Брестский государственный университет им. А.С.Пушкина

Кафедра уголовного и гражданского права

П Р Е С Т У П Л Е Н И Я ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации по курсу:

«УГОЛОВНОЕ ПРАВО РЕСПУБЛИКИ БЕЛАРУСЬ.
ОСОБЕННАЯ ЧАСТЬ»

Для студентов, обучающихся по специальности
«Правоведение»

*Брестский государственный университет
имени А.С. Пушкина*

2000

Методические рекомендации написаны в соответствии с новой программой по курсу «Уголовное право Республики Беларусь. Особенная часть» и ставят целью облегчить самостоятельную работу студентов при подготовке к практическим занятиям.

Методические рекомендации предназначены для студентов стационара юридического факультета и ОЗО, обучающихся по специальности «Правоведение».

Печатается по решению редакционно-издательского совета университета.

Составитель: Лосев В.В.

Рецензенты:
кандидат юридических наук, доцент Яловик В.С.,
кафедра «ЭВМ и системы» Брестского политехнического университета

Редактор: Коклюхин В.В.

Содержание

ВВЕДЕНИЕ

Появление в новом Уголовном Кодексе Республики Беларусь 1999 года раздела о преступлениях против информационной безопасности, ранее неизвестных белорусскому законодательству, ставит перед правоохранительными органами задачу раскрытия и расследования этого вида преступлений. Вместе с тем, сфера отношений вокруг компьютерной информации еще сравнительно недавно была уделом технических специалистов и многие юристы до сих в недостаточной степени владеют терминами и понятиями этой сферы.

Информационная революция фактически уже произошла. Стремление общества к созданию более совершенных и эффективных моделей своего существования, в том числе и в области применения электронной техники и информационных технологий, закономерно порождает проблемы различного характера. Создание электронно-вычислительной техники четвертого и пятого поколений с потенциально неограниченными возможностями, их широкое распространение в экономической, социальной и управленческой сферах, в военной области, появление в быту огромного количества персональных компьютеров явились не только новым свидетельством технического прогресса, но и с неизбежностью повлекли за собой и негативные последствия, связанные со злоупотреблениями при использовании средств ЭВМ, информационных технологий.

Сообщения об информационных преступлениях отрывочны. Сегодня никто в мире не имеет полной картины информационной преступности. Причина не только в том, что это совершенно новый вид преступности, но и в том, что государственные, банковские и коммерческие структуры не очень склонны афишировать последствия, причиненные информационными нападениями, и «эффективность» своих систем защиты. Этим обусловлена высокая латентность преступности в области информационных отношений.

Причиной криминализации как в российском, так и в белорусском уголовных законодательствах противоправных действий в области электронной техники и информационных технологий является их высокая общественная опасность. Как отмечает В.С. Комиссаров, эта опасность выражается в том, что такие действия «могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных, включая и жизнеобеспечивающие, объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и

необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям» [5, с.9].

В.С. Комиссаров и В.В. Крылов в своих работах, посвященных рассматриваемому виду преступлений, приводят ставшие широко известными факты совершения преступлений с помощью ЭВМ. Считается, что первым человеком, использовавшим еще в 1969 году в США возможности ЭВМ для совершения налогового преступления на сумму 620 тыс. долларов, был Альфонсе Конфессоре. В конце 70-х годов с использованием компьютерной техники из «Секьюрити пасифик бэнк» в США было похищено более 10 млн. долларов. В сентябре 1989 года к тюремному заключению был приговорен Арманд Мур, организовавший «компьютерное ограбление» чикагского банка «Ферст нэшнл бэнк». Муру и его сообщникам, среди которых были сотрудники банка, удалось с помощью подбора кода к электронной системе банка перевести из Чикаго в два австрийских банка сумму, превышающую 69 млн. долларов. При попытке поместить эти деньги на свои счета в Америке они были изобличены. В России в 1991 году во «Внешэкономбанке» преступники из числа сотрудников его вычислительного центра открыли несколько личных счетов по поддельным паспортам и начали перевод на них иностранной валюты. Когда на их счетах было уже 125,5 тыс. долларов США, они были изобличены. В сентябре 1993 года была пресечена попытка «электронного мошенничества» на сумму более 68 млрд. рублей в Центральном Банке Российской Федерации. В 1995 году российский инженер Левин путем перевода на счета в банки 7 стран похитил из «Сити бэнк» в США 10 млн. долларов, 400 тыс. из которых не обнаружены.

Значительные и, вместе с тем, никем не определяемые точно потери возникают в результате распространения вредоносных программ. Первый зафиксированный случай массового заражения относится к 1987 году, когда так называемый «пакистанский вирус» заразил только в США более 18 тыс. компьютеров. «Лехайский вирус» по состоянию на февраль 1989 года заразил около 4 тыс. компьютеров в США.

Опасность преступлений с использованием электронной техники и информационных технологий возрастает, когда преступники проникают в компьютерные системы объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики. Так, в США группа хакеров осуществила несанкционированный доступ более чем к 50 автоматизированным банкам данных, в том числе Лос-Аламосской ядерной лаборатории, крупного ракового центра и других жизненно важных объектов США. В Нью-Йорке они проникли в компьютерные сети базы ВВС Гриффитс и выкрали секретные военные данные. В конце 1997 года компьютерные умельцы прорвались в «Яху» – одну из самых популярных поисковых систем в Интернете и под угрозой заражения всей

сети компьютерным вирусом потребовали освобождения из-под ареста одного из своих коллег. В 1992 году была умышленно нарушена работа АСУ реакторов Игналинской АЭС в Прибалтике [5, с.9; 7, с.1-2].

В.С. Комиссаров приводит данные одного интересного исследования, проведенного в 1996 году Институтом защиты компьютеров (США) совместно с ФБР. Это исследование было направлено на определение распространенности компьютерных преступлений и мер, принимаемых для их предотвращения. Ответы были получены из 428 организаций.

Респонденты подтвердили, что их информационные системы находятся в опасности: 42% испытали различные формы вторжения или другого несанкционированного использования компьютерных систем в течении последнего года. Свыше 50% из них установили факты несанкционированных действий со стороны собственных служащих. Что касается частоты вторжений, то 22 респондента указали, что они испытали 10 или большее количество «нападений» на их системы в 1995 году. Наиболее частой формой нападений было несанкционированное изменение данных. Практиковались они прежде всего в медицинских (36,8% от всех нападений) и финансовых (21%) учреждениях.

Свыше 50% респондентов рассматривают конкурентов как вероятный источник нападений (от подслушивания до проникновения в информационные и коммуникационные системы) и полагают, что похищенная информация могла быть использована их конкурентами. Опрос показал также, что свыше 50% опрошенных не имеют плана действий на случай сетевого вторжения. Свыше 60% не имеют стратегии сохранения доказательств для дальнейшего рассмотрения в суде уголовных или гражданских дел. Свыше 70% респондентов не имеют устройств, предупреждающих о вторжении в их коммуникационные и информационные системы. Что характерно, менее 17% опрошенных указали, что они уведомят правоохранительные органы в случаях нападения на информационные системы. В качестве причины этого более 70% назвали опасение антирекламы [7, с.3-4].

Приведенные данные наглядно характеризуют тенденции роста и общественную опасность компьютерной преступности. Поэтому реакция белорусских законодателей, установивших уголовную ответственность за совершаемые с использованием компьютерной техники преступления против информационной безопасности, была своевременной.

Основной проблемой современного этапа является уровень специальной подготовки и технической грамотности должностных лиц правоохранительных органов – следователей, прокуроров и судей. Поэтому целью методических рекомендаций является не только анализ преступлений против информационной безопасности, но и рассмотрение

специальных терминов, относящихся к информационным технологиям и употребляемых законодателем в тексте нового Уголовного Кодекса Республики Беларусь 1999 года.

ВОПРОС 1. ПОНЯТИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1.1. Правовое регулирование информационных отношений.

Терминологическая неточность изложения закона или методологических рекомендаций по его исполнению может повлечь неправильное его применение и, как следствие, ошибки при определении преступности или непреступности деяния, в квалификации содеянного. Такие ошибки в уголовно-репрессивной сфере всегда влекут ущемление конституционных прав и свобод граждан или, наоборот, необоснованное освобождение от уголовной ответственности лиц, совершивших преступления.

Правовое регулирование в области информационных отношений в нашей республике осуществляется, в первую очередь, Законом Республики Беларусь от 6 сентября 1995 года «Об информатизации» [2]. В нем законодатель раскрыл понятие информационных правоотношений как отношений, возникающих в процессе формирования и использования документированной информации и информационных ресурсов, создания информационных технологий, автоматизированных или автоматических информационных систем или сетей. Этот Закон устанавливает порядок защиты информационного ресурса, права и обязанности субъектов, принимающих участие в процессах информатизации, а также, что важно, дает законодательное определение основных понятий информационных отношений. Прямо в тексте Закона Республики Беларусь «Об информатизации» указано, что он не распространяется на отношения, возникающие при создании и функционировании печати и иных средств массовой информации, и отношения, возникающие при обработке недокументированной информации.

По сравнению с белорусским российское законодательство в области регулирования информационных правоотношений ушло далеко вперед. Так, еще 23 сентября 1992 года были приняты Законы Российской федерации «О правовой охране программ для электронных вычислительных машин и баз данных» и «О правовой охране топологий интегральных микросхем». 20 февраля 1995 года принят Закон РФ «Об информации, информатизации и защите информации», а 4 июля 1996 года – Закон РФ «Об участии в международном информационном обмене».

Вместе с тем, не только эти законы Республики Беларусь и Российской Федерации обеспечивают правовое регулирование информационных отношений. В настоящее время правоотношения в области функционирования ЭВМ, информации и информационных ресурсов регулируются различными отраслями права – гражданским

правом, административным и т. д. В нашей республике это Гражданский Кодекс Республики Беларусь, Закон Республики Беларусь от 14 декабря 1990 года (с последующими изменениями и дополнениями) «О банках и банковской деятельности в Республике Беларусь», «Положение о коммерческой тайне», утвержденное Постановлением Совета Министров Республики Беларусь от 6 ноября 1992 года № 670, и др.

В Российской Федерации информационные отношения регулируют Гражданский Кодекс РФ, Закон РФ от 9 июля 1993 года (с изменениями и дополнениями от 19 июля 1995 года) «Об авторском праве и смежных правах», Закон РФ от 21 июля 1993 года «О государственной тайне», Закон РФ от 29 декабря 1994 года «Об обязательном экземпляре документов», Закон РФ от 16 февраля 1995 года «О связи» и некоторые другие.

Рассмотрим основные положения Закона Республики Беларусь «Об информатизации».

Ст. 1 этого Закона дает законодательные разъяснения, что понимать под основными терминами в области информационных правоотношений. Уяснение их содержания необходимо для последующего рассмотрения понятийного аппарата, использованного законодателем при конструировании составов преступлений против информационной безопасности в новом Уголовном Кодексе Республики Беларусь.

Итак, ст. 1 Закона «Об информатизации» определяет, что:

- **Информация** – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах;
- **Документированная информация (документ)** – это зафиксированная на материальном носителе информация с реквизитами, позволяющими их идентифицировать;
- **Материальный носитель информации** – материал с определенными физическими свойствами, который может быть использован для записи и хранения информации;
- **Информационные процессы** – процессы сбора, обработки, накопления, хранения, актуализации и предоставления документированной информации пользователю;
- **Информационный ресурс** – организованная совокупность документированной информации, включающая базы данных и знаний, другие массивы информации в информационных системах;
- **Информационная технология** – совокупность методов, способов, приемов и средств обработки документированной информации, включая прикладные программные средства, и регламентированного порядка их применения;
- **Автоматизированная или автоматическая информационная система** – совокупность информационных ресурсов, информационных технологий и комплекса программно-технических средств,

осуществляющих информационные процессы в человеко-машинном или автоматическом режиме;

- **Комплекс программно-технических средств** – совокупность общесистемных программных и технических средств, обеспечивающих реализацию информационных процессов;
- **Информационная сеть** – комплекс программно-технических средств для передачи и обработки данных по каналам связи;
- **Информационная продукция** – материализованный результат информационных процессов, предназначенный для обеспечения информационных потребностей органов государственной власти, юридических и физических лиц;
- **Информационные услуги** – информационная деятельность по доведению до пользователя информационной продукции, проводимая в определенной форме;
- **Данные** – документированная информация, циркулирующая в процессе ее обработки на электронно-вычислительных машинах;
- **База данных** – совокупность взаимосвязанных данных, организованная по определенным правилам на машинных носителях;
- **Банк данных** – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;
- **База знаний** – совокупность формализованных знаний об определенной предметной области, представленных в виде фактов и правил;
- **Собственник информационных ресурсов, информационных систем, технологий, средств их обеспечения** – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;
- **Владелец информационных ресурсов, информационных систем, технологий, средств их обеспечения** – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;
- **Пользователь (потребитель) информации** – субъект, обращающийся к информационной системе или посреднику за получением необходимой документированной информации.

Под информатизацией, согласно ст. 2 Закона, понимается организационно-экономический и научно-технический процесс обеспечения потребностей органов государственной власти, юридических и физических лиц в получении сведений о лицах, предметах, фактах, событиях, явлениях и процессах на базе информационных систем и сетей, осуществляющих формирование и обработку информационных ресурсов и выдачу пользователю документированной информации.

В ст. 3 Закона определены основные принципы информатизации:

- Общедоступность документированной информации, не отнесенной в установленном порядке к категории документированной информации с ограниченным доступом;
- Оперативность, полнота и точность предоставляемой пользователю документированной информации;
- Участие государства в формировании информационных ресурсов и обеспечение соответствия этих ресурсов задачам информатизации;
- Предоставление пользователю документированной информации на государственном языке Республики Беларусь или на языке, обусловленном договором субъектов правоотношений в сфере информатизации;
- Защита прав собственности на объекты права собственности в сфере информатизации.

В соответствии с указанным третьим принципом ст. 4 Закона гласит, что содействие развитию информатизации, защита прав и интересов граждан и государства при ее осуществлении является государственной политикой Республики Беларусь.

Согласно ст. 5 объектами права собственности являются:

- Документированная информация;
- Информационные ресурсы;
- Информационные технологии;
- Комплексы программно-технических средств;
- Информационные системы и сети.

Их собственниками могут быть государство, юридические и физические лица. Право собственности возникает при создании объектов информатизации за свой счет, а также при заключении договора на их создание или приобретение либо договора, предусматривающего условия перехода права собственности другому субъекту. Кроме того, право собственности физических лиц на объекты информатизации возникает при получении их в наследство на законных основаниях. Право авторства и право собственности могут принадлежать разным лицам.

Субъектами правоотношений в сфере информатизации выступают государство в лице органов государственной власти, юридические и физические лица, а также зарубежные государства, международные организации, иностранные физические и юридические лица (ст. 6 Закона). Субъекты правоотношений при создании и эксплуатации объектов информатизации могут выступать в качестве разработчиков, собственников, владельцев, пользователей или обработчиков документированной информации в информационных системах или сетях. Формы отношений этих субъектов регулируются договорами в соответствии с законодательством Республики Беларусь.

Отношения собственника (владельца) информационных ресурсов и обработчика регламентированы ст. 7 Закона. Так, собственник (владелец) или уполномоченные им лица определяют режим обработки и правила использования информационных ресурсов в информационных системах и сетях. Обработчик обязан обеспечить полноту, точность, качество документированной информации и программ ее обработки, обусловленные договором на информационные услуги. Запрещена передача информации третьим лицам, кроме случаев, предусмотренных договором с собственником. В свою очередь, обработчик обеспечивает доступ к информационному ресурсу всех пользователей в соответствии с условиями его обработки, предусмотренными договором между обработчиком и собственником.

Порядок и режим доступа к информационным ресурсам урегулирован ст. ст. 19 – 21 Закона. Органы государственной власти, юридические и физические лица имеют равные права на доступ к информационным ресурсам. Исключение составляют случаи, когда запрашиваемые сведения касаются документированной информации ограниченного доступа.

Однако, не может быть ограничен доступ к документированной информации:

- устанавливающей правовой статус государственных органов и юридических лиц;
- определяющей права, свободы и обязанности физических лиц и порядок их реализации;
- о чрезвычайных ситуациях, экологической, метеорологической, демографической, санитарно-эпидемиологической и другой, обеспечивающей безопасность существования общества;
- отнесенной к источникам знаний и накапливаемой в информационных системах в сфере образования, здравоохранения, науки, культуры и права.

Порядок доступа к открытой документированной информации определяется ее собственником или уполномоченным им лицом на основании договора или в порядке исполнения служебных обязанностей. При этом органы государственной власти или уполномоченные ими юридические лица обязаны организовать работу по формированию и предоставлению пользователю открытых информационных ресурсов, являющихся собственностью государства.

Интересным является установление порядка доступа физических и юридических лиц к документированной информации о них. Так, ст. 21 Закона определяет, что лица, чьи информационные ресурсы содержат документированную информацию о других физических или юридических лицах, обязаны дать возможность лицу ознакомиться с материалами,

затрагивающими его права и законные интересы. Причем последние имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и точности, право оспаривать эту информацию в установленном законом порядке, а также знать, кто и в каких целях накапливает или использует документированную информацию о них. Отказ в доступе к документированной информации или ее сокрытие могут быть обжалованы в судебном порядке.

Целями защиты информационных ресурсов и прав субъектов информатизации в соответствии со ст. 22 Закона являются:

- предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы;
- сохранение полноты, точности, целостности документированной информации, возможности управления процессом обработки и пользования в соответствии с условиями, установленными собственником этой информации или уполномоченным им лицом;
- обеспечение прав физических и юридических лиц на сохранение конфиденциальности документированной информации о них, накапливаемой в информационных системах;
- защита прав субъектов в сфере информатизации;
- сохранение секретности, конфиденциальности документированной информации в соответствии с правилами, определенными законодательством.

Собственники информационных систем или уполномоченные ими лица обязаны обеспечить уровень защиты документированной информации и, кроме того, обязаны сообщать владельцу информационных ресурсов обо всех фактах нарушения защиты информации.

Таковы основные положения Закона Республики Беларусь «Об информатизации».

1.2. Понятие и общая характеристика преступлений против информационной безопасности.

Как уже было сказано выше, потребность уголовно-правового регулирования в области информационных общественных отношений вызвала появление в новом Уголовном Кодексе Республики Беларусь 1999 года главы 31 «Преступления против информационной безопасности», составляющей одноименный раздел XII УК и объединяющей статьи 349 – 355.

В.С. Комиссаров отмечает, что установление уголовной ответственности за правонарушения в этой сфере имеет целью «путем угрозы уголовным наказанием максимально снизить негативные издержки неправомерного или недобросовестного обращения с ЭВМ и компьютерной информацией» [5, с.10].

В принципе, преступления, предусмотренные в главе 31 нового УК Республики Беларусь «Преступления против информационной безопасности», можно называть компьютерными. Вместе с тем, понятие «компьютерные преступления» более широкое и многоаспектное, чем понятие «преступления против информационной безопасности». Так, с криминалистической точки зрения, с использованием компьютера как орудия или средства совершения преступления можно осуществить и шпионаж, и мошенничество, и подлог документов, и фальшивомонетничество, и злоупотребление служебными полномочиями, и многие другие преступления самыми различными способами. Компьютер может быть и предметом преступления, но ошибочным было бы называть похищение аппаратной структуры компьютера «компьютерным преступлением», поскольку хотя в этом случае посягательство и направлено на компьютер как на предмет, оно нарушает отношения собственности, а не информационную безопасность, и должно квалифицироваться как преступление против собственности – кража, грабеж и т.д. в зависимости от способа хищения.

Поэтому рассматриваемые преступления против информационной безопасности необходимо называть именно так и не иначе. В УК Российской Федерации 1996 года аналогичные преступления названы «преступлениями в сфере компьютерной информации». Представляется, что такое понятие хотя и указывает на область их совершения, но, вместе с тем, являясь расширительным, не позволяет отграничить преступления, посягающие только на компьютерную информацию, от других преступлений, совершаемых с помощью компьютеров путем изменения компьютерной информации, к примеру, от «компьютерного мошенничества», названного в новом УК Республики Беларусь хищением путем использования компьютерной техники.

В названии главы 31 нового УК Республики Беларусь четко определен родовой объект рассматриваемых преступлений – информационная безопасность. Тем самым предусмотренные ст. ст. 349 – 355 УК преступления отграничены от преступлений против человека, против собственности, против государства и других, которые посягают на основной защищаемый объект путем воздействия на информационную безопасность.

Информационную безопасность в качестве объекта рассматриваемых преступлений можно определить, на взгляд автора, как совокупность

общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями. Следует отметить, что причинение ущерба только самому себе – умышленно или по неосторожности – не влечет ответственности, если при этом не причиняется ущерб третьим лицам.

В юридической литературе иногда допускается смешение понятий «объект преступления» и «предмет преступления» при описании признаков рассматриваемых преступлений. Так, к примеру, по мнению В.Б. Вехова, «с точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых **машинная информация** является **объектом** преступного посягательства. В данном случае в качестве **предмета** (выделено мною) или орудия преступления будет выступать **машинная информация**, компьютер, компьютерная система или компьютерная сеть» [4, с.23].

Вместе с тем, теория уголовного права объектом преступления признает охраняемые уголовным законом общественные отношения, на которые посягают преступные деяния. Предметом же преступления являются материальные предметы, воздействуя на которые лицо посягает на те или иные общественные отношения [10, с.70, 74].

Поэтому разграничение понятий «объект преступления» и «предмет преступления» применительно к преступлениям против информационной безопасности» следует провести следующим образом: противоправное воздействие на компьютерную информацию как предмет преступления посягает на объект преступления - информационную безопасность, т.е. общественные отношения в этой специфической сфере.

Таким образом, предметом преступлений против информационной безопасности является компьютерная информация, то есть содержащиеся на машинных носителях, в компьютерной системе или сети сведения о лицах, предметах, фактах, событиях и явлениях, и компьютер как информационная структура – носитель этой информации. В предусмотренных главой 31 УК преступлениях против информационной безопасности компьютерная информация как предмет преступления является обязательным признаком состава. Если преступное посягательство было направлено не на компьютерную информацию, а только на ее носитель – компьютер как вещь, содеянное будет расценено как преступление против собственности – похищение компьютера или его уничтожение только как вещи, в зависимости от характера посягательства, а не как преступление против информационной безопасности. Отграничивая компьютерную информацию от других видов информации,

которые являются предметом преступных посягательств, сразу необходимо отметить, что в главе 31 УК Республики Беларусь говорится именно об информации, которая неотделима от компьютера и доступ к которой может быть обеспечен только с использованием компьютера. Записи компьютерных программ, первичные базы данных и другая подобная информация, исполненная рукой человека, отпечатанная на печатной машинке или набранная типографским способом, то есть информация, зафиксированная не на машинном, а на ином материальном носителе (к примеру, на бумаге), не является предметом преступлений, предусмотренных ст. ст. 349 – 355 УК.

Что характерно для рассматриваемых преступлений, при их совершении компьютер может выступать одновременно и в качестве предмета, и в качестве орудия совершения преступления. Указанное свойство компьютера определяется технологической спецификой его строения (архитектурой), под которой понимается концепция взаимосвязи элементов сложной структуры, включающей в себя компоненты логической, физической и программной структур. Как известно, в качестве орудия (средства) совершения преступления выступают вещи, с помощью которых совершается преступление. С этой точки зрения компьютер является таким же техническим средством совершения преступления, как автомобиль, оружие или иное техническое приспособление.

Примером может служить преступление, предусмотренное ст. 349 УК: «несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда». В данном случае компьютер используется как орудие совершения преступления для доступа к предмету преступления - информации, хранящейся в нем, что влечет указанные негативные последствия для этой информации.

Субъектом преступлений против информационной безопасности является вменяемое лицо, достигшее 16-летнего возраста.

Объективная и субъективная стороны этих преступлений, а также описанные в диспозициях отдельных статей специальные признаки субъекта будут подробно рассмотрены ниже при анализе видов преступлений против информационной безопасности.

Характеризуя в целом преступления против информационной безопасности, необходимо отметить следующее. В соответствии со ст. 12 УК Республики Беларусь преступления, предусмотренные ч. ч. 1 и 2 ст. 349, ст. ст. 352 и 353, ч. 1 ст. 351 и ч. 1 ст. 355 УК, относятся к преступлениям, не представляющим большой общественной опасности;

предусмотренные ч. 3 ст.349, ч. ч. 1 и 2 ст. 350, ч. 1 ст. 351, ч. ч. 2 и 3 ст. 355 УК относятся к менее тяжким преступлениям; предусмотренные ч. 2 ст. 351 (компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия) и ч. 2 ст. 354 (разработка, использование либо распространение вредоносных программ, повлекшее тяжкие последствия) - к тяжким преступлениям.

Останавливаясь на вопросах квалификации неоконченной преступной деятельности, следует отметить, что в соответствии с ч. 2 ст. 13 УК приготовление к преступлению, не представляющему большой общественной опасности, уголовную ответственность не влечет. Соответственно исключается уголовная ответственность за приготовление к преступлениям, указанным в первой группе. Приготовление же к умышленным преступлениям, указанным во второй и третьей группах, и покушение на их совершение уголовно наказуемы.

1.3. Понятийный аппарат преступлений против информационной безопасности.

Прежде чем перейти к анализу преступлений против информационной безопасности, необходимо более подробно остановиться на ряде технических терминов, использованных законодателем при конструировании составов этих преступлений и получивших поэтому статус юридических понятий.

Вначале рассмотрим термины, общие для всех составов преступлений против информационной безопасности. Понятия, относящиеся к их объективной стороне, т.е. описывающие способ совершения преступления, его последствия и некоторые другие, раскроем ниже при анализе конкретных составов.

Средства компьютерной техники по своему функциональному назначению делятся на две основные группы – 1/ аппаратные средства, или оборудование (HardWare) и 2/ машинная информация, включая программные средства (SoftWare).

Описывая аппаратные средства, законодатель использует словосочетания «компьютерная система», «компьютерная сеть» и «машинные носители». Сразу отметим, что термины «компьютер» и «электронно-вычислительная машина (ЭВМ)» тождественны. В литературе дается множество определений, что же следует понимать под компьютером. Все они отражают тот или иной предмет исследований авторов. Нам же необходимо определение, которое бы в сжатом виде характеризовало и техническую, и правовую сторону. Поэтому, как представляется, под компьютером (или ЭВМ) следует понимать комплекс

программно-технических средств, обеспечивающий реализацию информационных процессов. Само это определение, как и многие другие, далеко от совершенства, однако оно основано на рассмотренном выше Законе Республики Беларусь «Об информатизации».

Исходя из текста этого Закона, можно определить компьютерную систему как автоматическую или автоматизированную информационную систему, представляющую собой совокупность информационных ресурсов, информационных технологий и комплекса программно-технических средств, осуществляющих процессы в человеко-машинном или автоматическом режиме. Под компьютерными сетями следует понимать компьютеры, объединенные между собой линиями электросвязи.

Уголовным законом охраняется компьютерная информация, хранящаяся не только в компьютерной системе или сетях, но и на машинных носителях. К машинным носителям компьютерной информации относятся устройства памяти ЭВМ и периферийные устройства ЭВМ.

Устройствами памяти ЭВМ являются устройства внешней памяти и оперативное запоминающее устройство (ОЗУ) ЭВМ.

Внешняя память (внешние запоминающие устройства) компьютера обеспечивают накопление и сохранение информации. Имеется несколько основных типов устройств для долговременного хранения данных.

Гибкий диск (дискета) – это круглая, чаще пластмассовая пластинка, запаянная в квадратную картонную или пластиковую оболочку. На пластинке с магнитным покрытием производится запись и считывание информации специальным устройством – дисководом.

Накопитель на жестких магнитных дисках (хард-диск или «винчестер») – это встроенное в компьютер устройство, выполняющее функции хранения значительных объемов информации и программ. По существу это электронное устройство, где с высокой скоростью вращаются несколько магнитных дисков, обеспечивающих считывание и запись на эти диски программ и данных, а также высокую скорость доступа к ним.

На магнитные ленты ввод и вывод информации производится при помощи «стримеров», которые могут быть как встроены в системный блок, так и представлять собой периферийное устройство. Стримеры чаще всего используются для хранения копии винчестера с целью восстановления информации в случае аварии жестких магнитных дисков.

Компактные диски (CD-ROM) – это современное, чрезвычайно емкое устройство для записи и воспроизведения информации. Известны три типа таких дисков. Первый – с постоянной записью, на такой диск запись информации производится изготовителем и в процессе эксплуатации пользователь может производить лишь считывание данных. Второй тип дисков обеспечивает возможность однократной записи

пользователем необходимой информации. Третий вид дисков имеет возможность неоднократной перезаписи информации.

В последнее время получили широкое распространение такие устройства внешней памяти, как магнито-оптические и DVD-диски, которые позволяют хранить еще больший объем информации.

Переходя к функциям оперативного запоминающего устройства следует дать понятие файла: это логически связанная совокупность данных или программ, для размещения которой во внешней памяти выделяется определенная область. При запуске компьютера (включении электропитания) в ОЗУ загружаются в определенном порядке файлы с командами (т.е. программы) и данными, обеспечивающими для компьютера возможность их обработки. Последовательность и характер такой обработки задается вначале командами операционной системы, а затем и командами пользователя. Фактически к моменту окончания процесса запуска компьютера его ОЗУ содержит набор командных файлов и файлов данных. В дальнейшем при необходимости данные в виде файлов или их частей перемещаются из ОЗУ назад на внешние запоминающие устройства или направляются в блоки памяти устройств вывода или иным пользователям компьютерной сети с помощью устройств связи. Это перемещение обусловлено либо командами операционной системы (ОС), либо командами программы пользователя, либо прямыми командами пользователя. Таким образом, находящаяся в ОЗУ информация может быть всегда индивидуально определена и идентифицирована, так как при нахождении в ОЗУ она не теряет своих индивидуальных свойств, местоположение и порядок ее движения в ОЗУ достаточно жестко регламентирован командами ОС, программ и пользователя. При отключении электропитания ОЗУ утрачивает свое содержание.

В процессе обработки информации компьютер ведет активный обмен со своими периферийными устройствами, в том числе с устройствами ввода и вывода информации, которые, в свою очередь, нередко имеют собственные ОЗУ, где временно хранятся массивы информации, предназначенные для обработки этими устройствами. Примером такого устройства является лазерный принтер, где могут стоять «в очереди» на печать несколько документов. Создание собственных ОЗУ в периферийных устройствах является тенденцией развития их производства. Передача в такие ОЗУ порций информации из ОЗУ основного компьютера увеличивает быстродействие последнего за счет увеличения ресурсов памяти.

Компьютерными устройствами, не относящимися к машинным носителям, которые не хранят, а только перемещают информацию, являются компьютерные устройства связи и сетевые устройства.

Модемы и факс-модемы – это устройства связи между компьютерами по телефонным и радиолиниям. Они обеспечивают и сопряжение компьютеров с сетями. Модемы (сокращение от «модулятор» и «демодулятор») по способу подключения к компьютеру делятся на внутренние, т.е. находящиеся непосредственно в компьютере в виде специальной модемной платы, и внешние, выпускаемые в виде отдельного блока, соединяемого с компьютером проводами. Модемы осуществляют связь с главным компьютером, сетями или другими ПК для передачи файлов и иного интерактивного обмена, передачу и получение «электронной почты», прием и передачу текста и графики на расстояние в виде факсимильного сообщения. Факс-модемы появились позже и представляют собой устройства, сочетающие возможности модема и средства для обмена факсимильными изображениями с другими факс-модемами и обычными телефаксными аппаратами. Многие факс-модемные устройства предназначены для работы в так называемом фоновом режиме, то есть могут находится в памяти машины во время работы с другими программами и актуализироваться тогда, когда на данный компьютер поступает вызов абонента. Программа может работать в фоновом режиме и при рассылке сообщений, автоматически дозваниваясь по заданному списку до каждого абонента. Следует учитывать, что в таком режиме работы компьютер доступен для посторонних воздействий, поскольку модем работает как на передачу, так и на прием информации. Таким образом, модемы являются основным устройством, позволяющим осуществлять проникновение в компьютер извне.

Компьютерные сети условно можно разделить на «локальные» и «глобальные». Первые предназначены для решения задач в одной организации, фирме, их подразделениях и охватывают сравнительно небольшие пространства. На электрическом уровне локальные сети соединяют компьютеры между собой с помощью кабелей и специальных, устанавливаемых в каждом ПК, сетевых плат (плат интерфейса сети). Объединения локальных сетей между собой образуют глобальные сети.

На сегодняшний момент фактически все существующие большие сети имеют возможность пересылки сообщений и иного обмена информацией между собой. Центральным программно-техническим устройством, решающим коммуникационные задачи в локальной сети, является сервер. Иногда сервером называют центральную машину в сети, обеспечивающую основную обработку информации и хранящую данные, которые используются всеми пользователями сети. Программное обеспечение большинства локальных сетей обеспечивает определение приоритетов доступа и возможность обеспечения конфиденциальности информации. Наиболее употребительной формой общения в сетях является электронная почта. Она, кроме передачи писем, предоставляет

возможность телеконференций, когда все пользователи электронной почты могут передать любое сообщение на «доску объявлений» по определенным темам (ньюс-группам).

Описанные компьютерные устройства связи и сетевые устройства в большей мере относятся к телекоммуникационной технике, чем чисто к компьютерам, так как не предназначены для хранения информации, а представляют собой среду для ее распространения. Поэтому их нельзя включать в обобщенное понятие «машинный носитель» информации, употребляемый в тексте уголовного закона.

Важным для последующего анализа видов преступлений против информационной безопасности является уяснение понятия «компьютерные программы». Все многообразие программных средств (ПС) может быть разделено на несколько больших групп. Поскольку для ПС характерно свойство комплексности (многозадачности) применения, в качестве критерия для отнесения ПС к той или иной группе выбирается основное назначение ПС, хотя необходимо оговориться, что такой критерий является условным.

Первая группа – операционные системы (ОС). Под операционной системой понимают комплекс программных средств, обеспечивающий взаимодействие всех устройств компьютера между собой и с оператором (пользователем). Это единственная программа, которая хранится в ОЗУ компьютера в течении всего времени работы с ним до выключения питания.

Вторая группа программных средств – сервисные (обслуживающие) программы, которые зачастую являются продолжением программ, входящих в операционную систему, делают более удобной работу пользователя и расширяют возможности ОС.

К третьей группе ПС можно отнести средства и языки программирования, т.е. программы, создающие программы.

Отдельные группы программных средств включают средства обработки текстов и изображений, системы управления базами данных и системы управления знаниями (так называемые «экспертные системы»), электронные таблицы, интегрированные пакеты, игровые программы, специализированные программные средства, которые решают задачи в узкой предметной области.

ВОПРОС 2. ВИДЫ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

2.1. Несанкционированный доступ к компьютерной информации

В части 1 ст. 349 УК Республики Беларусь установлена уголовная ответственность за **«несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда».**

Состав этого преступления материальный. Оно признается оконченным с момента наступления указанных последствий от совершенного действия - несанкционированного доступа к компьютерной информации, сопровождавшегося нарушением системы защиты. В.С. Комиссаров обоснованно считает, что неправомерным, то есть несанкционированным доступом следует признавать «получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению, совершаемое без согласия собственника либо иного уполномоченного лица» [5, с.14].

Обязательным признаком объективной стороны является способ доступа – «с нарушением системы защиты». Обязанность обеспечивать уровень защиты документированной информации возложена согласно ст. 23 Закона «Об информатизации» на собственника информационной системы или уполномоченное им лицо. Способами доступа с нарушением системы защиты могут быть использование чужого имени (пароля), маскировка под законного пользователя, изменение физических адресов технических устройств, модификация программного и информационного обеспечения, нахождение слабых мест и «взлом» системы защиты, хищение носителя информации и др.

Так как состав этого преступления материальный, то обязательным признаком его объективной стороны является наступление одного из перечисленных в диспозиции вредных последствий, которые согласно смысла части 1 статьи 349 УК в целом можно объединить понятием «существенный вред». Поэтому само по себе ознакомление с информацией в результате несанкционированного доступа к ней, не образующее состава другого преступления (к примеру, шпионажа как преступления против государства или коммерческого шпионажа) и не повлекшее этих последствий, преступлением не является.

Последствия в диспозиции статьи перечислены альтернативно, то есть наступление одного из них в результате несанкционированного

доступа к информации уже образует оконченное преступление. При этом первые три предусматривают последствия только для компьютерной информации – «изменение, уничтожение и блокирование информации», а четвертое – «вывод из строя» - относится к компьютерному оборудованию, которое включает в себя и аппаратные средства, и программное обеспечение. Рассмотрим, что же понимается под этими вредными последствиями.

Изменение информации – это существенное видоизменение первоначального содержания соответствующих файлов, где она сосредоточена, которое затрудняет законное пользование этой компьютерной информацией (кроме изменения информации, связанного с адаптацией программы для компьютера или базы данных).

Уничтожение информации – это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние. Уничтожение информации выражается в удалении файлов (каталогов) из памяти компьютера, которое исключает возможность их восстановления. Следует учитывать, что имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от уголовной ответственности. Вместе с тем, сопряженный с уничтожением одновременный перевод информации на другой машинный носитель не считается ее уничтожением в уголовно-правовом смысле, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен или исключен. Переименование файла, где содержится информация, а также автоматическое вытеснение старых версий файлов последними по времени также не расценивается как уничтожение информации.

Блокирование информации – это не связанное с уничтожением создание невозможности ее использования или существенных препятствий к свободному использованию информации, приводящее к ее недоступности, когда при сохранении самой информации она не может нормально востребоваться законным пользователем.

Вывод из строя компьютерного оборудования – это различные нештатные ситуации, связанные со сбоями в работе оборудования, выдачей неверной информации, отказом в выдаче информации, отключением элементов компьютерной системы (серверов, модемов и т.д.). При этом обязательным условием квалификации только по ст. 349 УК является сохранение физической целости компьютера. Если же наряду с указанными последствиями нарушается и целостность компьютерной системы, как физической вещи, то содеянное требует дополнительной квалификации по статьям о преступлениях против собственности.

Перечисленные четыре последствия в целом характеризуют причинение вреда компьютерной информации и компьютерному оборудованию, то есть затрагивают интересы собственника информации, ее владельца или уполномоченных ими лиц.

Причинение иного существенного вреда – это оценочное понятие. Что понимать под существенным вредом, в каждом конкретном случае необходимо решать суду. Как представляется, является ли вред существенным, необходимо определять с учетом имущественного положения и организационных возможностей собственника компьютера или сети. Причиненный вред может быть как материальным, так и нематериального характера.

При оценке материального ущерба как существенного логичным было бы, как кажется, распространить на рассматриваемую статью положения п. 3 приложения к главе 24 УК «Преступления против собственности» и признавать существенным вредом материальный ущерб в значительном размере, то есть на сумму, в сорок и более раз превышающую размер минимальной заработной платы.

Понятием «иного существенного вреда» нематериального характера, на взгляд автора, должно охватываться значительное ущемление прав и законных интересов организаций, учреждений, предприятий, нарушение нормальной их работы, а также конституционных прав граждан, как являющихся, так и не являющихся собственником, владельцем или правомерным пользователем информационной системы, доступ к которой повлек это ущемление.

Важным является установление причинной связи между несанкционированным доступом и наступлением перечисленных последствий. Поэтому не является преступлением простое временное совпадение несанкционированного доступа и сбоя в компьютерной системе, который мог быть вызван неисправностями компьютера или ошибками в программе, а не действиями лица, осуществившего несанкционированный доступ.

При анализе объективной стороны возникает и такой вопрос, касающийся места совершения преступления: как поступать в случае, если действие – несанкционированный доступ – было совершено на территории Республики Беларусь, а одно из перечисленных последствий наступило за пределами Беларуси, или такое же действие было совершено за границей, а последствия наступили в нашей республике, ведь глобальные компьютерные сети объединяют многие страны мира? Какое решение принять, если один из соучастников преступной группы, совершившей преступление против информационной безопасности, выполнил свои действия в Беларуси, а остальные – в других странах? При решении этого вопроса необходимо руководствоваться положениями ст. 5 УК 1999 года,

которая гласит: в части первой – что «лицо, совершившее преступление на территории Республики Беларусь, подлежит ответственности по настоящему Кодексу», то есть по УК Республики Беларусь 1999 года; в части второй – что «преступление признается совершенным на территории Республики Беларусь, если оно начато, или продолжалось, или было окончено на ее территории, или совершено в пределах Республики Беларусь в соучастии с лицом, совершившим преступление на территории иностранного государства». Это правило распространяется и на другие составы преступлений против информационной безопасности.

По субъективной стороне преступление, предусмотренное ст. 349 УК, является неосторожным. Если действие – несанкционированный доступ к компьютерной информации путем нарушения системы защиты – совершается умышленно, то отношение виновного лица к перечисленным выше последствиям – неосторожное, что прямо указано в диспозиции рассматриваемой статьи. Субъективную сторону этого преступления можно описать следующим образом: лицо осознает, что осуществляет несанкционированный, то есть без разрешения собственника или уполномоченного им лица, доступ к компьютерной информации путем нарушения системы защиты, при этом предвидит возможность наступления перечисленных вредных последствий такого доступа, но без достаточных оснований рассчитывает на их предотвращение (преступное легкомыслие), или не предвидит возможности их наступления, хотя при необходимой внимательности и предусмотрительности должно было и могло их предвидеть (преступная небрежность).

Если несанкционированный доступ, не повлекший указанных последствий, был совершен с целью совершения другого преступления с использованием компьютерной техники – хищения, шпионажа и т.д., но преступная деятельность была пресечена вследствие ее обнаружения, содеянное подлежит самостоятельной квалификации как приготовление к этому преступлению или покушение на него.

Субъект рассматриваемого преступления – общий, то есть любое вменяемое лицо, достигшее 16 лет, независимо от гражданства.

Наказание по части 1 ст. 349 УК – штраф или арест на срок до 6 месяцев.

В части 2 статьи 349 УК предусмотрена ответственность за **«то же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети».**

Анализ текста части 2 ст. 349 УК говорит о том, что здесь сформулирован не квалифицированный состав преступления, описанного в части 1, а качественно иное преступление, которое, во-первых, имеет не

материальный, а формальный состав, и, во-вторых, является умышленным. К таким выводам можно прийти по следующим соображениям.

Под **«тем же действием»** в части 2 рассматриваемой статьи следует понимать именно действие, указанное в части 1, т.е. «несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты», а не наступление перечисленных в части первой этой статьи вредных последствий, поскольку наступление последствий не охватывается понятием «действие».

Как известно, преступлением с формальным составом считается такое, при описании обязательных признаков которого законодатель не указывает наступление последствий и соответственно которое он считает оконченным на более ранней стадии, т.е. с момента совершения деяния, независимо от наступления последствий. Поэтому, не указывая в части 2 на необходимость наступления последствий, чтобы признать предусмотренное в части 1 действие оконченным преступлением, законодатель тем самым описал предусмотренный в части 2 ст. 349 УК состав как формальный.

О том, что преступление, предусмотренное частью 2 ст. 349 УК, является умышленным (в отличие от неосторожного, предусмотренного частью 1 этой статьи), свидетельствуют такие перечисленные альтернативные обязательные признаки, как «корыстная или иная личная заинтересованность», а также совершение этого преступления «группой лиц по предварительному сговору». Как известно, мотивы приобретают уголовно-правовое значение и учитываются только в преступлениях, совершаемых с прямым умыслом. Соучастие также возможно только умышленное и только в умышленном преступлении.

Таким образом, следует прийти к выводу, что в части второй ст. 349 УК сформулировано иное преступление с отсылочной (к части первой этой статьи) диспозицией.

Основываясь на положении п. 10 ст. 4 УК, под корыстной заинтересованностью в данном составе следует понимать стремление извлечь из совершенного преступления - несанкционированного доступа к компьютерной информации - для себя или близких выгоду имущественного характера либо намерение избавиться таким способом от материальных затрат.

Как «иную личную заинтересованность» следует расценивать стремление виновного при совершении описанного в части 1 действия – «несанкционированного доступа к информации» - извлечь какие – либо выгоды нематериального характера лично для себя либо лиц, чья судьба ему небезразлична.

Совершение несанкционированного доступа к компьютерной информации группой лиц по предварительному сговору будет в том случае, когда исполнители заранее договорились о совместном совершении данного преступления.

Лицами, имеющими доступ к компьютерной системе или сети, признаются те, кто на законных основаниях работает на них или обслуживает непосредственно их работу – программисты, инженеры-электрики, специалисты по эксплуатации ЭВМ, администраторы баз данных, наладчики компьютерного оборудования и т.п. Таким образом, эти лица вовлечены в сферу специфических общественных отношений, связанных с использованием и обработкой компьютерной информации, и поэтому они являются специальными субъектами. Опасность совершения преступления указанными лицами состоит в том, что они, выходя за пределы предоставленных им прав и злоупотребляя оказанным доверием, получают доступ к информации, на работу с которой не были уполномочены собственником или иным лицом, владеющим ею на законном основании. При этом лица, имеющие доступ в помещение, где находится компьютер, но работа которых не состоит в использовании и обработке компьютерной информации (к примеру, уборщицы, специалисты по ремонту кондиционеров, составители первичной информации на бумажных носителях и т.п.), не являются специальными субъектами преступления, описанного в ч. 2 ст. 349 УК. Если они получают несанкционированный доступ к компьютерной информации, то такое их действие будет считаться уголовно наказуемым только в том случае, если наступят перечисленные в части 1 этой статьи последствия или будут установлены другие обстоятельства, указанные в части 2.

Что примечательно, несанкционированный доступ к компьютерной информации, не повлекший наступление вредных последствий, если он был совершен при указанных в части второй обстоятельствах, законодатель не просто называет преступлением, но даже расценивает как более тяжкое преступление, чем то, которое повлекло перечисленные в части 1 общественно опасные последствия в виде существенного вреда. При наличии одного из указанных в части 2 обязательных признаков содеянное по этой части ст. 349 УК по сравнению с частью 1 наказывается строже: штрафом, или лишением права занимать определенные должности или заниматься определенной деятельности, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

В части 3 ст. 349 УК установлена уголовная ответственность за **«несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютерной системы, компьютерной сети,**

повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия».

Это – третье, отличное от описанных в частях первой и второй, преступление, а не квалифицированный их состав. К выводу об этом можно прийти по следующим соображениям.

Состав преступления, описанный в части 3 ст. 349 УК – материальный. Неправомерными признаются следующие действия:

1. несанкционированный доступ к компьютерной информации, что под этим понимается, рассмотрено выше;
2. самовольное пользование электронной вычислительной техникой, средствами связи компьютеризированной системы или компьютерной сети, под которым следует понимать взаимодействие лица с перечисленными устройствами без разрешения на то со стороны собственника, владельца, уполномоченного ими лица или законного пользователя.

В части 3 не указан способ совершения преступления, являющийся обязательным признаком состава, предусмотренного частью 1 – «с нарушением системы защиты».

В качестве последствий перечисленных действий указан вред не только для компьютерной информации или компьютерного оборудования, т.е. вред интересам собственника информации, но также и наиболее тяжкие последствия для третьих лиц, наступающие в результате неправомерных действий с компьютерными информацией или оборудованием. Эти последствия перечислены в части 3 ст. 349 УК альтернативно: **крушение, авария, катастрофа, несчастные случаи с людьми, отрицательные изменения в окружающей среде, иные тяжкие последствия.**

Под иными тяжкими последствиями, что является оценочным понятием, необходимо, как представляется, понимать причинение материального ущерба в особо крупном размере, уничтожение, блокирование или модификацию информации особой ценности, к примеру, составляющей государственную тайну, или имеющей государственное значение, либо содержащей результаты исследований, в которых принимали участие большие коллективы в течении длительного времени и т.д.

Преступление, описанное в части 3 ст. 349 УК, является неосторожным, о чем имеется прямое указание. Одно из альтернативных действий – несанкционированный доступ к компьютерной информации или самовольное пользование электронной вычислительной техникой - виновное лицо совершает умышленно, понимая противоправный его характер и то, что совершает это действие без разрешения собственника

или уполномоченного лица, о чем говорит признак «самовольность». Психическое отношение к последствиям заключается в том, что лицо либо предвидело возможность наступления одного из перечисленных общественно опасных тяжких последствий, но без достаточных оснований рассчитывало на их предотвращение, либо не предвидело возможность их наступления, хотя при необходимой внимательности и предусмотрительности должно было и могло их предвидеть.

Наказание по части 3 ст. 349 УК – ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет.

Представляется интересным сравнить два неосторожных преступления, предусмотренных ч. 1 ст. 349 (рассмотрено выше) и ст. 219 («уничтожение либо повреждение имущества по неосторожности, повлекшее причинение ущерба в особо крупном размере») УК Республики Беларусь. Как видим, уничтожение или повреждение имущества по неосторожности является преступлением только в том случае, если ущерб превысил сумму, в тысячу и более раз превышающую минимальную заработную плату. Если же ущерб был причинен на меньшую сумму, то такое уничтожение либо повреждение имущества по неосторожности уголовно-наказуемым не является. Несоизмеримо выше по сравнению с защитой прав собственника имущества законодатель защищает права собственника информации: преступлением в соответствии с частью 1 ст. 349 УК признается причинение по неосторожности вреда информации, вывод по неосторожности из строя компьютерного оборудования либо причинение иного существенного вреда, даже без наступления такого последствия, как материальный ущерб в особо крупном размере. Об усиленной защите информации уголовно-правовыми средствами свидетельствует и существенная разница между установленными законодателем максимальными санкциями за эти два преступления. Так, за неосторожное преступление против собственности, предусмотренное ст. 219 УК, предусмотрено наказание в виде исправительных работ на срок до двух лет, или ареста на срок до шести месяцев, или ограничения свободы на срок до двух лет. В ч. 3 ст. 349 УК за причинение по неосторожности в результате несанкционированного доступа к компьютерной информации тяжких последствий, в том числе ущерба в особо крупном размере, установлено наказание в виде ограничения свободы на срок до пяти или лишения свободы на срок до семи лет.

2.2.Модификация компьютерной информации

В части 1 ст. 350 УК описаны признаки основного состава преступления и одновременно дается определение термина «модификация компьютерной информации»: **«изменение информации, хранящейся в**

компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившее существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации».

Модификация компьютерной информации – это разновидность, или самостоятельная форма, несанкционированного доступа к компьютерной информации. Состав этого преступления материальный. В диспозиции альтернативно перечислены действия, входящие в понятие «модификация»: 1/ изменение компьютерной информации; 2/ внесение заведомо ложной информации.

Модификация является уголовно-наказуемой в том случае, если изменение информации не было связано с адаптацией программы для компьютера или базы данных, которая осуществляется только в целях обеспечения функционирования программы на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Не является «модификацией» в уголовно-правовом смысле использование программ, модифицирующих данные без изменения их содержания с возможностью восстановления первоначального вида – архиваторов, кодировщиков и т.п.

В качестве последствия в диспозиции части 1 ст. 350 УК предусмотрено причинение существенного вреда. Что под ним следует понимать, рассмотрено выше при анализе части 1 ст. 349 УК.

Как указано в тексте анализируемой статьи, модификация компьютерной информации наказывается по ст. 350 УК только в том случае, когда отсутствуют признаки преступления против собственности. Действительно, предусмотренное ст. 212 УК преступление «хищение путем использования компьютерной техники» по объективной стороне схоже с рассматриваемым преступлением «модификация компьютерной информации», так как общим способом их совершения является изменение компьютерной информации либо введение в компьютерную систему ложной информации. Различие в том, что при совершении хищения этим способом происходит умышленное противоправное безвозмездное завладение чужим имуществом с корыстной целью. Если же виновное лицо действовало без корыстной цели и его действия по модификации компьютерной информации не были направлены на завладение чужим имуществом, содеянное надлежит квалифицировать по ст. 350 УК, а не как преступление против собственности.

Данное преступление совершается умышленно, причем умысел может быть как прямым, так и косвенным. Об этом свидетельствует отсутствие в диспозиции указания на возможность привлечения к уголовной ответственности за причинение существенного вреда по

неосторожности. Содержание умысла виновного лица можно раскрыть так: виновный сознает общественно опасный характер своего действия – модификации компьютерной информации, предвидит возможность наступления общественно опасного последствия – существенного вреда, желает его наступления либо, если не желает, то сознательно допускает наступление этого последствия либо относится к нему безразлично.

Наказание по части 1 ст. 350 УК – штраф, или лишение права занимать определенные должности или заниматься определенной деятельностью, или арест на срок от трех до шести месяцев, или ограничение свободы на срок до трех лет, или лишение свободы на тот же срок.

В части 2 ст. 350 УК предусмотрена ответственность за **«модификацию компьютерной информации, сопряженную с несанкционированным доступом к компьютерной системе или сети либо повлекшую по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса».**

В части 2 ст. 350 УК говорится именно о модификации компьютерной информации, определение которое, данное в части 1, включает в себя как деяние, так и последствие. Поэтому в части 2 ст. 350 УК предусмотрен квалифицированный состав, а не самостоятельное преступление.

Первый признак характеризует деяние – его обстоятельства, а второй – последствия. Анализируя часть 2 ст. 350 УК, следует отметить, что и при первом, и при втором квалифицирующем признаке этот состав является материальным, поскольку законодатель без каких-либо оговорок употребил в части 2 термин «модификация компьютерной информации». Понятием же «модификации», согласно части первой ст. 350 УК, охватывается причинение существенного вреда. Поэтому изменение компьютерной информации или внесение заведомо ложной информации, сопряженные с несанкционированным доступом к компьютерной системе или сети, является уголовно-наказуемым только в случае умышленного причинения существенного вреда.

Модификация компьютерной информации при втором квалифицирующем признаке является неосторожным преступлением, о чем есть прямое указание в тексте закона. Указание на последствия – отсылочное к части 3 ст. 349 УК.

Наказание по части 2 ст. 350 УК – ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

2.3. Компьютерный саботаж

В части первой статьи 351 УК закреплено, что же понимается по компьютерным саботажем. Это **«умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж)».**

Состав этого преступления материальный. Преступные действия в диспозиции статьи не описаны. Ими могут быть любые действия, направленные на причинение альтернативно перечисленных уголовно наказуемых последствий в виде уничтожения, блокирования, приведения в непригодное состояние компьютерной информации или программы, вывода из строя компьютерного оборудования, разрушения компьютерной системы, сети или машинного носителя. На характеристике этих последствий, за исключением последнего, останавливаться не будем, поскольку это было сделано ранее.

Как разрушение компьютерной системы следует расценивать уничтожение как всех аппаратных средств этой системы, так и отдельных из них, без которых эта компьютерная система не может работать. К примеру, уничтожение монитора как устройства вывода информации не приведет к прекращению работы системного блока, однако без воспроизведения информации на экране системный блок будет бесполезен для пользователя.

Под разрушением компьютерной сети следует понимать, как представляется, не уничтожение любых отдельных компьютеров в сети, а только сервера или коммуникационных линий между сервером и другими компьютерами в сети.

Разрушение машинного носителя - это полное уничтожение либо такое повреждение любого типа машинного носителя, которое исключает получение информации, хранившейся на нем. При этом из текста закона не следует, что обязательно при разрушении машинного носителя должна утрачиваться, уничтожаться какая-либо информация. Поэтому даже уничтожение «чистой» чужой дискеты, судя по описанию признаков преступления в части 1 ст. 351 УК, может быть расценено как уголовно-наказуемое деяние, что таковым, конечно же, не является, поскольку не посягает на информационную безопасность.

Что характерно, при формулировании этого состава преступления «компьютерный саботаж» законодатель не сделал оговорку, что для признания его преступным необходимо причинение какого-либо материального ущерба, и, кроме того, не указал нижнюю границу такого ущерба. Сравнивая же умышленные преступления «компьютерный

саботаж» и предусмотренное ст. 218 УК «умышленное уничтожение либо повреждение имущества, повлекшее причинение ущерба в значительном размере», мы видим, что уничтожение или повреждение имущества является уголовно наказуемым лишь в случае причинения ущерба на сумму, в сорок и более раз превышающую размер минимальной заработной платы. Тем самым законодатель еще раз подчеркнул большую общественную опасность посягательства на информационную безопасность, чем на отношения собственности.

Так как компьютерный саботаж является умышленным преступлением, то и наказание за это преступление - более строгое, чем за предусмотренное ст. 349 УК неосторожное преступление с аналогичными последствиями: штраф, или лишение права занимать определенные должности или заниматься определенной деятельностью, или арест на срок от трех до шести месяцев, или ограничение свободы на срок до пяти лет, или лишение свободы на срок от одного года до пяти лет.

Часть вторая ст. 351 УК предусматривает квалифицированный состав компьютерного саботажа: **«сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия».** Что понимается под несанкционированным доступом к компьютерной системе или сети, было рассмотрено выше.

В ч. 2 ст. 351 УК нет ссылки на ч. 3 ст. 349 УК, однако, как представляется, перечень тяжких последствий в этих составах должен быть одинаковым. Следует обязательно отметить, что так как в части 2 ст. 351 УК нет указания на неосторожность по отношению к тяжким последствиям, это преступление следует считать умышленным. Поэтому ответственность по части 2 ст. 351 УК наступает только в том случае, если виновный предвидел тяжкие последствия своих действий, желал их наступления (то есть действовал с прямым умыслом) или не желал, но сознательно допускал наступление тяжких последствий либо относился к ним безразлично.

Наказание по части 2 ст. 351 УК – самое строгое, установленное законодателем для преступлений против информационной безопасности: лишение свободы на срок от трех до десяти лет.

2.4.Неправомерное завладение компьютерной информацией

Статьей 352 УК предусмотрена уголовная ответственность за различные способы неправомерного завладения информацией: **«несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации,**

передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда».

В отличие от уголовного законодательства Российской Федерации, которое «копирование информации» называет последствием несанкционированного доступа к ней (ст. 272 УК РФ), белорусские законодатели расценили такое деяние как самостоятельное преступление, что представляется более логичным, ведь копирование информации как таковое не причиняет ей либо компьютерному оборудованию вред. Поэтому копирование информации необходимо рассматривать в рамках объективной стороны преступления не как последствие, а как действие.

В диспозиции статьи 352 УК Республики Беларусь альтернативно перечислены действия, которые раскрывают способы совершения этого преступления:

Несанкционированное копирование информации, хранящейся в компьютерной системе, сети или на машинных носителях – это снятие копии с оригинальной информации без ее повреждения, и сохранение возможности ее использования по назначению (в отличие от уничтожения, изменения и блокирования информации) без разрешения собственника, владельца, уполномоченных ими лиц или правомерного пользователя.

Иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях – это любые незаконные способы получения информации без согласия ее собственника, владельца или уполномоченных ими лиц, а также законного пользователя, либо с их согласия, но против их воли, с целью использования этой информации по своему усмотрению. Примером такого завладения может быть хищение системного блока, а также машинных носителей - компакт-дисков, дискет и т.п. с целью считывания информации. В этом случае завладение компьютерной системой или машинным носителем требует дополнительной квалификации как преступление против собственности – кража, грабеж, вымогательство и т.п. в зависимости от способа хищения имущества, поскольку такое завладение посягает не только на информационную безопасность, но и на отношения собственности.

Перехват информации, передаваемой с использованием средств компьютерной связи – это неправомерное завладение информацией, носителем которой являются не компьютеры, а коммуникационные линии между ними в компьютерных сетях.

Состав рассматриваемого преступления материальный. Оно считается оконченным с момента причинения существенного вреда. Понятие существенного вреда было рассмотрено выше при анализе части 1 ст. 349 УК.

По субъективной стороне неправомерное завладение компьютерной информацией - это умышленное преступление. Действие –

несанкционированное копирование, иное неправомерное завладение компьютерной информацией либо ее перехват - совершается с прямым умыслом, при этом виновный относится к последствию – причинению существенного вреда - как с прямым, так и с косвенным умыслом.

Субъектом этого преступления может быть любое лицо, достигшее 16-летнего возраста.

Наказание – общественные работы, или штраф, или арест на срок до шести месяцев, или ограничение свободы на срок до двух лет, или лишение свободы на тот же срок.

2.5. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Ст. 353 УК Республики Беларусь предусматривает ответственность за **«изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети».**

Предметом этого преступления являются специальные программные и специальные аппаратные средства для получения неправомерного доступа к защищенной компьютерной системе или сети.

Состав рассматриваемого преступления формальный. Оно считается оконченным с момента совершения любого из двух указанных в диспозиции альтернативных действий.

Под изготовлением специальных программных средств понимается создание компьютерных программ, предназначенных для получения неправомерного доступа к защищенной компьютерной системе или сети.

Изготовление аппаратных средств – это создание различных электронных материальных систем этого же назначения.

Как сбыт таких средств расценивается их продажа, дарение, передача в возмездное или безвозмездное пользование, возврат долга и т.д.

Данное преступление совершается только с прямым умыслом. Обязательным признаком субъективной стороны является специальная цель при изготовлении предметов преступления – цель их сбыта. Таким образом, само по себе изготовление специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети без цели их сбыта, а для собственного пользования, уголовно не наказуемо.

Корыстная цель не является обязательным признаком рассматриваемого преступления, поэтому даже безвозмездная передача указанных специальных средств признается преступлением.

Субъект этого преступления – общий, лицо, достигшее 16-летнего возраста.

Наказание – штраф, или арест на срок от трех до шести месяцев, или ограничение свободы на срок до двух лет.

2.6. Разработка, использование либо распространение вредоносных программ.

Ст. 354 УК Республики Беларусь предусматривает ответственность за **«разработку компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработку специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами».**

Общественная опасность этого преступления обусловлена тем, что вредоносные программы способны в любой момент парализовать работу компьютерной системы или сети, что может привести к самым тяжелым последствиям.

Предметом этого преступления являются вредоносные компьютерные программы. Что характерно, вредоносность или полезность программы применительно к этому составу преступления следует определять не в зависимости от ее основного назначения или просто способности блокировать, модифицировать или копировать информацию, а по следующим двум условиям. Первое – предполагает ли действие таких программ предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы. Второе – предполагает ли программа получение их согласия (то есть санкции) на реализацию программой своего назначения. Если программа не отвечает хотя бы одному из этих двух условий, она признается вредоносной.

Вредоносными являются программы, содержащие участки кода с реализацией алгоритмов «почтовая бомба», «троянский конь», «асинхронная атака», «люк» «червь» и других подобных, либо в которых имеются вирусы. Специальные вирусные программы поэтому также входят в перечень предметов этого преступления.

Вредоносность «компьютерных вирусов» связана с их свойством самовоспроизводиться, переходить через коммуникационные сети из одной системы в другую, проникать в ЭВМ, т.е. распространяться, как вирусное заболевание, и создавать помехи работе на компьютере без ведома и санкции добросовестного пользователя. Чаще всего сбои в работе компьютера сопровождаются полным или частичным уничтожением

информации. Вирусные программы обычно включают команды, обеспечивающие самокопирование и маскировку.

Кроме вредоносных программ, предметом рассматриваемого преступления являются машинные носители с такими программами.

При изложении признаков рассматриваемого деяния белорусские законодатели не совсем удачно использовали законодательную технику и при описании предмета преступления употребили множественное число. Буквальное толкование диспозиции приводит к выводу, что для применения этой статьи необходимо совершить перечисленные действия не в отношении одной, а обязательно в отношении нескольких программ. Вместе с тем, как представляется, для привлечения к ответственности по ст. 354 УК достаточно совершения хотя бы одного из указанных действий и даже только в отношении одной вредоносной программы – разработки, внесения изменений в компьютерную программу, использования вредоносной программы либо распространения носителя с такой программой.

Возникает вопрос – относятся ли к предмету рассматриваемого преступления такие вирусные программы, которые в случае заражения чужого компьютера не приводят к уничтожению, модификации или копированию информации, а только вызывают появление на экранах мониторов стихов, рисунков или нецензурных выражений, и этим их «вредное» действие ограничивается. Представляется, что если такие программы, пусть они и являются вирусными, не приводят к уничтожению, изменению, блокированию или копированию информации, то они не являются вредоносными и поэтому перечисленные в диспозиции действия в отношении таких программ не должны признаваться преступными. По мнению В.С. Комиссарова, «применение в таких случаях мер уголовно-правового характера будет не только бессмысленным, но и нарушающим основополагающие принципы уголовного права» [5, с.17].

По объективной стороне состав рассматриваемого преступления – формальный. Любое из перечисленных в диспозиции ст. 354 УК действий образует оконченное преступление, независимо от наступления вредных последствий – уничтожения, блокирования, модификации или изменения информации. По сути, законодатель приравнял вредоносные программы к таким изъятым из оборота предметам и веществам, как оружие, радиоактивные вещества, наркотические средства и т.п., признав преступными сами действия в отношении вредоносных программ.

Рассмотрим эти альтернативные действия.

Под разработкой вредоносных программ понимается написание их текста (алгоритма) как последовательности логических команд и последующее преобразование его в машинно-читаемый язык, независимо от введения его в память компьютера или без такого введения в память.

Внесение изменений в существующие программы – это их модификация, то есть изменение текста программы путем исключения его фрагментов, замены их другими, дополнения текста программы. Изменение признается уголовно-наказуемым только в том случае, если виновный исправил работающую в компьютере программу либо распространил исправленную программу на любом носителе. Исправление изложенной на бумаге программы не образует состав этого преступления.

Как заведомое использование специальных вирусных программ расцениваются любые действия по введению этих программ в оборот, кроме распространения носителей с такими программами (что предусмотрено как самостоятельное деяние в данной статье), либо самостоятельное их применение в отношении чужой компьютерной информации. Понятно, что распространение программ без передачи их носителя возможно только по компьютерной сети – локальной, региональной или международной. Использование таких программ для личных нужд, к примеру, в целях уничтожения собственной компьютерной информации, не наказуемо.

Распространение носителей со специальными вирусными программами – это передача машинных носителей с такими программами третьим лицам как за плату, так и бесплатно, как в постоянное владение, так и временно.

Данное преступление может быть совершено только с прямым умыслом. Обязательным признаком субъективной стороны при совершении таких действий, как разработка компьютерных программ или внесение изменений в существующие программы, является специальная цель – цель несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе. При отсутствии такой цели разработка программ и внесение изменений в существующие программы не наказуемы. Для признания преступными остальных действий, связанных со специальными вирусными программами, наличие такой цели не обязательно.

Следует отметить, что уголовно-наказуемым будет заведомое использование вредоносных программ как в том случае, когда они используются для заражения других компьютеров, так и тогда, когда они используются в целях защиты своего программного обеспечения, баз данных и другой информации от несанкционированного копирования. Мотивы преступления на квалификацию не влияют.

Субъект этого преступления – общий, лицо, достигшее 16-летнего возраста. Ответственность по ст. 354 УК несут не только разработчики вредоносных программ, но и другие пользователи, которые могут использовать или распространять эти программы.

Наказание по части 1 ст. 354 УК – штраф, или арест на срок от трех до шести месяцев, или ограничение свободы на срок до двух лет, или лишение свободы на тот же срок.

Часть 2 ст. 354 УК предусматривает квалифицированный состав и устанавливает наказуемость за **«те же действия, повлекшие тяжкие последствия».**

Наказание в этом случае - одно из самых строгих, установленных законодателем для преступлений против информационной безопасности: лишение свободы на срок от трех до десяти лет.

Тяжкими в смысле части 2 ст. 354 УК должны быть признаны перечисленные в части 3 ст. 349 УК последствия - крушение, авария, катастрофа, несчастные случаи с людьми, отрицательные изменения в окружающей среде. К тяжким также необходимо относить такие прямо не указанные в части 3 ст. 349 УК последствия, как причинение особо крупного материального ущерба, уничтожение, блокирование, модификация или копирование информации особой ценности и т.д.

Для привлечения к ответственности по части 2 ст. 354 УК необходимо установить, что виновный относился к последствиям с прямым или косвенным умыслом, так как в этой части ст. 354 УК нет указания на неосторожную форму вины. Причинение этих же последствий, но по неосторожности, должно влечь ответственность по совокупности преступлений, предусмотренных ч. 1 ст. 354 УК и статьями о неосторожных преступлениях против человека или собственности.

2.7. Нарушение правил эксплуатации компьютерной системы или сети.

Ст. 355 УК Республики Беларусь предусматривает ответственность за **«умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда».**

Необходимо отметить, что предусмотренные ст. ст. 349 и 355 УК преступления имеют много схожего. Основное отличие между ними заключается в санкционированности или несанкционированности доступа, влекущего перечисленные последствия. В рассматриваемом составе, предусмотренном ст. 355 УК, предусмотрен именно правомерный (то есть санкционированный) доступ.

Состав этого преступления – материальный. Нарушение установленных правил эксплуатации ЭВМ или сети ЭВМ может быть

совершено как действием, так и бездействием. При совершении этого преступления действием ненадлежаще исполняются указанные правила либо прямо нарушаются установленные в этих правилах запреты. Бездействием является невыполнение таких правил вовсе.

Фактически такое нарушение может выражаться либо в несоблюдении, либо в игнорировании определенных правил аппаратного или программного обеспечения безопасности компьютерной системы или сети – к примеру, это использование машинных носителей информации без проверки на наличие «вирусных» программ, несоблюдение последовательности операций, неправильное подключение периферийных устройств и т.п.

Как видно, диспозиция части 1 ст. 355 УК – бланкетная. Правила эксплуатации компьютерных систем и сетей определяются либо нормативными актами других отраслей права, либо разрабатываются производителями технических средств и поставляются с ними, либо определяются собственником или владельцем этих технических средств. Поэтому всегда необходимо обращаться к этим правилам для того, чтобы установить, какое же конкретно требование и какого нормативного акта, инструкции, правил эксплуатации нарушил виновный. При этом следует учитывать, что по данной статье наказывается нарушение не любых правил работы с ЭВМ, а только технических правил эксплуатации. Поэтому, как справедливо отмечал В.С. Комиссаров, нарушение организационных форм работы ЭВМ и их правовой регламентации не образует состава рассматриваемого преступления [5, с.18].

Данное преступление считается оконченным с момента наступления указанного в диспозиции последствия - причинения существенного вреда. Понятие существенного вреда раскрывается путем перечисления: это уничтожение, блокирование, модификация компьютерной информации, нарушение работы компьютерного оборудования или иной существенный вред. Этот вред может быть причинен как собственнику, владельцу или пользователю, так и третьим лицам (в случае, к примеру, если проведение лечебных мероприятий проводится под контролем компьютера и больному причиняется вред здоровью). Что понимается под перечисленными последствиями, было рассмотрено выше.

По субъективной стороне это преступление является неосторожным. Деяние – нарушение правил эксплуатации – совершается умышленно, о чем имеется прямое указание в диспозиции статьи, однако отношение к последствиям может быть только неосторожное. Соответственно, неосторожное нарушение правил, повлекшее причинение существенного вреда, не может быть признано преступным.

Как представляется, обязательным для привлечения к ответственности по этой статье должно быть установление факта

доведения правил лицу, имеющему доступ к компьютеру, так как лицо, не знающее правил эксплуатации, компьютерной системы или сети, умышленно эти правила нарушить не может. Презумпция знания закона в данном случае неприемлима, так как эти технические правила эксплуатации устанавливаются не законами.

Если отношение виновного лица к последствиям было умышленное, то содеянное должно быть расценено как умышленное преступление - компьютерный саботаж - и влечь наказание по ст. 351 УК.

Субъект данного преступления, в отличие от состава, предусмотренного ст. 349 УК, специальный: это достигшее 16-летнего возраста лицо, имеющее доступ к компьютерной системе или сети, то есть законный пользователь. Кто понимается под этим специальным субъектом, рассмотрено выше при анализе части 2 ст. 349 УК.

Наказание по части 1 ст. 355 УК – штраф, или лишение права занимать определенные должности или заниматься определенной деятельностью, или исправительные работы на срок до двух лет, или ограничение свободы на тот же срок.

Часть 2 ст. 355 УК предусматривает ответственность за **«то же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности».**

Понятие «информация особой ценности» – оценочное. К ней может быть отнесена информация, имеющая государственное значение, составляющая государственную тайну, результаты исследований, в которых принимали участие большие коллективы в течении длительного времени, и т.п.

Что примечательно, законодатель в части 2 ст. 355 УК вновь употребляет термин «то же деяние». Однако под «деянием» понимаются только действие или бездействие. Деяние не включает в себя последствия. Поэтому, если толковать дословно часть 2 ст. 355 УК, то под «тем же деянием» здесь необходимо понимать именно деяние, указанное в части 1, то есть «нарушение правил эксплуатации компьютерной системы или сети». Следовательно, нарушение правил эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, следует признавать оконченным преступлением даже в том случае, если не наступили перечисленные в части 1 последствия, являющиеся существенным вредом. Таким образом, в части 2 ст. 355 УК предусмотрен не квалифицированный, а основной состав умышленного преступления, причем этот состав является формальным.

Наказание по части 2 ст. 355 УК – лишение права занимать определенные должности или заниматься определенной деятельностью, или ограничение свободы на срок до трех лет, или лишение свободы на тот же срок.

В части 3 предусмотрен материальный состав с неосторожной формой вины. В ней установлена ответственность за **«деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части 3 ст. 349 настоящего Кодекса»**.

Содержание этих последствий было рассмотрено выше.

Наказание – ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

ЗАКЛЮЧЕНИЕ

Кажется, только недавно белорусские законодатели криминализировали деяния в сфере компьютерной информации. Однако, развитие технических средств и программного обеспечения всегда будет опережать правовое регулирование информационных отношений, в связи с чем появление в недалеком будущем «пробелов» в республиканском законодательстве, в том числе и в Уголовном Кодексе, неизбежно. Поэтому особенно важным сегодня становится деловое взаимодействие технических специалистов и юристов с целью развития теории уголовного права и своевременной реакции законодателя на технический прогресс, привлечение инженеров-программистов к разработке мер профилактики преступлений против информационной безопасности и методик их расследования.

НОРМАТИВНЫЕ ИСТОЧНИКИ И ЛИТЕРАТУРА по теме «Преступления против информационной безопасности»

1. Уголовный Кодекс Республики Беларусь // Национальный реестр правовых актов Республики Беларусь. 15 октября 1999г. № 76.
2. «Об информатизации»: Закон Республики Беларусь от 6 сентября 1995г. № 3850-XII // Ведомости Верховного Совета Республики Беларусь. Ноябрь 1995 г. № 33(179), ст. 428.
3. Уголовный Кодекс Российской Федерации. По состоянию на 15 февраля 1999 года. – М.: Издательство «ОЛМА-ПРЕСС»; Новосибирск: ООО «Издательство ЮКЭА», 1999.
4. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. / Под ред. акад. Б.П.Смагоринского – М.: Право и Закон, 1996.
5. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность. – Юридический мир. 1998. № 2. С.9-19.
6. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. Под общей редакцией Ю.И.Скуратова и В.М. Лебедева. – М., Издательская группа Инфра.М-НОРМА, 1996.
7. Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа Инфра.М-НОРМА, 1997.
8. Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. – М.: Гелиос, 1998.
9. Лукашов А.И., Саркисова Э.А. Уголовный кодекс Республики Беларусь: сравнительный анализ и комментарий. – Мн.: «Тесей», 2000.
10. Мороз В.В., Безлюдов О.А. Уголовное право Республики Беларусь (общая часть): Учебник. Мн.: БелНИУФЭ, 1997.
11. Российское уголовное право. Особенная часть: Учебник / Под ред. М.П. Журавлева и С.И. Никулина. М.: Издательство «Спарк», 1998.
12. Савенок А.Л. Информационные преступления и действие уголовного закона в пространстве. – Проблемы законности и правопорядка в Республике Беларусь / Материалы республиканской научно-практической конференции. – Новополоцк: ПГУ, 2000. С.283-285.

Учебное издание

Преступления против информационной безопасности

Методические рекомендации по курсу:
Уголовное право Республики Беларусь.
Особенная часть

Для студентов юридического факультета,
обучающихся по специальности «Правоведение»

Составитель: Лосев В.В.

Редактор: Коклюхин В.В.

Ответственный за выпуск: Гребельная С.К.

Подписано в печать 17.10.2000. Формат 60x84/16. Бумага офсетная.
Гарнитура Таймс. Печать плоская. Усл. печ. л. 2,6. Уч.-изд. л. 2,7.
Тираж 100 экз. Заказ № 309. Цена договорная.
Издатель и полиграфисполнение
Брестский государственный университет им. А.С. Пушкина.
224665, Брест, Советская, 8.
Лицензия ЛВ №307 от 1.07.98.
Лицензия ЛП №260 от 30.04.98.