борьбе с преступлениями в сфере компьютерной информации и игнорирование общественной опасности данной категории преступлений со стороны порождают у лиц с неустойчивым уровнем правосознания ощущение полной безнаказанности и провоцируют их к совершению преступлений.

В.Б. Вехов выделяет семь основных условий, способствующих совершению компьютерных преступлений:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) отсутствие контроля за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;

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, 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, ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации[27, с. 114].

Также к основным детерминантам киберпреступности следует отнести некачественные услуги и приложения, предоставляемые гражданам и частным организациям в рамках «электронного правительства», в том числе машиночитаемые открытые данные, могут привести к нарушению прав и законных интересов граждан.

Отклонения от установленных требований технических стандартов, вызванные низким уровнем производственной и эксплуатационной культуры, небрежность и халатность со стороны заказчиков и разработчиков решений на этапе создания, принцип остаточного финансирования обеспечения информационных систем системами защиты информации и контроля защищенности несут в себе высокие риски технологических сбоев.

Несвоевременное устранение владельцами информационных систем уязвимостей в программном обеспечении существенно увеличивает угрозы несанкционированного доступа.

Объем данных, обрабатываемых в государственном и частном секторах, растет, что приводит к необходимости выработки новых форм их хранения. В тоже время, такие формы хранения данных как облачное хранилище или использование онлайн-сервисов часто основываются операторами и поставщиками услуг на непрозрачных или не стандартизованных решениях, в том числе с точки зрения безопасности данных. При этом гармонизированные стандарты значительно отличаются от первоисточника из-за низкого качества их перевода и адаптации.

Ситуация усугубляется возможностью намеренного внедрения в программное обеспечение и телекоммуникационное оборудование не декларируемых функций (так называемых «бэкдоров»), которые не всегда могут быть выявлены на этапе сертификации, устранения уязвимостей в процессе эксплуатации или распознаны антивирусными программами и потому могут быть использованы для нарушения работы информационных систем и сетей телекоммуникаций.

Транснациональный и трансграничный характер многих продуктов ИКТ и международная связанность сетей телекоммуникаций общего пользования используются преступностью в целях совершения противоправных действий в отношении пользователей и операторов ИКТ-услуг и владельцев Интернет-ресурсов, размещенных в национальном сегменте, а также информационных систем, взаимодействующих с Интернетом.

Высокая латентность и зачастую международный характер таких преступлений повышают их общественную опасность. Ситуация усугубляется укоренившимися в обществе стереотипами о безнаказанности так называемой «киберпреступности», ненужности принимаемых государством мер по укреплению сферы безопасного использования ИКТ, ограниченными возможностями органов правопорядка по привлечению к ответственности виновных в совершении высокотехнологичных преступлений, несмотря на развитые уголовно-правовые институты информационной безопасности.

Нагнетаемая отдельными странами милитаризация сферы ИКТ, трудности в доказывании причастности государств к использованию ИКТ в нарушение принципов международного права, вызванные в значительной степени стихийно сложившимся характером существующей международной системы управления Интернетом, сохраняющийся цифровой разрыв между странами препятствует формированию в мировом сообществе надежных международно-правовых инструментов предотвращения военного использования достижений в сфере информатизации и телекоммуникаций.

При этом по своей сути арсенал, используемый в военных целях, не отличается от арсенала программно-технических средств, используемых киберпреступностью, о чем свидетельствуют массовые случаи использования ИКТ в разведывательных, подрывных и иных целях, угрожающих поддержанию международного мира и безопасности.

Следует отметить, что причины и условия, способствующие совершению преступлений, во многом создают сами потерпевшие, имеет место неосмотрительность со стороны потерпевших, допускающих посторонних к своим информационным системам без предварительной защиты информации.

Как правило, используемое программное обеспечение не обладает высокой степенью защищенности от неправомерного доступа, что позволяет перехватывать данные и использовать полученную информацию в неправомерных целях.

Вместе с тем, согласно исследованиям В. А. Бессонова, 16,6 % респондентов утверждают, что совершение преступлений в сфере компьютерной информации возможно без упущений со стороны потерпевших. Как показывают исследования В. А. Бессонова, у 82,3 % людей хранящаяся в чужом компьютере информация вызывает любопытство и желание с ней ознакомиться. Отмечая данный факт как одну из составляющих причинного комплекса, вряд ли можно согласиться с мнением автора, предлагающего ввести понятие «виктимность компьютера». Виктимность — это исключительно личностное свойство, присущее только человеку. Можно вести речь о виктимности владельца компьютера, но никак не хранящейся в нем информации и тем более самого компьютера. Последний в силу своих качеств допустимо рассматривать лишь как привлекательный для преступников предмет либо как источник повышенной опасности[94, с. 121-133].

В комплексе причин компьютерной преступности одними из основных остаются экономические факторы.

Так, исследуя причины и условия совершения преступлений, предусмотренных ст. 205 УК РК, суды, в частности, отмечали превышение стоимости лицензионного программного обеспечения в десятки, а порой и в сотни раз над стоимостью контрафакта и соответственно высокий спрос населения именно на контрафакт. По ряду дел лица, привлекаемые к ответственности, признавались, что материалы для записи скачивали из сети Интернет.

Основываясь на результатах анализа статистических данных Министерства внутренних дел РК, судебной практики, а также специализированной литературы, можно выделить основные детерминанты преступности в сфере компьютерной информации: информационно-технологическое оборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных;

реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием компьютерной техники; низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности; ненадлежащее отношение к вопросу обеспечения информационной безопасности; низкий уровень программно-технических средств защиты информации; небрежность в обеспечении конфиденциальности информации.

Таким образом, основными причинами совершения преступлений в сфере информатизации и связи следует отнести такие причины как: низкая правовая грамотность населения, работников сферы информационно-коммуникационных технологий и руководителей организаций по вопросам информационной безопасности; нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере информационно-коммуникационных технологий установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме; непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно-коммуникационной инфраструктуры; действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово-банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно-коммуникационных услуг; деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Республики Казахстан, путем оказания разведывательного и подрывного воздействия на информационно-коммуникационную инфраструктуру.

## 3.2 Меры борьбы с уголовными правонарушениями в сфере информатизации и связи

Современный мир характеризуется динамичными глобальными процессами и трансформацией системы международных отношений. В условиях интеграции и укрепления экономических и политических позиций государств совершенствуются механизмы многостороннего управления, в которых все большую роль играют информационные факторы. Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность

функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества.

Вместе с тем технологическая эволюция одновременно с позитивом порождает новые проблемы и угрозы информационной безопасности государств, усугубляя существующие. В обстановке глобальной конкуренции информационное давление становится действенным и эффективным методом решения межгосударственных конфликтов. Все интенсивнее используются возможности глобальных информационно-коммуникационных сетей экстремистскими и террористическими организациями для пропаганды и популяризации своей идеологии, распространения радикальных идей, вовлечения все большего числа единомышленников и их обучения, поддержания контактов и финансирования. Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности. Организованные транснациональные преступные группы все активнее используют современные информационно-коммуникационные технологии в криминальных целях. Меняется динамика уголовных правонарушений в сфере информатизации и связи - для нее характерна устойчивая тенденция роста.

При этом, несмотря на увеличение зарегистрированных преступлений с использованием современных информационно-коммуникационных технологий, официальная статистика не отражает объективную картину распространения киберпреступлений, показывая лишь незначительную часть реально совершенных. Особенность киберпреступлений заключается в их высокой латентности, появлении новых, изощренных способов совершения преступлений, доказательство которых сильно затруднено из-за отсутствия необходимых правовых, организационных и технических инструментов. Поэтому борьба с киберпреступностью обусловливает потребность соответствующего оперативного реагирования, совместных скоординированных действий спецслужб и правоохранительных органов государств. В этой связи «вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью»[95, с. 28-33], остро стоит на повестке дня не только в Казахстане, но ряде других государств.

Правовой основой обеспечения политики государства по защите информационной безопасности в Республике Казахстан выступает Конституция Республики Казахстан от 30 августа 1995 г. В п.3 ст. 18 Конституции закреплена обязанность государственных органов,

общественных объединений, должностных лиц и средств массовой информации обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации. В п.2 ст. 20 Конституции Республики Казахстан указывается, что каждый имеет право свободно получать и распространять информацию любым, не запрещенным законом способом. Перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом[96].

В соответствии со ст. 4 п. 5 Закона Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» информационная безопасность относится к видам национальной безопасности. В соответствии с данным законом 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 [64].

Государственная политика в области защиты информационной безопасности начата в 1998-2011 годах. В указанный период были приняты основные законы – ЗРК от 15 марта 1999 года N 349-1 «О государственных секретах», ЗРК от 23 июля 1999 года № 451-I «О средствах массовой информации», ЗРК от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи», ЗРК от 5 июля 2004 года N 567 «О связи», ЗРК от 11 января 2007 года № 214 «О лицензировании», ЗРК от 11 января 2007 года № 217 «Об информатизации».

Особое место в обеспечении информационной безопасности Республики Казахстан занимают Концепции информационной безопасности Республики Казахстан. Первая «Концепция информационной безопасности Республики Казахстан» была принята указом Президента Республики Казахстан от 10 октября 2006 года № 199, вторая «Концепция информационной безопасности Республики Казахстан до 2016 года» была принята указом Президента Республики Казахстан от 14 ноября 2011 г. N 174, третья «Концепция кибербезопасности «Киберщит Казахстана» утверждена постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407.

Концепции определяют государственную политику, перспективы деятельности государственных органов в области обеспечения информационной безопасности, и разработаны в соответствии с Конституцией Республики Казахстан и Законами Республики Казахстан.

Вся структура правового регулирования отношений в области информационной безопасности акцентирует внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности.

В законодательстве об информационной безопасности можно выделить три основных направлений правовой защиты объектов в информационной сфере:

- защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации;

- защита информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц;

- защита информационных прав и свобод (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; право собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в условиях информатизации[10, с. 113].

Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием состоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества. Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности. Меняется динамика уголовных правонарушении в сфере информатизации и связи, для нее характерна устойчивая тенденция роста. С 2008-2018 гг. в Казахстане было зафиксировано 946 уголовных правонарушений в сфере информатизации и связи.[4].

В соответствии с постановлением Правительства Республики Казахстан от 11 сентября 2002 года № 993 уполномоченным государственным органом по защите государственных секретов и обеспечению информационной безопасности является Канцелярия Премьер-Министра Республики Казахстан[97]. Также вопросы информационной безопасности находятся в ведении органов национальной безопасности, осуществляющих общую межведомственную координацию деятельности по обеспечению национальной безопасности.

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.

В соответствии с постановлением Правительства Республики Казахстан от 17 апреля 2008 года №362 создано Республиканское государственное предприятие на праве хозяйственного ведения «Центр технического сопровождения и анализа в области телекоммуникаций» Агентства Республики Казахстан по информатизации и связи, в дальнейшем в соответствии с постановлением Правительства Республики Казахстан от 27 июля 2017 года №457 «О некоторых вопросах государственной технической службы» Предприятие переименовано в Республиканское государственное предприятие на праве хозяйственного ведения «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан.

Основная цель данного предприятия является осуществление отдельных видов деятельности в сферах информатизации и обеспечения информационной безопасности.

Предприятие осуществляет следующие виды деятельности, отнесенные к государственной монополии:

в сфере информатизации:

1) сопровождение единого шлюза доступа к Интернету и единого шлюза электронной почты «электронного правительства»;

2) испытание объектов информатизации «электронного правительства» на соответствие требованиям информационной безопасности;

3) согласование задания на проектирование информационно-коммуникационной услуги на соответствие требованиям информационной безопасности;

4) экспертизу инвестиционного предложения и финансово-экономического обоснования бюджетных инвестиций и технического задания на создание и развитие объекта информатизации «электронного правительства» на соответствие требованиям информационной безопасности;

5) мониторинг отказоустойчивости серверов доменных имён, обслуживающих казахстанские доменные имена верхнего уровня;

6) сопровождение разработки планов адресации и нумерации сетей телекоммуникаций операторов связи, осуществляющих деятельность на территории Республики Казахстан;

7) работы по разработке средств защиты информации в части обнаружения, анализа и предотвращения угроз информационной безопасности для обеспечения устойчивого функционирования информационных систем и сетей телекоммуникаций государственных органов;

8) реализацию следующих задач и функций Национального координационного центра информационной безопасности:

- содействие собственникам, владельцам и пользователям объектов информатизации в вопросах безопасного использования информационно-коммуникационных технологий;

- обеспечение взаимодействия оперативных центров информационной безопасности по вопросам мониторинга обеспечения информационной безопасности объектов информатизации;

- осуществление сбора, анализа и обобщения информации оперативных центров информационной безопасности об инцидентах информационной безопасности на объектах информационно-коммуникационной инфраструктуры «электронного правительства» и других критически важных объектах информационно-коммуникационной инфраструктуры;

- осуществление технического сопровождения информационной системы Национального координационного центра информационной безопасности;

- участие в разработке порядка обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами информационной безопасности и Национальным координационным центром информационной безопасности;

- в случаях получения информации об инцидентах информационной безопасности на объектах информатизации незамедлительное информирование органов национальной безопасности Республики Казахстан;

- осуществление межотраслевой координации по вопросам мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», казахстанского сегмента Интернета, а также критически важных объектов информационно-коммуникационной инфраструктуры, реагирования на инциденты информационной безопасности с проведением совместных мероприятий по обеспечению информационной безопасности в порядке, определяемом законодательством Республики Казахстан;

- осуществление мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» посредством системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности;

- осуществление мониторинга событий информационной безопасности объектов информатизации государственных органов;

- создание и обеспечение функционирования единой национальной резервной платформы хранения электронных информационных ресурсов, установление периодичности резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры в порядке, определяемом уполномоченным органом в сфере обеспечения информационной безопасности;

- осуществление организационного и технического сопровождения системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности;

- осуществление мероприятий по выявлению, пресечению и исследованию угроз и инцидентов информационной безопасности на объектах информатизации «электронного правительства» и формирование рекомендаций по их устранению или предотвращению;

- осуществление координации мероприятий по обеспечению информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, а также реагированию на инциденты информационной безопасности;

в сфере обеспечения информационной безопасности:

9) техническое сопровождение системы централизованного управления сетями телекоммуникаций Республики Казахстан, а также международных точек стыка;

10) организацию и техническое сопровождение точек обмена интернет-трафиком операторов междугородной и международной связи на территории

Республики Казахстан, а также присоединение сетей операторов междугородной и международной связи к точке обмена интернет-трафиком;

11) организацию и техническое сопровождение удостоверяющего центра информационной безопасности [98].

С учетом обусловленной многократным увеличением количества пользователей национальной информационной инфраструктуры, возрастающим количеством компьютерных инцидентов, на основе международного опыта, в 2010 году создана Казахстанская Служба реагирования на компьютерные инциденты (далее - KZ-CERT), на которую возложены функции национального и международного координатора в сфере безопасного использования информационных технологий.

Служба реагирования на компьютерные инциденты (далее –KZ-CERT) – это единый центр для пользователей национальных информационных систем и сегмента сети Интернет, обеспечивающий сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз компьютерной безопасности.

Основная задача KZ-CERT - снижение уровня угроз информационной безопасности для пользователей казахстанского сегмента сети Интернет. В этой связи KZ-CERT оказывает содействие казахстанским и зарубежным юридическим и физическим лицам при выявлении, предупреждении и пресечении противоправной деятельности, имеющей отношение к сетевым ресурсам казахстанского сегмента сети Интернет.

KZ-CERT осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории РК. В компетенцию службы входит обработка следующих компьютерных инцидентов с целью их выявления и нейтрализации:

- атаки на узлы сетевой инфраструктуры и серверные ресурсы, с целью нарушения их работоспособности (DoS (Denial of Service) и DDoS) и конфиденциальности информации;
- несанкционированный доступ к информационным ресурсам;
- распространение вредоносного программного обеспечения, незатребованной корреспонденции (спам);
- сканирование национальных информационных сетей и хостов;
- подбор и захват паролей и другой аутентификационной информации;
- взлом систем защиты информационных сетей, в том числе с внедрением вредоносных программ (сниффер, rootkit, keylogger и т.д.).

KZ-CERT не несет ответственности за возможные ошибки, ущерб и другие виды прямых или косвенных потерь, произошедших по вине пользователей в результате неправильного истолкования полученной от KZ-CERT информации.

Действуя в рамках нормативной правовой базы РК, KZ-CERT не уполномочен заниматься решением вопросов, находящихся в ведении правоохранительных органов.

KZ-CERT осуществляет:

- мониторинг и выявление механизмов и интернет-ресурсов, нарушающих законодательство РК;
- разработку рекомендаций пользователям по защите интересов личности, общества и государства в информационной сфере;
- оказание консультативных услуг по вопросам обеспечения информационной безопасности;
- оперативный прием сообщений о хакерских атаках.

KZ-CERT занимается:

- координацией действий подразделений компьютерной безопасности государственных органов, операторов связи, а также других субъектов национальной информационной инфраструктуры по вопросам предотвращения правонарушений в области использования компьютерных и информационных технологий;
- сбором, анализом и накоплением информации о современных угрозах компьютерной безопасности и об эффективности применяемых средств защиты.

В настоящее время KZ-CERT выступает в качестве Центра реагирования на обращения пользователей национальных информационных систем, а также сети Интернет, которым необходимо оказание содействия в предотвращении компьютерных инцидентов, в обращении к казахстанским интернет - провайдерам и официальным государственным структурам, осуществляющим реагирование на компьютерные инциденты, обеспечивающим консультативную и техническую поддержку в выявлении, устранении, оценке, прогнозировании и предотвращении угроз информационной безопасности [99].

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с уголовными правонарушениями в сфере информатизации и связи. Помимо этого необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с уголовными правонарушениями в сфере информатизации и связи.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, а также разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного

оружия и совершенствования нормативной правовой базы в данной сфере. Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [100, с. 47].

Одним из актуальных вопросов обеспечения безопасности информационного пространства является подготовка отвечающих современным требованиям специалистов в этой области. В целях развития сферы информационной безопасности и электронной промышленности Постановлением Правительства Республики Казахстан от 26 апреля 2018 года № 221 национальным институтом развития в сфере обеспечения информационной безопасности определено РГП на ПХВ «Институт информационных и вычислительных технологий» Комитета науки Министерства образования и науки РК.

Основными задачами национального института развития в сфере обеспечения информационной безопасности являются: участие в реализации государственной политики, разработка документов по стандартизации, осуществление научно-технической деятельности, проведение научно-технической экспертизы проектов, осуществление подготовки, переподготовки и повышения квалификации в сфере информационной безопасности [101].

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с уголовными правонарушениями в сфере информатизации и связи. Помимо этого необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с уголовными правонарушениями в сфере информатизации и связи.

Для эффективной работы по противодействию уголовных правонарушений в сфере информатизации и связи требуется правовое обеспечение информационной сферы на государственном уровне, в связи, с чем следует обратить особое внимание на правовые механизмы, регулирующие:

1) информационные правоотношения, возникающие при поиске, получении, потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг;

2) процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг;

3) информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры.

Недостаточная согласованность используемых правовых механизмов, фрагментарность деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточная эффективность, противоречивость правовых норм, характерная для нынешнего состояния правового обеспечения противодействия уголовным правонарушениям в сфере информатизации и связи, в совокупности создают серьезную угрозу информационной безопасности государства.

Анализ показывает, что национальное уголовное законодательство государств в сфере ответственности за уголовные правонарушения в сфере информатизации и связи характеризуется относительным разнообразием. Развитие и изменение национального законодательства по противодействию уголовным правонарушениям в сфере информатизации и связи в вышеназванных государствах обусловлены появлением и тенденциями развития уголовных правонарушений в сфере информатизации и связи, и при подробном анализе обнаруживаются лишь некоторые закономерности. Совершенствование информационных технологий и проникновение их во все сферы человеческой жизнедеятельности ведет к возникновению новых форм преступных посягательств и криминализации новых деяний, а это, в свою очередь, к необходимости выработки эффективных мер борьбы с ними, внесению изменений в уже существующее уголовное законодательство и принятию новых норм.

Бесспорно, эффективное международное сотрудничество в борьбе с уголовными правонарушениями в сфере информатизации и связи невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой - уголовной ответственности не предусмотрено. Отсутствие единообразия в национальном уголовном законодательстве стран может негативно отразиться на развитии методов эффективной борьбы с уголовными правонарушениями в сфере информатизации и связи - явлением, для которого не существует государственных границ. Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются преступниками, орудующими в сфере информатизации и связи, независимо от юрисдикции государств, с помощью компьютера и доступа в Интернет. Эффективное противостояние уголовным правонарушениям в сфере информатизации и связи, учитывая ее трансграничный характер, невозможно, если расследование преступлений, выдача правонарушителей, их преследование в суде затруднены или вообще неосуществимы из- за «нестыковок» в национальном уголовном законодательстве отдельных стран. Фактически, эти различия ограждают преступников в сфере информатизации и связи от преследования, являясь своеобразным «барьером», позволяют уйти от ответственности, оставляя безнаказанными их деяния.

Вследствие этого государства, прилагающие усилия для защиты своих граждан от преступников совершающих уголовные правонарушения в сфере

информатизации и связи, тратят их впустую. С другой стороны, из-за различий уголовноправового регулирования отношений в сфере информационных технологий лица, соблюдающие законы своего государства, могут подвергнуться уголовному преследованию в другом. Такая ситуация диктует потребность выработки международной стратегии борьбы с уголовными правонарушениями в сфере информатизации и связи и унификации национальных законодательств в области уголовно-правового регулирования отношений в сфере информационных технологий.

Приходится констатировать, что законодательное регулирование анализируемых отношений в уголовно-правовой сфере отстает от стремительного развития компьютерных технологий. В настоящее время ответственность за уголовные правонарушения в сфере информатизации и связи в уголовном законодательстве не отражает глобальных перемен в непрерывном, стремительном процессе информационного развития человечества. Уголовное законодательство недостаточно эффективно регулирует отношения, складывающиеся при совершении уголовных правонарушений в сфере информатизации и связи, вследствие чего не реализуются его охранительные и предупредительные функции. Уголовная ответственность в законодательстве Казахстана, как и в законодательстве некоторых государств СНГ, предусмотрена за компьютерные преступления, т. е. за преступления, которые совершаются в отношении компьютеров и компьютерной информации, при этом деяния, которые совершаются с их использованием и посягают на другие объекты уголовно-правовой охраны, остаются вне сферы уголовной ответственности. В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности требуют криминализации ряда общественно опасных деяний и самостоятельной охраны названных отношений в отдельной главе Особенной части Уголовного кодекса. Таким образом в целях борьбы с уголовными правонарушениями в сфере информатизации и связи вводятся законодательные акты, которые будут заслоном от совершения подобных уголовных правонарушений. Для обеспечения государственных органов полной, достоверной и своевременной информацией требуется принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, разработка средств защиты информации, совершенствования нормативной правовой базы в данной сфере. Так, в новом Уголовном кодексе от 3 июля 2014 года предусмотрена новая глава 7 «Уголовные правонарушения в сфере информатизации и связи». В данной главе содержится 9 составов преступлений, за которые предусмотрена уголовная ответственность. А именно ст. 205 УК РК «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», ст. 206 УК РК «Неправомерные уничтожение или модификация информации», ст. 207 УК РК «Нарушение работы информационной системы или сетей», ст. 208 УК РК

«Неправомерное завладение информацией», ст. 209 УК РК «Принуждение к передаче информации», ст. 210 УК РК «Создание, использование или распространение вредоносных», ст. 211 УК РК «Неправомерное распространение электронных информационных ресурсов ограниченного доступа», ст. 212 УК РК «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели», ст. 213 УК РК «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства».

Во многих странах мира в целях пресечения факта информационного преступления в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль так называемого хакера, то есть преступника в сфере компьютерной информации и техники, который позволяет выявить уровень его квалификации и технической подготовки. 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. Подобная практика активно используется в США, Европе и других странах, где уголовные правонарушения в сфере информатизации и связи широко развиваются. Некоторые ученые считают, что налаживание подобной практики и в нашей стране, где уголовные правонарушения в сфере информатизации и связи пока неразвиты, позволит еще в зачаточной форме уничтожить основы уголовных правонарушений в сфере информатизации и связи. Для этого необходимо активизировать потребность международного сотрудничества. Но ввиду того, что в современных условиях значительная часть средств борьбы с уголовными правонарушениями в сфере информатизации и связи, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

Для обеспечения государственных органов полной, достоверной и своевременной информацией требуются принятие обоснованных решений, в том числе для защиты государственных информационных ресурсов, а также разработка отечественных средств защиты информации и системы подтверждения соответствия импортируемых технических средств установленным требованиям, а также дальнейшая проработка вопросов противодействия техническим разведкам, защиты от информационного оружия и совершенствования нормативной правовой базы в данной сфере.

Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации[102, с. 47].

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, меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые.

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

К организационным мерам отнесем охрану вычислительного 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 вычислительного 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 правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют, или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашения.

К мерам предупреждения компьютерных преступлений также относится защита информации (данных).

Защита информации (данных) представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Защита данных в сети. При рассмотрении проблем защиты данных в сети, прежде всего, возникает вопрос о классификации сбоев и нарушений, прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных «угроз» можно выделить:

1. Сбои оборудования: сбои кабельной системы; перебои электропитания; сбои дисковых систем; сбои систем архивации данных; сбои работы серверов, рабочих станций, сетевых карт и.т.д.

2. Потери информации из-за некорректной работы ПО: потеря или изменение данных при ошибках ПО; потери при заражении системы компьютерными вирусами.

3. Потери, связанные с несанкционированным доступом: несанкционированное копирование, уничтожение или подделка информации; ознакомление с конфиденциальной информацией, составляющей тайну посторонних лиц.

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей: случайное уничтожение или изменение данных; некорректное использование программного обеспечения.

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономно). Остановимся подробнее на первом типе, представляющем большой интерес. Наиболее распространены два алгоритма:

1) Стандарт шифрования данных DES (Data Encryption Standard) был разработан фирмой IBM в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 бит проверки на четность и требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм утвердительно решает проблему превращения конфиденциальной информации в недоступную.

2) Алгоритм RSA был изобретен Ривестом, Шамиром и Альдерманом в 1976 году и представляет собой значительный шаг в криптографии. Этот алгоритм также был принят в качестве стандарта Национальным бюро стандартов. DES, технически является симметричным алгоритмом, а RSA - асимметричным, т.е. он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрования сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает ненужными секретные соглашения о передаче ключей между корреспондентами. DES определяет длину данных и ключа в битах, а RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но становится длительнее процесс шифрования и де шифрования). Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации

ключа RSA - десятки секунд. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES - разработчики аппаратуры[103, с. 69].

Физическая защита данных. Кабельная система остается главной проблемой большинства локальных вычислительных сетей: по данным различных исследований именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим способом избавить себя от "головной боли" по поводу неисправностей прокладки кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охраны систем. К структурированным кабельным системам относятся, например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании DIGITAL, кабельная система корпорации IBM.

Системы электроснабжения. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии является установка источников бесперебойного питания, Различные по своим технологическим и потребительским характеристикам, подобные устройства могут обеспечить питание по всей локальной сети или отдельных компьютеров в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функцию и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и др. - оснащены собственными дублированными системами электропитания[104, с. 163].

За рубежом корпорации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной из них, электроснабжение осуществляется с резервной подстанции.

Выбор надежного оборудования. Важнейшим фактором обеспечения надежности работы системы является подбор соответствующего оборудования. Практически все отечественные системные интеграторы рекомендуют заказчикам применять технику известных компаний, так называемый brand name. Такое оборудование проходит серьезный выходной контроль изготовителя, имеет высокий уровень совместимости и длительный срок гарантийного обслуживания[105, с. 73].

Системы архивирования и дублирования информации. Несмотря на очевидность этой процедуры и ее относительную несложность, в некоторых

организациях она производится недостаточно часто или игнорируется вообще. Опыт показывает: если содержимое системы копируется еженедельно в пятницу вечером, то все неприятности случаются в пятницу же, но в районе обеда. Резервное копирование должно сопровождаться целым рядом не менее очевидных организационных мероприятий. Носители - ленты или магнитооптические диски - должны храниться за пределами серверной комнаты. Поскольку носитель используется многократно, нужно знать стандарты на число допустимых перезаписей и тесты, позволяющие определить степень его изношенности. Широкий выбор устройств для копирования также может сыграть злую шутку с пользователями: о совместимости этих устройств следует позаботиться до того, как одно из них выйдет из строя.

Большое значение для безопасности информационной системы имеют такие акции системного администратора, как своевременное обновление программного обеспечения. Как правило, при выходе новой версии немедленно становится общедоступной информация об ошибках предыдущей (в том числе о недостатках системы защиты). Если обновление не было вовремя произведено, вероятность взлома системы многократно возрастает.

Новые информационные технологии должны быть не только орудием, средством совершения преступлений нарушителями закона, но и должны стать эффективным наступательным инструментом в борьбе с различными угрозами и в том числе преступностью во всех ее проявлениях, в связи с чем нужно привлекать в государственные структуры высококвалифицированных специалистов по борьбе с компьютерной преступностью.

## Заключение

В законодательстве об информационной безопасности можно выделить три основных направлений правовой защиты объектов в информационной сфере: - защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации;

- защита информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц;

- защита информационных прав и свобод (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; право собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в условиях информатизации.

Несмотря на новизну компьютерных преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает.

Проведенный анализ показал, что законодательство об уголовной ответственности за уголовные правонарушения в сфере информатизации и связи и отличается определенным своеобразием; не во всех государствах бывшего Союза ССР законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных информации и технологий. Многие европейские государства и США повели решительную борьбу с уголовными правонарушениями в сфере информатизации и связи и с момента их появления в жизни общества, следовательно, правовая регламентация уголовной ответственности за совершение компьютерных преступлений отличается очень высокой степенью детализации и высоким уровнем юридической техники.

Очевидно, что национальному законодателю следует оценить опыт зарубежных государств и выяснить пригодность вышеупомянутых правовых инструментов для защиты компьютерной информации.

К информационным системам, выступающим предметом рассматриваемого уголовного правонарушения, следует относить:

- информационные системы, содержащие государственные электронные информационные ресурсы, отнесенные к государственным секретам;

- информационные системы, содержащие конфиденциальные электронные информационные ресурсы, в том числе содержащие персональные данные, охраняемую законом тайну;

- иные информационные системы, доступ к которым ограничен их собственником или владельцем.

Основываясь на результатах анализа статистических данных Министерства внутренних дел РК, судебной практики, а также специализированной литературы, можно выделить основные детерминанты преступности в сфере компьютерной информации:

1) информационно-технологическое оборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных;

2) реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием компьютерной техники;

3) низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности;

4) ненадлежащее отношение к вопросу обеспечения информационной безопасности;

5) низкий уровень программно-технических средств защиты информации;

6) небрежность в обеспечении конфиденциальности информации.

Для эффективной работы по противодействию уголовных правонарушений в сфере информатизации и связи требуется правовое обеспечение информационной сферы на государственном уровне, в связи, с чем следует обратить особое внимание на правовые механизмы, регулирующие:

1) информационные правоотношения, возникающие при поиске, получении, потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг;

2) процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг;

3) информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры.

Новые информационные технологии должны быть не только орудием, средством совершения преступлений нарушителями закона, но и должны

стать эффективным наступательным инструментом в борьбе с различными угрозами и в том числе преступностью во всех ее проявлениях, в связи, с чем нужно привлекать в государственные структуры высококвалифицированных специалистов по борьбе с компьютерной преступностью.

Большое значение для безопасности информационной системы имеют такие акции системного администратора, как своевременное обновление программного обеспечения. Как правило, при выходе новой версии немедленно становится общедоступной информация об ошибках предыдущей (в том числе о недостатках системы защиты). Если обновление не было вовремя произведено, вероятность взлома системы многократно возрастает.

Новые информационные технологии должны быть не только орудием, средством совершения преступлений нарушителями закона, но и должны стать эффективным наступательным инструментом в борьбе с различными угрозами и в том числе преступностью во всех ее проявлениях, в связи с чем нужно привлекать в государственные структуры высококвалифицированных специалистов по борьбе с компьютерной преступностью.

Список использованных источников

1 Послание Президента Республики Казахстан Н.Назарбаева народу Казахстана. 17 января 2014 г. « Казахстанский путь – 2050: Единая цель, единые интересы, единое будущее» // https://www.akorda.kz/

2 Послание Президента Республики Казахстан Н.Назарбаева народу Казахстана. 31 января 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность» // https://www.akorda.kz/

3 Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 Об утверждении Концепции кибербезопасности "Киберщит Казахстана" // http://adilet.zan.kz/

4 Статистические сведения о состоянии преступности в Республике Казахстан // http://service.pravstat.kz

5 Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешнеполитические перспективы и новые концепты международной стратегии Казахстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан — Лидера Нации. — 2012. — 12 марта. // iwep.kz/index

6 Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002.

7 Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан // knb.kz.

8 Послание Президента страны народу Казахстана 1997 года «Казахстан – 2030 Процветание, безопасность и улучшение благосостояния всех казахстанцев» // http://adilet.zan.kz.

9 Исабаев Б. Обеспечение информационной безопасности Республики Казахстан: политико-правовой аспект / Б. Исабаев // Адам элемі [Электронный ресурс]. - 2011.№1(47).

10 Нурпеисова А.К. Правовые аспекты информационной безопасности в Республике Казахстан / А.К. Нурпеисова // Вестник Карагандинского юридического института МВД РК - 2011. - № 3.

11 О подписании Соглашения между правительствами государств-членов Шанхайской организации в области обеспечения международной информационной безопасности: Постановление Правительства Республики Казахстан, 12 июня 2009 г., № 902 // http://adilet.zan.kz / Информационно-правовая система нормативных правовых актов Республики Казахстан.

12 О подписании Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности: Постановление Правительства Республики Казахстан, 28 мая 2012 г., № 692 // http://adilet.zan.kz. / Информационно-

правовая система нормативных правовых актов Республики Казахстан. - Республика Казахстан.

13 Об утверждении Соглашения между Правительством Республики Казахстан и Правительством Республики Беларусь о сотрудничестве в области защиты информации: Постановление Правительства Республики Казахстан, 6 января 2006 г., № 10 // http://adilet.zan.kz./ Информационно-правовая система нормативных правовых актов Республики Казахстан. - Республика Казахстан.

14 Об утверждении Соглашения между Правительством Республики Казахстан и Правительством Российской Федерации о взаимной защите секретной информации: Постановление Правительства Республики Казахстан , 9 сентября 2004 г., № 947 // http://adilet.zan.kz.

15 Конституция Республики Казахстан, 30 августа 1995 г. // http://adilet.zan.kz.

16 Гражданский кодекс Республики Казахстан (Особенная часть), 1 июля 1999 г., № 409 // http://adilet.zan.kz.

17 Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V // http://adilet.zan.kz.

18 Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V // http://adilet.zan.kz.

19 Кодекс Республики Казахстан от 26 декабря 2017 года № 123-VI «О таможенном регулировании в Республике Казахстан» // http://adilet.zan.kz.

20 Уголовный кодекс Республики Казахстан от 3 июля 2014 г., №226-V // http://adilet.zan.kz.

21 О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей: Закон Республики Казахстан, 10 июля 2009 г., № 178-IV // http://adilet.zan.kz.

22 Указ Президента Республики Казахстан от 10 октября 2006 года № 199 «О Концепции информационной безопасности Республики Казахстан» // http://adilet.zan.kz.

23 Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года» // http://adilet.zan.kz.

24 Максимов В.Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Книжное издательство, 1999.

25 Данные комитета по правовой статистике и специальным учетам за период с 1995-2007 гг.

26 Дремин В.Н. Глобализация информационных систем как фактор глобализации преступности. — Киев, 2002. Вып. 1. С.36-40.

27 Вехов В.Б. Компьютерные преступления: способы совершения, методы расследования. — М., 1996. — с.

28 Правовая информатика и кибернетика: Учебник для ВУЗов / Под ред. Н.С. Полевого. — М., 1993. — с.

29 Скоромников К.С. Неправомерный доступ к компьютерной информации и его расследование // Прокурорский надзор и следственная практика. — 1998. — № 1. — С.165-169.

30 Комментарий к Уголовному кодекса РФ / Отв. ред. д-р юрид. наук, проф. А.В. Наумов. — М., 1996. — 876с.

31 Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Автореф. дис. … канд. юрид. наук. — М., 1998. — с.

32 Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью (уголовно-правовые и криминологические аспекты): Дис. … канд. юрид. наук. — М., 2006. — 225 с.

33 Шахов А. В. Электронные взломщики — преступники под маской романтиков // Оборудование, системы, технологии. 1997. Март—апрель. С. 89.

34 Большой юридический словарь / Под ред. А. . Сухарева. — М.: ИНФРА-М, 1997. — с.

35 Курс советской криминологии. — М., 1985. Т. 1. — с.

36 Более 30 тысяч сайтов обучают компьютерному взлому // www/ cnews/ru

37 Панфилова Е.И. Компьютерные преступления. – М., 2006.

38 Лукашук И.И., Наумов А.В. Международное уголовное право. – М., 1999. – С. 123.

39 Международное уголовное право / Под общ. ред. В. Н. Кудрявцева. – М., 1999.

40 Костенко Н.И. Международная уголовная юстиция. Проблемы развития. – М., 2003.

41 Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М., 1998.

42 Борчева Н.А. Компьютерное право и ответственность за компьютерные преступления за рубежом // На пути к информационному обществу: криминальный аспект: Сборник статей. – М., 2002. – С. 10; 2004.

43 Уголовный кодекс Республики Беларусь // www.pravo.levonevsky.org/kodeksby

44 Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – Минск, 2002.

45 Уголовный кодекс Республики Таджикистан // http://www.crime.vl.ru/index.php?p=1323&more=1&c=1&tb=1&pb=1

46 Уголовный кодекс Украины // www.crime.org.ua

47 «О внесении изменений в Уголовный кодекс Украины относительно ответственности за незаконное вмешательство в работу сетей электросвязи» (№ 908-IV от 5 июня 2003 года).

48 Уголовный кодекс Республики Узбекистан //http://www.kodeks.uz/ugolkod
49 Уголовный кодекс Республики Кыргызстан //http://www.prison.memo.ru/laws.htm
50 Уголовный кодекс Республики Туркменистан //http://www.turkmenistan.gov.tm/_ru/laws/?laws=40
51 Уголовный кодекс Азербайджанской Республики //http://www.zakon.msk.su
52 Уголовный кодекс Грузии // www.urbia.gol.ge/kodeksi/59.htm
53 Уголовный кодекс Молдовы // www.yk-md.ru
54 Уголовный кодекс Армении //http://www.base.spinform.ru/
55 Уголовный кодекс Нидерландов // www.icpo.at.tut.by/crimru.htm
56 Уголовный кодекс Испании // www.icpo.at.tut.by/crimru.htm
57 Уголовный кодекс Франции // www.icpo.at.tut.by/crimru.htm
58 Туманова Л.В., Снытников А. А. Обеспечение и защита права на информацию в США. – М., 2001.
59 Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. – М., 2005.
60 Школин И. Инвесторы против пиратства // Финанс. – 2007. – № 6.
61 Малков В. Д. Криминология: учебник для вузов. Изд. 3-е. – М., 2007.
62 Крылов В.В. Информационные компьютерные преступления. – М., 1987.
63 Вассер Э. С. Преступления в предпринимательской и банковской сферах за рубежом. – М., 2005.
64 Закон Республики Казахстан: от 6 января 2012 г. № 527-IV «О национальной безопасности Республики Казахстан» // http://adilet.zan.kz.
65 Боер В. М. Информационно-правовая политика России. – СПб., 2008.
66 Вус М.А., Войтович Н.А., Гусев В.С. Россия на пороге информационного общества // Россия на пороге информационного общества. Материалы семинара 22 апреля 1997 г. - СПб.: 1997.
67 Всеобщая декларация прав человека и гражданина утв. Генеральной Ассамблеей ООН 10 декабря 1948 года // Сборник документов по международному гуманитарному праву. – М.: Проспект, 2000.
68 Ковалева Н. Н., Холодная Е. В. Комментарий к Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – М.: ООО «Новая правовая культура», 2007.
69 Панин А.А. Философия: Учебник для вузов. – М.: Проспект, 2002.
70 Юрченко И.А. Информация конфиденциального характера как предмет уголовно-правовой охраны. – М., 2000.

71 Виннер Н. Кибернетика и общество. – М., 1958.

72 Закон РК от 16 ноября 2015 года № 401-V «О доступе к информации» // http://adilet.zan.kz

73 Гурьянов К.В. Файлы CRACK как идентификационный признак совершения преступлений в сфере производства компьютерного (информационного) контрафакта // Эксперт-криминалист. – 2007. – № 3.

74 Нормативное постановление Конституционного Совета Республики Казахстан от 20 августа 2009 г. №5// http://adilet.zan.kz

75 Закон Республики Казахстан от 15 марта 1999 года N 349-1 О государственных секретах // http://adilet.zan.kz

76 Борчашвили И.Ш. Комментарий к Уголовному кодексу Республики Казахстан. Особенная часть (том 2). - Алматы: Жеті Жарғы, 2015. - 1120 с.

77 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..

78 Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. – 1998. – № 3.

79 Букалерова Л.А. Уголовно-правовая охрана официального информационного оборота. – М.: Юрлитинформ, 2006.

80 Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М., 2005.

81 Касперский Е. Компьютерные вирусы: внутри и снаружи. – М., 2006.

82 Жельников В. Криптография от папируса до компьютера. – М., 1996.

83 Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004.

84 Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. – М.: Собрание, 2004.

85 Крутских А.В. Информационный взрыв безопасности на рубеже XXI века // Международная жизнь. – 1999. – № 2.

86 Криминология / под ред. В. Н. Бурлакова, Н. М. Кропачева. СПб.: Питер, 2004.

87 Криминология: учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2-е изд., перераб. и доп. М. : Волтерс Клувер, 2005.

88 Долгова А.И. Криминология. М.: ИНФРА-М, 2002.

89 Криминология / под ред. В. Н. Бурлакова, Н. М. Кропачева. СПб.: Питер, 2004.

90 Репецкая А.Л. Криминология. Общая часть / А. Л. Репецкая, В. Я. Рыбальская. Иркутск : Изд-во ИГЭА, 1999.

91 Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук. М., 2002.

92 Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания: дис. ... канд. юрид. наук. Краснодар, 1998.

93 Беккариа Ч. О преступлениях и наказаниях. М.: ИНФРА-М, 2004.

94 Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: дис....канд. юрид. наук. Н. Новгород, 2000.

95 Протасевич А.А., Зверянская П.П. Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальского государственного университета экономики и права. - 2011. - №3.

96 Конституция Республики Казахстан, 30 августа 1995 г. // http://adilet.zan.kz

97 Постановление Правительства Республики Казахстан от 11 сентября 2002 года № 993 «Вопросы Канцелярии Премьер-Министра Республики Казахстан» http://adilet.zan.kz/

98 Интернет портал // http://sts.kz/

99 Интернет портал //http://kz-cert.kz/

100 Ахметов Е. «Киберпреступность в Казахстане» // Журнал «Законность и правовая статистика» 2009, № 2 (11).

101 Постановление Правительства Республики Казахстан от 26 апреля 2018 года № 221 «Об определении национального института развития в сфере обеспечения информационной безопасности» // http://adilet.zan.kz/

102 Ахметов Е. «Киберпреступность в Казахстане» // Журнал «Законность и правовая статистика» 2009, № 2 (11).

103 Вечерский Д.А., Шалькевич И.И. Расследование компьютерных преступлений. - Минск 2001.

104 Голубев В. Компьютерная преступность - угроза национальной безопасности // http://www.crime-research.org/library/interv2.html.

105 Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. - М., 2001.