**Тема № 7. Правовые и организационные основы обеспечения информационной безопасности в компьютерных сетях**

ПЛАН

Введение

1. Защита коммерческой тайны

2. Техническая охрана

3. Предупреждение преступлений, совершенных в использовании компьютерных технологий

Выводы

**Введение**

Интенсивное внедрение информационных технологий в области экономики, управления и, особенно, в кредитно-банковский вызвало появление нового класса преступлений-преступления, совершенные с использованием компьютерной технологии или преступление в использовании (компьютеров), систем и компьютерных сетей.

Распространение компьютерных вирусов, мошенничество с использованием пластиковых платежных карт, украсть деньги с банковских счетов, кражи компьютера и нарушение правил эксплуатации автоматических электронных вычислительных систем-это не исчерпывающий перечень таких преступлений. Вот почему проблема их счетчик имеет важное значение как для ДНР, так и для многих других стран. Особенность заключается в том, что такое преступление, как неотъемлемой части уровень общей преступности, каждый год имеет тенденцию к обострению и транснациональных. Такие незаконные действия уже сегодня представляют общественную опасность, действительно угрозы информационной безопасности – элементом национальной безопасности. Национальной инфраструктуры тесно связаны с использованием современных компьютерных технологий. Повседневной деятельности банковских и энергетических систем, воздуха управления движением, транспортной сети, любой (сущности, полностью зависят от надежной и безопасной эксплуатации автоматизированных электронных вычислительных систем.

Как любой новой технологии создают новые виды преступной деятельности, поэтому каждый новый тип преступности требует новых мер защиты и методы работы правоохранительных органов.

Быстрое развитие информатизации в ДНРнесет в себе потенциал для использования компьютерных технологий с топором молоть. Анализ законодательства, регулирующего отношения общественной информации в ДНР, позволяет утверждать, что нашего государства, а также меры по стимулированию развития инфраструктуры на основе новейших технологий, принимает необходимые меры против компьютерных преступлений.

**Вопрос 1**

**Защита коммерческой тайны**

Условно различают два вида общественной информации, которые используются в бизнесе, это два вида информационной безопасности: пассивный и активный.

Пассивная защита характеризуется тем, что владелец информации дает ему режиме открытость, доступность для всех заинтересованных сторон, но эти лица не могут использовать его для коммерческих целей. Он принадлежит владельцу исключительное право уполномочить кого-то использовать эту информацию. Следующие сведения безопасности набор патентов и авторского права. Для защиты интересов собственника в случае несанкционированного использования будет реализовываться в судах на основании законодательства.

Примеры информационных объектов, для которых их владельцы распространение пассивной защиты, довольно много: Изобретения, полезные модели, промышленные образцы (дизайн), товарные знаки, бренд, музыкальных, драматических, литературных, и аудиовизуальных написание достижений различного характера, компьютерные программы, лекций и т.д.

Активная защита информации, которая является более подходящим для защиты коммерческой тайны против владелец несанкционированного использования, с тем, что владелец указывает, что режим определенного доступа, например, ограничивает доступ к информации от узкого круга специалистов из числа сотрудников, организовать зону безопасности на предприятии, с использованием средств массовой информации, которые делают его невозможным несанкционированное копирование, и т.д.

Пример информации, которые могут подпадать под активной защиты и представляют собой коммерческую тайну информации может служить тип «ноу-хау», т.е. технической информации – режимы, методы, процесс карты и т.д., результаты различных исследований, методы управления, а также информационные объекты, которые являются столь значительную коммерческую ценность, что владелец – по соображениям целесообразности или безопасности – обеспечивает информационный режим для ограничения доступа.

На сегодняшний день, потери коммерческой тайны в ДНРспособствует для ее защиты. Наблюдается разделить усилия государственных и частных предпринимателей для обеспечения целостности информации, отсутствие владельцев коммерческой тайны организационного опыта для его защиты, недостаточностью правовой подготовки и информационной культуры.

Применения организационного и правового механизма для защиты коммерческой тайны сталкиваются с целым рядом нерешенных проблем, среди них отсутствие четкого определения понятия «коммерческая тайна», принимая во внимание интересы юридических и физических лиц; Разработка механизма для осуществления прав собственности на информацию, за коммерческой тайны; методы для определения его значение; определение органа государственной исполнительной власти, который будет создавать и реализации государственной политики по защите прав на коммерческую тайну, и т.д.

Что касается режима доступа к информации ее установки регулируется искусства. 28 Закона ДНР «об информации», определяет порядок правовых норм предоставляются для получения, использования, распространения и хранения информации. Режим доступа к информации состоит из открытых информацию и информацию с ограниченным доступом, который, в соответствии с их правовой режим является конфиденциальной и секретной. Согласно ст. 30 упомянутого закона конфиденциальной информации является информация, которые находятся в владения, использования или удаления определенных физических или юридических лиц и по их просьбе, в соответствии с предусмотрено их условия.

Искажение информации меняется его содержание, нарушение его целостности, включая частичное разрушение.

Граждане, юридические лица, имеющие профессиональный, Бизнес-информация, производство, банковские, коммерческие и иные, держать свои собственные средства или, которая является предметом их профессиональных, Бизнес, производство, банковские, коммерческие и другие интересы и не нарушать законом тайну имеют право самостоятельно определять режим доступа к нему, включая принадлежность к категории конфиденциальной информации и установить его в систему (пути).

Последняя информация, что который содержит информацию, которая представляет государство или другие секретный закон предусматривает раскрытие из которых вред личности, общества и государства.

Среди ученых есть два основных подхода к концепции информационной безопасности.

Первый подход основан на оценке концепции информационной безопасности как широкого явления, частью которого является защита информации. Например, м. Арсентьев считает, что информационная безопасность является удаление информации неопределенность в отношении объективно и субъективно существующие фактические и потенциальные угрозы через контроль над глобального информационного пространства и наличия возможностей, условий и средств борьбы с этими угрозами вместе определяет уровень информационной безопасности (степень) каждого предмета.

Другая группа ученых связывает информационной безопасности с защитой информации. Хотя концепция информационной безопасности трактуется по-разному. Например, Статье и Теньков определяют информационной безопасности как безопасность информации и инфраструктуры, которая поддерживает, с населением программного обеспечения, аппаратных и программных средств и методов, а также организационные меры для того, чтобы предотвратить повреждение владельцев этой информации или инфраструктуры, которая поддерживает.

Легитимизованная сущность категории «информационная безопасность» подала законодателем в концепции национальной программы информатизации (утверждена Законом ДНР от 4 февраля 1998 года № 75/98 - ВР). *«Информационная безопасность» является неотъемлемой частью политической, предпринимательской, обороны и других компонентов национальной безопасности.* Объекты информационной безопасности являются информационные ресурсы, каналы обмена информацией и телекоммуникаций, механизмы функционирования телекоммуникационных систем и сетей и другие элементы информационной инфраструктуры страны.

На основании содержания концепции «информационная безопасность» лежит понятие «безопасность». Что касается вышесказанного, информационная безопасность можно определить, как состояние защищенности жизненно важных интересов личности, общества и государства в информационной среде от внешних и внутренних угроз. Информационная среда является сферой деятельности субъектов, связанный с информацией о создании, реорганизации и потребления.

Таким образом, информационная безопасность является состояние защищенности жизненно важных интересов личности, объектов, общества государства в информационной среде от внешних и внутренних угроз, которая обеспечивает его формирования, использования и развития в интересах граждан, общества и государства.

Содержание категории «информационная безопасность» считает развитие в сложных правовых документов относительно использования технологии (компьютер) для обработки и хранения информации советника, государственных стандартов документации, техническое обслуживание, использование, сертификационные испытания компьютерного программного обеспечения для защиты данных, средств диагностики, локализации и предотвращения компьютерных вирусов, новые технологии защиты информации с помощью спектральных методов, надежность криптографические методы защиты и т.д.

Что касается определения органа государственной исполнительной власти, который будет создавать и реализации государственной политики по защите прав на коммерческую тайну, в Закон ДНР «о службе безопасности ДНР» в статье 25, что обязанности СБУ «для оказания помощи в порядке, установленном законом, предприятий, учреждений, организаций и предпринимателей в сохранении коммерческой тайны, раскрытие которой может нанести ущерб жизненно важным интересам ДНР.» Как вы можете видеть, формулировка положения не позволяют четко определить, является ли СБУ органом государственной исполнительной власти, который будет создавать и реализации государственной политики по защите прав на коммерческую тайну, или нет. Кроме того, законодательство не определяет, что понимается под термином «облегчить», а также механизм «акции».

Специальный вид конфиденциальной информации является информация, которая является государственной тайной. В соответствии с законодательством ДНР такая информация является:

1) в области обороны:

-содержание стратегических и оперативных планов и других документов, боевого управления, подготовки и проведения военных операций, стратегический и развертывания войск, а также другие важные показатели, которые характеризуют Организации, прочность, распоряжения, боевых действий и готовности, боевой и другие военной подготовки, и материально-технического обеспечения вооруженных сил ДНР и других военных формирований;

-о возможностях гражданской обороны ДНР, возможности районов, регионов и отдельных объектов для защиты, эвакуации и рассредоточения населения, обеспечить его жизни и деятельности объектов национальной экономики в военное время или чрезвычайных ситуаций;

-геодезические, гравиметрические, картографических и метеорологических данных и характеристик, которые имеют важное значение для обороны страны;

2) в области экономики, науки и технологии:

-планы мобилизации и мобилизационных возможностей экономики ДНР, резервы и объем поставок стратегического сырья и материалов, а также резюме диапазона и уровня накопления, на общие объемы поставок, уплотнение, пополнения, и фактических запасов государственного заповедника;

-планы, содержание, финансирование и осуществление государственного заказа для обеспечения безопасности и оборонных нужд;

-о планах, объемы и другие важные показатели горного производства и реализации некоторых стратегического сырья и продуктов;

-о состоянии запасов драгоценных металлов денежной группы, драгоценных камней, валюты и других ценностей, операций, связанных с производством банкнот и ценных бумаг, их хранения, защиты от подделки, торговля, Обмен или вывод из обращения;

-о научных, исследования, разработки и дизайна, работы, на основе которой могут быть созданы передовые технологии, новые виды производства и технологических процессов, которые имеют важные обороны или предпринимательской ценности, или значительное влияние на экономическую деятельность и национальной безопасности ДНР;

3) в области международных отношений:

-директив, планов, указав делегаций и должностных лиц по вопросам внешней политики и внешнепредпринимательской деятельности ДНР, направленных на обеспечение его национальных интересов и безопасности;

-о военной, научно -технического и иного сотрудничества с иностранными государствами, если раскрытие такой информации будет вред национальной безопасности ДНР;

-экспорт и импорт оружия, военной и специальной техники, отдельных стратегического сырья и продуктов;

4) в сфере государственной безопасности и общественного порядка:

-сотрудников органов, осуществляющих оперативно розыскной деятельности;

-инструменты, содержание, планы, финансирование и материально-технического обеспечения, форм, методов и результатов оперативно розыскной деятельности; о лицах, приватно сотрудничать или сотрудничал в прошлом с органами, которые осуществляют такую деятельность; о составе и конкретных лиц, которые являются наемного органов, осуществляющих оперативно розыскную деятельность;

-об организации и процедуре государственных административных зданий и других государственных учреждений, должностных лиц и других лиц, защита которых осуществляется в соответствии с законом «о государственной защите государственных органов и должностных лиц;

-системы управления и особых случаев;

-по организации, содержание, статус и планов развития криптографической защиты секретной информации, содержание и результаты научных исследований в области криптографии;

-другие средства, формы и методы защиты государственных секретов.

Кроме того, информация защищена должно быть предметом собственности и защиты юридических документов и требований, которые задаются сведения о владельце (владелец информации может быть государство, юридическим лицом, группой лиц, частным лицом).

**Вопрос 2.**

**Техническая охрана**

Одним из наиболее важных частей защиты информации является технической защиты. Утечки информации в компьютерных системах могут быть допущены как случайно и преднамеренно, с применением технических средств снятия информации.

Анализ действующего законодательства информация показывает, что украинские законодатели основном соединяет сущность категории «информационная безопасность» из категории «информационной безопасности автоматизированных систем». Эта категория также имеет определение на законодательном уровне как системный фактор (объект) правовой правовое регулирование отношений общественной информации, связанные с использованием систем автоматизированного (компьютер). В нашей стране в области общественных отношений служит Закон ДНР «о защите информации в автоматизированных системах».

Информационной безопасности компьютерных систем тесно связана с обеспечением информационной безопасности. Она включает в себя инструменты и набор действий, направленных на использование физические, организационные и программно-технических средств охраны, которая должна обеспечить для идентификации пользователей, распределения полномочий доступа к системе, регистрации и учета незаконных, несанкционированных вмешательств.

Таким образом, информационная безопасность является состояние защищенности жизненно важных интересов личности, объектов, общества государства в информационной среде от внешних и внутренних угроз, которая обеспечивает его формирования, использования и развития в интересах граждан, общества и государства.

*Среди различных классификаций безопасности угрозы могут быть определены следующим образом:*

*1.* *Источник:*

-внешние – угрозы, связанные с стихийные бедствия, технологические, политические и социальные факторы, развитие информационных и коммуникационных технологий и других внешних воздействий;

-внутренний-угрозы, относящиеся к сбоям компьютера и коммуникационного оборудования, ошибки программного обеспечения.

*2.* *Природа возникновения:*

-природные (цель)-угрозы, вызванные воздействие на информацию среды объективные физические процессы или природных явлений, не зависящим от воли лица;

-искусственные (субъективного) – угрозы, вызванные влиянием информационной среды человека.

Среди антропогенных угроз различать:

-непреднамеренных угроз (случайных) – ошибки программного обеспечения, кадров, компьютер и коммуникационного оборудования и т.д.;

-умышленное угрозы – несанкционированный доступ к информации, разработка специального программного обеспечения, которое используется для изготовления такого доступа, развития и распространения вирусных программ, и т.д. поддерживает угрозы, вызванные действиями людей и сосредоточена на незаконное нарушение конфиденциальности, целостности или доступности информации, а также использование ресурсов в своих собственных целях.

*3. на основе воздействия:*с помощью; использование скрытых каналов.

*4. с целью реализации:*нарушение конфиденциальности, целостности; нарушение доступности.

*5. характер воздействия:*активные, пассивные.

*6. объект воздействия:*угроз, которые влияют на информационные среды в целом; угроз, которые влияют на отдельные элементы.

*7. путем влияния на объект атаки:*те, которые непосредственно влияют на объект нападения; косвенно влияет на объект нападения.

Кроме того, в литературе, на основе данных статистики, попытка классификации основных угроз согласно степени их опасности, (принимая во внимание вероятность их проявления и стоимости ликвидации последствий):

-несанкционированного доступа (первое место);

-огонь;

-намеренно нарушение нормальной работы (вирусной инфекции, преднамеренного введения искаженных данных, преднамеренного вывода отказа оборудования и его похищение) – статистика, некоторые страны называют угрозу стоит на втором месте;

-использование программного обеспечения, которое содержит ошибки.

Таким образом основные проблемы информационной безопасности, связанных, прежде всего, смежных угроз (действия), поскольку они являются главной причиной поплавка и сила преступлений и правонарушений. Согласно статистике, это незаконное вмешательство в эксплуатацию автоматических электронных вычислительных систем являются самыми опасными. Ежегодные потери от указанного вида преступности постоянно растут. По данным бухгалтерского учета правительство Соединенных Штатов Америки палата ежегодные потери от краж и мошенничества, совершенных с использованием информационных технологий только через Интернет, как высоко как $5 млрд.

Контрмеры утечки случайной информации, причиной которых может быть программно-аппаратный сбой или человеческий фактор можно подразделить на следующие функциональные группы: дублирование информации, повысить надежность компьютерных систем, создания отказоустойчивых компьютерных систем, оптимизации взаимодействия человека и компьютера системы, свести к минимуму потери от аварий и стихийных бедствий (в том числе путем создания распределенных компьютерных систем), блокировка ложных срабатываний.

Общие для всех преступлений в районе изучали тот факт, что они связаны с или вмешательство в работу компьютера (компьютеры) систем и компьютерных сетей или с использованием компьютерных технологий в качестве инструмента. Специальные общественной опасности преступлений, связанных с незаконным доступ к компьютерной информации определяется следующими факторами:

1. интенсивное осуществление различных информационных технологий и процессов, основанных на использовании компьютеров, во многих областях человеческой деятельности.

2. высокий уровень задержки в этой области.

3 относительная доступность широкого круга людей, специальных знаний и методов, необходимых для совершения преступлений.

Наибольший интерес представляет собой преднамеренное изменение информации, также известный как промышленные (технический) шпионаже.

В то время как защита информации в компьютерных системах (CS) от традиционных шпионажа и саботажа используется же средства и методы защиты и защиты других объектов, которые не используются КС. Для защиты объектов КС от угроз данного класса необходимо решать следующие задачи:

• Создайте объект системы;

• Организация работы с конфиденциальной информацией ресурсы для КС;

• противодействие наблюдения;

• Предотвращение подслушивания;

• Защита от преступных действий.

Сведения о компьютере, который все еще может быть идентифицирован как информация записана на телекоммуникационных каналов машина копирования или информации в виде восприятия, доступных компьютеров, можно классифицировать по следующим признакам:

из-за ее родной: записанные на магнитной ленте, флоппи-диск (дискету), лазерные диски, жесткий диска (жесткий диск), память компьютера, компьютерной системы или сети;

-внешний вид: текст, графика, звук, программное обеспечение, файлы данных;

-для атрибутов файла: Архив, только для чтения, система, скрыты. Возможности классификации и другие функции.

Изучение практики функционирования систем обработки данных и компьютерные сети показали, что существует множество возможных путей утечки информации и как несанкционированный доступ к ней систем и сетей:

-Перехват электронного излучения;

-Сила электромагнитного облучения (подсветка) линии;

-Использование «прослушивания» устройств;

удаленное изображение захвата;

-перехвата акустических волн излучения;

-кража средств массовой информации и промышленных отходов, обработки систем;

-чтение информации из массивов других пользователей; o чтения остаточной информации в оборудовании;

-чтобы скопировать медиа-файлы с преодоления мер защиты;

-модификация программного обеспечения путем устранения или добавление новых функций;

-использовать недостатки операционных систем и прикладного программного обеспечения;

незаконных подключений к линии оборудования и коммуникаций, включая как активный ретранслятор;

-вредоносных выход недостаточность механизмов;

-Когда маскировки зарегистрированного пользователя и назначение его полномочий;

-введение новых пользователей;

-внедрение компьютерных вирусов.

Криминологические исследования показывают:

1) 52% установленных правонарушителей прошли специальную подготовку в области автоматизированной компьютерной обработки информации;

2) 97% являлись служащими государственных учреждений и организаций, которые использовали компьютерных систем и информационных технологий в их повседневной деятельности;

3) 30% из них были непосредственно связаны с эксплуатации средств компьютерной техники.

Имеет место и совершения преступлений сотрудниками организаций, которые занимают ответственные посты. Эксперты указывают, что более чем на 25% компьютерных преступлений, совершенных лидерами организаций. Современные руководители, как правило, специалисты высокого уровня, имеют достаточную подготовку компьютера и профессиональные знания, иметь доступ к информации по широкому кругу и может отдавать приказы, но не непосредственно отвечает за работу компьютерной системы.

**Вопрос 3.**

**Предотвращение преступлений, совершенных в использовании компьютерных технологий**

Особенно острые вопросы информационной безопасности как одного из важных компонентов безопасности, предпринимательской деятельности, а также национальной безопасности государства в целом, возникает в контексте появления транснациональной компьютерной преступности и кибертерроризма. ***Под компьютерный терроризм (kìberterorizmom)*,**вы должны понимать нападение на информации, которая обрабатывается компьютером, компьютерные системы и сети, которая создает опасность для жизни и здоровья людей или возникновения других серьезных последствий, которые включают материальный ущерб, нарушение общественной безопасности и т.д.

***Киберпреступности (киберпреступности)*–**Этоявление международного значения, уровень которых зависит от уровня развития и внедрения современных компьютерных технологий, сетей, их повсеместного использования и доступа к ним.Внутренней и глобальной практики показывают, что количество клиентов Интернет продолжает быстро расти, и наряду с этого растет и число нападений, которые ежедневно подвергаются воздействию компьютерных систем от внешней среды.

Основная цель киберпреступности это компьютерная система, которая управляет целый ряд процессов, а также информацию, которая циркулирует в них.

Общественное мнение опросы в разных странах и, прежде всего, высокоразвитых, показывают, что среди вопросов, которые волнуют людей большинство киберпреступлений занимает одно из ведущих мест. Кроме того, по мнению экспертов, это за счет использования передовых информационных технологий с целью преступника, а также растущей уязвимости современного индустриального общества сегодня, это явление является более опасным, чем 5 лет назад. Несмотря на усилия многих государств, направленных на борьбу с две бомбы..., их число в мире, но скорее постоянно растет. Эта проблема уже давно перешли границы и стала вопросом международного масштаба.

Проявление находится в виде искажения или уничтожения компьютерной информации или носители такой информации, а также распространение компьютерного вируса. В этом контексте, во время разрушения информации, чтобы понять ее потери, когда информация в использовании (компьютеров), систем и компьютерных сетей перестает существовать для физических и юридических лиц, имеющих право собственности его в полном объеме или ограниченной. Прекращение доступа к информации следует рассматривать как блок. Такие действия могут быть выражены, например, электромагнитное, лазер и другие воздействия на средства массовой информации, в котором он имеет, или что он передается, в формировании сигнала коробки и блоков программ, воздействие которых на информацию, средства массовой информации и средства технической защиты вызывает нарушение целостности информации, ее искажение или уничтожения.

В сфере информационных отношений противоправных действий могут быть направлены на:

-незаконное вмешательство в работу (компьютеров), систем и компьютерных сетей;

-кража, хищение, вымогательство компьютерной информации или завладения его путем обмана или злоупотребления служебным положением;

-нарушение правил эксплуатации компьютера (компьютеры) компьютерной системы или сети.

*Дополнительные*незаконного вмешательства в работу (компьютеров), систем и компьютерных сетей объектов хозяйственной деятельности, получают различные виды ущерба, причиненного их права и законные интересы: например, право собственности, авторское право, право на неприкосновенность частной жизни, личную и семейную тайну, защиту окружающей среды и т.д.

В результате незаконного вмешательства в функционирование компьютерной системы может быть из следующих последствий: нарушение интеллектуальной собственности прав, раскрытие информации, составляющих государственной и коммерческой тайны, раскрытие информации о частной жизни граждан, собственности ущерб в виде потери и б не получил доходы, потерю репутации фирмы, и т.д. опасность данного преступления обостряется, когда исполнитель получает доступ к автоматизированных систем, которые обслуживают в сфере национальной обороны, ядерной энергетики, транспорта, связи, медицины, торговли, денежного обращения и т.д. и, в некоторых случаях все возможные последствия такого вмешательства воздаст предустановленной неизвестны. Даже разработчики компьютерного оборудования или программного обеспечения невозможно предсказать все возможные ситуации, которые могут возникнуть в ходе их работы, особенно если она относится к обратите внимание, что преступные действия.

Опасность незаконного вмешательства в компьютере информации определяется также в степени ее распространения в обществе и высокая, по сравнению с другими преступлениями, степень задержки.

Криминалистично важной компьютерной информации имеет следующие особенности:

1) компьютерной информации обычно большого объема и быстро обрабатываются. Например, компьютер с процессором Pentium с жестким диском, 1 ГБ можно хранить информацию для тысячи томов по 500 страниц каждая;

2) компьютере информацию очень легко и, как правило, без следа, уничтожены. Уничтожить данные компьютера равна 500 страниц текста, достаточно нажать две клавиши в три секунды весь он был удален, то, как сжечь 500 страниц печати текст необходимых специальных условий и значительного периода времени;

3) вычисляется путем информации, то есть, между ним и лицом, которому он принадлежит, не жесткие связи;

4) такого рода информация может быть расположен только на копии машины (дискета, магнитная лента, лазерный диск, полупроводниковых схем и т.д.) в компьютере ОЗУ (RAM);

5) компьютерной информации может быть создан, изменен, скопирован, прикладной (используется) только с помощью компьютера, если у вас есть соответствующие периферийные устройства чтения машина средств массовой информации (дисков, привод лазерных дисков (CD-ROM) диски, цифровые видео диски и т.д.);

6) Эта информация пересылается легко каналы телекоммуникационных сетей связи и информации практически любого размера могут быть переданы любые расстояния.

Также называется, может быть отметить относительную легкость передачи, преобразования, воспроизводство компьютерной информации; При извлечении, он легко хранится в основной источник; доступ в тот же файл, содержащий информацию, может иметь несколько пользователей.

Предметом преступных посягательств в случае незаконного вмешательства в работу (компьютеров), систем и компьютерных сетей может быть конфиденциальной информации, то есть, документально подтвержденную информацию, доступ к которым ограничен в соответствии с законодательством ДНР, классификации информации для защиты, по различным критериям (степень секретности, сведения о владельце, его менеджер, область, способом извлечения) определены в законодательстве ДНР.

*Несанкционированное вмешательство*в работе AEOM, их систем или компьютерных сетей является проникновение этих машин, их систем или сетей и действий, которые изменяют режим работы машины, ее системы или компьютерные сети, или полностью или частично приостановить их работу без разрешения (согласия) соответствующего владельца или уполномоченного, а также влияние на работу с помощью различных технических устройств, которые могут нанести вред работе машины AEOM.

*Компьютерная информация-*это текст, графика или любой другой информации (данных), существует в электронной форме, хранится на соответствующем носителе и могут сделать, изменять или использовать AEOM.

Незаконным может покрываться как случаи проникновения (воздействия) в операционной системе, AEOM или сети (например, проникновение системы один рабочий ПК с другого компьютера) и несанкционированного свою очередь сломанной машины и проникновения ее системы (ее работы), если она осуществляется с помощью специальных технических средств.

*Источник информации –*Это когда информацию, которая принадлежит один законный получатель получает в «руки» другому получателю, с использованием специальных технических средств. прежде всего, законного получателя не потерять возможность владеть этой информации, но способность владеть информацией можно перемещать как один, так и для неограниченного круга лиц.

*Когда потери компьютерной информации*ссылается на отсутствие способности использовать соответствующую информацию. потеря должна рассматриваться не только ликвидации файла, каталога и так далее, в форме, которой было информации, но также чего информацию в таком состоянии, что исключает использование всей или значительной части. *Когда потери компьютерной информации в СМИ* чтобы понять физическое отсутствие соответствующих материалов объектов или такие изменения их свойств, которое приводит к невозможности дальнейшего хранения сведений о компьютере на этих носителях.

*Подделка информации о компьютере — это* создание соответствующей информации, которая может быть для любой другой информации, но эта информация создается лицом, которое не имеет юридического права для создания (также поддельные информации может не иметь соответствующие детали).

*Блокирование информации — это* результат воздействия к КОМПЬЮТЕРАМ и элементы, которые вызвало временное или постоянное неспособность осуществлять любые операции над компьютерные информации. сведения о блокировке, под это определение, рассматривается как результат уголовного (незаконных) влияние на ее

*Нарушение установленного порядка маршрутизации компьютера информации –*Это передачи цифровой информации, а также вмешательство в установленном порядке передачи информации, которая нарушает порядок данного маршрута в маршрутизации информации сведения о компьютере могут быть физические и юридические лица и государственные органы (если порядок маршрутизации набора власти, то эта процедура не является обязательным для других).

*Создание вредоносного программного обеспечения или оборудования*этот набор действий, результатом которого является наличие вредоносного программного обеспечения или оборудования.

*Использование вредоносных программ или оборудования*набор действий, направленных на использование вредоносного программного обеспечения или оборудования.

  Введение в AEOM, их системы или сети с помощью указанного средства по крайней мере один компьютерный вирус — это компьютерная программа способна шагать в, когда вы нарушать нормальную работу AEOM, системы или компьютерные сети, а также уничтожение или повреждение компьютерной информации следует рассматривать *распространение компьютерных*вирусов.

*Программными средствами*существуют различные компьютерные программы, которая создает возможность для незаконного въезда в ваш компьютер, его системы или компьютерные сети, или способствует такой вход воспрещен.

*Под технические средства*средства, любые технические устройства, которые без использования компьютерных программ, сказываются на работе AEOM. Закон предусматривает обязательное свойство, используемое для совершения такого рода преступности программы и технические средства: их способность вызывать утечки, утраты, фальсификации, блокировки компьютера или носители такой информации.

*Преступление проявляется в виде:*несанкционированного продажу или распространение информации с ограниченным доступом, которая хранится в электронные вычислительные машины (компьютеров), автоматизированных систем, компьютерных сетей или хранения такой информации. *Объективная сторона заключается*в действиях, которые лицо незаконно, вопреки воли и желания владельца или законного пользователя осуществляет продажу или распространение информации с ограниченным доступом.

Следует также отметить, что такие продажи или распространения может вызвать ущерб материальный и моральный ущерб владельцу этой информации. Что касается режима доступа к информации ее установки регулируется искусства. 28 Закона ДНР «об информации», определяет порядок правовых норм предоставляются для получения, использования, распространения и хранения информации. Режим доступа к информации состоит из открытых информацию и информацию с ограниченным доступом, который, в соответствии с их правовым режимом является конфиденциальной и секретной. Согласно ст. 30 упомянутого закона конфиденциальной информации является информация, которые находятся в владения, использования или удаления определенных физических или юридических лиц и по их просьбе, в соответствии с предусмотрено их условия. Последняя информация, что который содержит информацию, которая представляет государство или другие секретный закон предусматривает раскрытие из которых вред личности, общества и государства.

*Является проявление преступлений*несанкционированного изменения, уничтожения или блокирование информации, обрабатываемой в компьютеры, автоматизированных систем или компьютерных сетей, или сохраненных на носители информации (предметом специального – человек, который имеет право доступа к такой информации).

*Изменение информации*включает в себя потери оригинального содержания информации, а также отсутствие обновления. эту информацию, которая существовала до его изменения по-прежнему существует, но с другой смысл.

*Уничтожение информации о компьютере*такие изменения в его первоначальное состояние (полное или частичное уничтожение информации на компьютерных носителях), на котором он прекращает свое существование из-за потери качества основных черт. что это не имеет значения, был жертвой копию этих виновным информации, или нет.

*Блокирование информации — это* результат воздействия к КОМПЬЮТЕРАМ и элементы, которые вызвало временное или постоянное неспособность осуществлять любые операции над компьютерные информации. сведения о блокировке, под это определение, рассматривается как результат уголовного (незаконных) влияние на ее

*Объективная сторона преступления выражается в виде:*несанкционированного перехвата или копирование информации, которая обрабатывается в компьютеры, автоматизированные системы, компьютерные сети, если это привело к его утечке.

*Когда несанкционированный перехват*относится к действию, направленные на получение информации, который был отправлен от одного получателя другой. в этом случае человек, который был информацию, которую он получает, но эта информация также получает третье лицо.

*Копирование –*эта передача информации или ее части одного из физического носителя в другой. Копирование компьютеринформацияследует признать незаконным, если, когда она осуществляется без разрешения владельца или законного пользователя, или с нарушением порядка.

*Также является незаконность*является нарушением правил эксплуатации AEOM, их систем или компьютерных сетей, которые могут быть сделаны как определенные действия и, бездействия, при условии возникновения в результате нарушения этой статьи.

*В соответствии с правилами эксплуатации*AEOM, их систем или компьютерных сетей, чтобы понять любое из правил, которые регулируют использование машин, систем или сетей, проведение работ с их использованием, защитить этих машин, их систем и сетей, и информации в них и т.д.

Информация, что защита (включая компьютер), который является собственностью государства или защита которых гарантируется государством, должны соответствовать правилам, которые устанавливаются специально уполномоченным государственным органом. В настоящее время этот орган является Департамент специальных телекоммуникационных систем и защиты информации СВ.

*Проявление преступлений* ***— это*** тамобструкции работы AEOM, компьютерных сетей или телекоммуникационных сетей путем массового распространения сообщений электросвязи. *Нарушение AEOM –*он выходит из строя AEOM (AEOM допускает ошибки в процессе, возможность повесить операционной системы AEOM), который является следствием массового распространения сообщений. *Прекращение AEOM –*это невозможность дальнейшей работы по AEOM, что приводит к массовой рассылки сообщений.

*Влияние этих преступлений****.***Исследования и анализ многочисленных случаев на информацию и несанкционированного доступа к нему, чтобы показать, что они могут распространяться на случайных и преднамеренного. преднамеренные угрозы могут быть удовлетворены путем долгосрочного массированной атаке несанкционированного вмешательства или вирусов.

Последствия, которые ведет осуществление угроз: разрушение (потеря) информация, изменения (изменить информацию о ложь, исправить форму и содержание, но который имеет другой смысл), обзор его от посторонних лиц. Цена упомянутых событий могут быть разными: от невинных шуток до ощутимые потери, в некоторых случаях, представляют собой угрозу для национальной безопасности страны. Предупреждение следующие последствия в автоматизированной системы и является главной целью создания систем информации о безопасности полетов. Для создания средства защиты информации необходимо определить характер угрозы, форм и способов их возможного и осуществления.

В юридической литературе предлагает следующую общую классификацию возможных последствий незаконных действий в использовании (компьютеров), систем и компьютерных сетей.

1. нарушение:

) временные расстройства, которые приводят к путанице в чартах рабочий график или других мероприятий, и т.д.;

b) отсутствием системы для пользователей;

в) повреждения оборудования (некоторые практические специалисты считают, что повреждения оборудования, когда это касается незаконного доступа, не дело);

d) повреждение программного обеспечения.

2. потеря значительных ресурсов – деньги, одежду, оборудование, информация.

3. потеря исключительного использования является тем, что определенная информация является ценным для владельца, только до тех пор, как он является владельцем монополии.

4. нарушение прав (авторских, смежных, патент, изобретатель, и т.д.).

Статья 16 Уголовного кодекса предусматривает следующие возможные последствия незаконного доступа к компьютерной информации: уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютера, компьютерной системы или сети.

*Уничтожение информации –*такие изменения в его первоначальное состояние (полное или частичное уничтожение информации на компьютерных носителях), на котором он прекращает свое существование из-за потери качества основных черт. это не имеет значения, был жертвой копию этих виновным информации, или нет.

Термин «разрушения» в научной литературе интерпретируется по-разному. Некоторые полагают, что уничтожение информации заключается в его выбрасывается с физического носителя или получение информации, данных, и т.д. соответствующей материальной формы.

Другие считают, что уничтожение информации, чтобы понять потери из-за невозможности восстановления (например, Савельев).

Ряд экспертов считают, что уничтожение информации – приносит ей полностью или в значительной степени непригодным для использования в других целях (Ляпунов, а. в., Комисаров v. s.).

Другая точка зрения (v. Крылов) на основе сочетания предыдущих подходов: *уничтожение информацию о компьютере –*это полное физическое уничтожение информации или ликвидации таких элементов, которые влияют на изменение существенных признаков идентифицирующей информации.

Существует также довольно простой, но довольно точное определение «уничтожения», как ее стирания из памяти компьютера.

Теоретически, как отметили эксперты программистов можно восстановить любой, даже когда записан в компьютерной информации его извлечения из глубокой памяти. Однако этот процесс является весьма трудоемким.

Вероятность возможности обновления информации с помощью программных средств или получают эту информацию от другого пользователя, не освобождает исполнителя от ответственности.

Уничтожение информации является не переименование файла, где он и само по себе является автоматическое перемещение старых версий файлов последний раз.

Переименование файлов не влияет на качество признаки информацию, которую они содержат, так что, если вам нравится идеально подходит в случае незаконного доступа к компьютерной информации, следующие может рассматриваться как *изменения информации или ее блокировки Блокировка компьютера информации –*он закрыл, причиной отсутствия использования по назначению законного пользователя или владельца.

Термин «блок» также имеет целый ряд определений и толкований среди специалистов. Некоторые авторы полагают, что блокирование является невозможность для использования при сохранении информации. Другие определяют, как искусственные проблемы (препятствия) блокировку доступа пользователей к компьютерной информации, относящейся к его разрушению. По словам Косой, институт, блокировка является неспособность получить доступ к компьютерной информации в течение долгого времени при сохранении той же информации в памяти вашего компьютера.

Каждый из этих определений можно назвать верным. Однако, наиболее успешным является определение ' v.: *блокирование информации —*результат воздействия на компьютеры и элементы, вызвавшие временной или постоянной неспособностью осуществлять любые операции на компьютере. Блокирование информации, согласно этому определению, рассматривается как результат преступного (незаконных) влияния на нее.

*Модификация*изменить данные первоначального состояния (например, реструктуризации или реорганизации базы данных, или добавить записи, содержащиеся в файлах, перевод программ для компьютеров или баз данных с одного языка на другой), которая не изменяет суть объекта.

Вопрос о модификации информации также довольно сложно и таким образом определяется в литературе по-разному.

Например,Косой., Савельев, пытался определите изменение как любые изменения компьютерной информации. Может осуществляться как путем частичной замены первоначальной информации о другой, и добавления новой информации к оригиналу. Модификация будет различные нарушения предыдущих Просмотр презентации: изменение порядка следования частей документа (страниц, пунктов, строк), поражения некоторые части документов других нарушений взаимного расположения документов в базе данных, в тексте документа на сторонние элементы.

Ляпунова, а. в. определить изменения как эффект, характерно появление новых свойств (видимо нежелательные).

Ткаченко v. понимает модификации информации, как она меняется, введение ненужной информации, запасных частей, что делает его трудным для использования.

Таким образом изменение сведений о компьютере можно определить, как сделать любые изменения, которые генерируют его отличие от того, который был введен в систему, и который имеет владельца ресурса.

*Копирование-*передачи информации или его часть от одного из физических носителей в другой. особенностью преступления является, что в некоторых случаях, это не позволяет говорить о копии в обычном смысле. Например, в случае секторальной информации о копировании, копия полностью идентичны с более успешным оригинал. является в этом случае, использовать термин «дублирования».

Тот факт вызова или Обзор компьютерной информации, которая хранится на компьютере копии, является состав преступления. Это необходимо для установления факта передачи информации на другой машина средств массовой информации. Тем временем несанкционированного введение в компьютере информации охраняется законом, может выступать в качестве профессиональной подготовки или попытка совершения умышленного преступления. С терминологической точки зрения «копия» определяется как точное воспроизведение всех вещей; процесс получения копии, копирование данных с сохранением первоначальной информации.

В научной литературе среди ученых имеют два подхода к решению проблемы пути вверх.

Первый (узкий) подход, учитывающий копирование как передачи информации от одного компьютера (оригинал) машина средств массовой информации (компьютер) на другой компьютер или любой другой носитель (например, копирование файлов с компьютера на дискете).

Сторонники этой точки зрения означает, что копирование предполагает использовать в качестве орудия преступления только компьютер и программное обеспечение (принтер, информация о диске, и т.д.).

Сторонники более широкого подхода считают, что копирование является передача информации из формы электромагнитного хранения в любой другой. В этом подходе способ копирования не имеет значения, с тем чтобы защитить подлежит сведения о компьютере, независимо от места его нахождения. Это может быть сделано с помощью фото, видео, переписывание вручную, расшифровки, перехват излучения шума принтера компьютера. Главное, что оригинал результате незаконного доступа к компьютерной информации и все эти записи являются убедительным свидетельством такого доступа.

*Срыв компьютера или сети*включает в себя неисправности компьютера, компьютерной системы или сети, которая препятствует нормальному функционированию компьютерных технологий при условии сохранения его физическую неприкосновенность (например, отображение неверную информацию на экране монитора, нарушение порядка выполнения команд, сети и т.д.).

В случае незаконного вмешательства в работу компьютера (компьютеров), систем и компьютерных сетей, приводит к серьезному ущербу для компьютерного оборудования и тем самым причины значительный ущерб владельцу или тому, кто обладает им вино, подлежит дополнительной квалификации намеренно уничтожения или повреждения имущества.

**Заключение**

Подводя итог всему, упомянутые выше, мы можем заключить, что уровень научно-технического прогресса, что мы имеем сегодня является довольно много факторов, которые могут причинить ущерб любой объект бизнес. Вот почему служба безопасности должны присутствовать на каждом из них.

Таким образом после пересмотра законодательства, которое регулирует социальные отношения в области использования информации,информационно-технического оборудования (компьютеры, их систем и компьютерных сетей, средств массовой информации, и т.д.), мы можем заключить, что эти преступления являются достаточно серьезную угрозу для интересов физических и юридических лиц. На нынешнем этапе развития страны законодатель стал значительно больше преподавателей в сфере ответственности незаконного использования компьютеров, их систем и компьютерных сетей. Это главным образом обусловлено ростом компьютерной преступности.

Анализ законодательства, которое регулирует отношения общественной информации в ДНР, позволяет утверждать, что нашего государства, а также меры по стимулированию развития инфраструктуры на основе новейших технологий, принимает необходимые меры против компьютерных преступлений. пример может служить указ президента «о мерах по развитию национального компонента глобальной информационной сети и обеспечение широкого доступа к этой сети в ДНР», а также раздел 16 «преступления в использовании компьютеров) систем и компьютерных сетей и сетей электронная связь» уголовного кодекса ДНР.

Особенностью этого вида преступлений является, что они нарушают на информации, которая находится на некоторые средства массовой информации – жесткий диск, диск, компакт-диск. В результате информация как объект права, собственности легко переехала в другой предмет собственности без значительного нарушения прав собственности на информацию. Перемещение объекта другого субъекта права собственности является неизбежным и, как правило, приводит к потере данного объекта, главным субъектом права собственности, т.е. является очевидным нарушением его прав собственности.

Опасность копирование и перемещение информации осложняется тем, что это обычно от владельца, храниться и обрабатываться в области доступности субъектов, которые не являются субъектами права собственности на него. Например, автоматизированных систем, включая сети. Учитывая особенности информации как объект права собственности, следует отметить, что в другой информации, очевидно, не отличается от традиционных объектов права собственности.

Следует также отметить, что преступления, указанные в статье 16 Уголовного кодекса ДНР очень трудным для изучения, потому что профессиональные преступные деяния, обычно с вредоносного программного обеспечения или технических средств, которые являются очень усложнить идентификации, который совершает преступление. Практика применения судами норм уголовного кодекса, которые регулируют общественные отношения в области использования компьютеров, их систем и компьютерных сетей на 1 января 2004 года, имеет, согласно практике рассмотрения судами уголовных.

Чтобы уменьшить рост компьютерной преступности необходимо резко изменить и улучшить информационной безопасности. Защита компьютерной информации требуется в следующих областях:

-подробно действующего уголовного законодательства и улучшения в этом направлении;

-совершенствование деятельности подготовки представителей правоохранительных органов, включая создание специальных подразделений для выполнения этой работы;

-усиленные меры безопасности против возможных злоупотреблений и найти идеальную защиту компьютерных технологий и информационных сетей.

Для его содержания эти мероприятия объединить условно в правовые, организационные и технические меры для защиты компьютерной информации.

Практической деятельности показывает, что положительный результат может быть достигнут только если использовать все эти события и они все одинаково важны и только дополняя друг друга, образуют преднамеренное системы защиты. Остается только отметить, что государство по-прежнему будет отмечаться много внимания преступления «компьютер» и создать новую надежной системы защиты информации.

Список ссылок

1. Бабаш А.В., Шанкин Г.П. История криптографии.Ч.1. - Гелиос АРВ, 2002. – 240с.

2. Бабаш А.В., Шанкин Г.П. Криптогорафия. – Москва: СОЛОН-Р, 2002, 511с.;

3. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.

4. Вехов. Компьютерные преступления, Москва: СОЛОН-Р 2006, c. 14.

5. Гмурман А.И. Информационная безопасность. М.: «БИТ-М», 2004 г.

6. Дъяченко С.И. Правовые аспекты работы в ЛВС. СП-б, «АСТ», 2002 г.