Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра Социальных коммуникаций

Правовое регулирование охраны компьютерной информации: информационно – правовой и уголовно – правовой аспекты.

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

Студента 3 курса 365 группы
направления 40.04.01 «Юриспруденция»
Юридического факультета
Егорова Андрея Николаевича

профессор, д-р юрид. наук,
профессор С.Е. Чаннов

заведующий, д-р социол. наук,
профессор О.Ю. Голуб

Саратов 2017

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена тем, что глобальное развитие компьютерных технологий не только облегчает выполнение своих обязанностей для большого количества профессий, но также приводит к появлению определенного ряда проблем, связанных с охраной и защитой информации, персональных и конфиденциальных данных, коммерческих тайн и т.д., которые должны находиться на должном уровне защиты.

Степень разработанности проблемы. Проблемы правового механизма обеспечения охраны и защиты информации исследовались в трудах Барсукова В.С., Батурина Ю.М., Бачило И.Л., Анина Б.Ю., Бирюкова А.А., Ковалева Н.Н., Копылова В.А., Лапиной М.А., Рассолова И.М., Серго И.Н.

Целью настоящего исследования является изучение и анализ положений, характеризующих понятие *«компьютерная информация»* и правовое регулирование ее охраны, а также выявление недостатков в современном законодательстве в сфере компьютерной информации и разработке рекомендаций по решению таких проблем.

Основными задачами исследования являются: рассмотрение понятия компьютерной информации и ее отличия от других видов информации; исследование законодательства России в сфере охраны компьютерной информации; определение информационно – правовой и уголовно – правовой характеристики преступлений в сфере компьютерной информации; анализ проблем, возникающих в области борьбы с компьютерными преступлениями и предложить пути их решения.

Объектом исследования являются отношения в сфере охраны и защиты компьютерной информации.

Предметом исследования являются законы и законодательные акты, направленные на борьбу с преступлениями, связанными с компьютерной информацией.

Нормативно-правовой основой предпринятого исследования являются: Уголовный кодекс Российской Федерации, ФЗ «Об информации, информационных технологиях и о защите информации», часть четвертая ГК РФ, ФЗ «О персональных данных», ФЗ « О коммерческой тайне», ФЗ «О государственной тайне», ФЗ «Об электронной подписи» и некоторые другие нормативно – правовые акты.

Эмпирическую основу исследования также составили данные опросов общественного мнения, проводимых различными социологическими фондами, посвященных отдельным проблемам охраны и защиты компьютерной информации.

Научная новизна работы состоит в том, что настоящее исследование представляет собой комплексное изучение правового механизма, а также правовых норм, обеспечивающих охрану и защиту компьютерной информации. В работе подробно изучаются правовые средства в области обеспечения защиты информации, а также подробно рассматриваются все его структурные элементы, в том числе и правовые нормы.

Наиболее важными, имеющими как теоретическое, так и практическое значение, представляются следующие выносимые на защиту положения:

1. Компьютерная информация - зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах. Ее отграничение от других видов информации – очень объемна, легко уничтожаема, находится только на машинном носителе, общедоступна, индивидуальна, оригинал и копия – равноценны, создается, изменяется и копируется только с помощью компьютера, легко и быстро передается на огромные расстояния, способна к сжатию и последующему восстановлению, доступна нескольким пользователям одновременно.

2. Защита компьютерной информации – система комплекс мер по охране информации от ее потери и разрушения, а также от несанкционированного доступа к ней.

3. Характеристика и анализ основных законодательных актов по защите компьютерной информации.

4. Методы защиты компьютерной информации, а именно периодическое проведение резервного копирования, регулярная антивирусная проверка ПК, использование блока бесперебойной энергии. А также средства защиты информации – идентификация, аутентификация, авторизация, криптографическая защита, защита электронной подписью, защита паролями.

5. Рекомендации по совершенствованию законодательства в сфере компьютерной информации.

Научная значимость работы предопределена тем, что в ней получила развитие слабо изученная до сегодняшнего времени проблема охраны и защиты компьютерной информации. По итогам проведенного исследования даны понятие компьютерной информации и ряд свойств, отграничивающих ее от других видов информации, рассмотрены механизмы ее охраны и защиты. Как следствие, это влечет укрепление методологической основы научного понимания проблемы охраны и защиты компьютерной информации, конкретизации и развитию терминологического аппарата отечественного законодательства.

Практическая значимость исследования состоит в том, что выводы и предложения, сделанные в рамках данной работы, могут быть использованы в целях совершенствования системы обеспечения охраны и защиты компьютерной информации. Они могут быть также использованы в законотворческом процессе в целях регулирования общественных отношений, возникающих в процессе обеспечения охраны и защиты компьютерной информации.

Структура работы. Работа состоит из введения, основной части работы, изложенной в трех главах «Теоретические основы охраны компьютерной информации», «Ответственность за нарушение законодательства», Разработка рекомендаций по решению проблем в сфере компьютерной информации», заключения и списка использованных источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы исследования, обозначается степень ее разработанности, определяются цели, задачи, объект и предмет, научная новизна, теоретическая и практическая значимость работы. Формулируются основные выводы и положения, выносимые на защиту, приводятся сведения об апробации результатов исследования, его структуре.

Первая глава ««Теоретические основы охраны компьютерной информации» состоит из двух частей: 1. «Понятие компьютерной информации и ее отграничение о других видов информации»; 2. «Понятие защиты компьютерной информации».

В первой части первой главы дается понятие компьютерной информации - зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах. Компьютерная информация обладает определенными особенностями, которые позволяют отграничивать, ее от информации как таковой и иных видов в силу того, что она:

1) как правило, довольно объемна и очень быстро обрабатываема;

2) легко и, как правило, бесследно уничтожаема. Отметим, что при удалении какого-нибудь файла физически он продолжает оставаться на носителе информации, удаляется только его имя из каталога. Физическое же удаление информации происходит при записи на его месте новой информации;

3) может находиться лишь на машинном носителе (флеш - накопителе, лазерном диске, переносном жестком диске и др.), в самом компьютере (оперативной памяти), в их системе (оперативной памяти периферийных устройств) и их сети (буферная память устройств связи);

4) общедоступна, при условии, что гражданин овладел основными навыками общения со средствами визуализации и отсутствуют особые ограничения на доступ. Следует иметь в виду, что компьютерная информация, как никакая другая, может быть выведена из разряда общедоступных путем

обычных, но многократно усиленных вычислительной мощью компьютеров методами аутентичной верификации и шифрования (криптографии), парольной защиты. В этом случае доступ к ней лицам, не знающим пароля, шифра или алгоритма защиты, блокируется фактически намертво;

5) индивидуальна — позволяет без специальных средств и приспособлений в естественном виде наблюдать и анализировать себя. Средством индивидуализации является собственно компьютер, инструмент, не простой в обращении и требующий от человека, работающего с ним, определенных навыков;

6) обладает свойством, которое делает оригинал и копию одинаково ценными. Исходя из специфики компьютерной информации, ее содержание не зависит от типа используемого материального носителя. Так, при копировании информации с флеш – накопителя на жесткий диск, с точки зрения содержания, файлы (оригинал и копия) будут тождественны.

7) создается, изменяется, копируется, применяется только с помощью компьютера; при наличии соответствующих периферийных устройств чтения машинных носителей информации (дисководы, устройства чтения лазерных дисков (CD/DVD-ROM), USB – входы, устройства чтения цифровых видеодисков, стримеры и др.)

8) легко передается по телекоммуникационным каналам связи компьютерных сетей. Возможно передать огромный объем информации практически на любое расстояние;

9) способна к сжатию и последующему восстановлению, то есть уменьшению объема при сохранении содержания. Это способствует не только ее передаче, но и эффективному хранению;

10) доступна нескольким пользователям одновременно. К одному и тому же информационному файлу могут иметь доступ одновременно несколько пользователей.

Во второй части первой главы рассматривается понятие защиты компьютерной информации. Защита информации делится на несколько составляющих:

1. От потери и разрушения.

Утеря конфиденциальных сведений может произойти вследствие: нарушений в работе персональных компьютеров; отключения устройства или сбоев в питании; повреждении информационных носителей; неверных действий юзеров; влияния, которыми обладают компьютерные вирусы; несанкционированных умышленных действий иных лиц.

Если сведения являются особо ценными, в целях безопасности может быть применена защита информации, что предотвратит ее уничтожение. Подойдут следующие меры защиты информации: присвоение файлам свойства read only (то есть, сделать информацию доступной только для чтения); использование специальных программных средств, позволяющих сохранять удаленные файлы, например, Norton Protected Recycle Bin (защищенная корзина) имитирует процесс удаления.

Угрозой для сохранения сведений в компьютере являются сбои в электропитании. Речь идет о резких скачках и падениях сети напряжения, нарушениях системы питания. Защитить свой ПК от потери сведений можно, если использовать бесперебойное питание, установив специальные источники. Благодаря источникам компьютер будет нормально работать, даже если отключится напряжение. Дальнейшее успешное функционирование ПК обеспечат аккумуляторные батареи.

2. От несанкционированного доступа. Несанкционированным доступом называют внесение изменений в информацию, прочтение или уничтожение сведений в случае отсутствия полномочий на данные меры.

Среди основных типовых способов завладения информацией несанкционированными способами выделяют: похищение информационных носителей; - копирование носителей с обходом мер по защите информации; - действия с маскировкой под зарегистрированное лицо; применение маскировки

под системные запросы (процесс носит название мистификации); - действия с использованием недочетов языков в программировании и недостатков в операционных системах; - выполнение перехвата электронного излучения; - выполнение перехвата акустического излучения; - фотографирование на дистанции; - манипуляции с подслушивающими устройствами; намеренный вывод защитных механизмов из строя.

Во второй главе «Ответственность за нарушение законодательства» раскрываются законодательные основы, регулирующие охрану компьютерной информации, рассматриваются гарантии обеспечения компьютерной информации, приводятся примеры нарушений в сфере компьютерной информации. Глава состоит из двух частей: 1. «Правовое регулирование охраны компьютерной информации: характеристика и анализ основных документов и Федерального Закона «О персональных данных»»; 2. «Российская практика нарушений законодательства: информационно-правовой и уголовно-правовой аспекты»

В первой части второй главы приводится характеристика основных законодательных актов по охране компьютерной информации. Уголовная ответственность за преступления в сфере компьютерной информации предусмотрена главой 28 УК РФ, содержащей три статьи.

Так, статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Статья 273 УК РФ предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

В соответствии со ст. 274 УК РФ уголовная ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Мошенничество в сфере компьютерной информации. Статья 159.6 УК РФ устанавливает ответственность за "хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

Во второй части второй главы проводится анализ российской практики нарушений законодательства, приводятся примеры различных правонарушений. Опасность преступлений в сфере компьютерной информации состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем производственного, оборонного, банковского, экономического и иного назначения, могут повлечь гибель людей, нанести вред их здоровью, причинить экономический вред в больших размерах, уничтожить имущество. Принимая во внимание данные обстоятельства, законодатель отнес гл. 28 "Преступления в сфере компьютерной информации" к разд. IX Уголовного кодекса Российской Федерации "Преступления против общественной безопасности и общественного порядка". Усовершенствование безопасности работы информационных и телекоммуникационных систем, критически важных объектов инфраструктуры и объектов повышенной опасности в РФ, повышение уровня защищенности корпоративных и индивидуальных информационных систем являются важными составными частями национальной безопасности страны.

В третьей главе «Разработка рекомендаций по решению проблем в сфере компьютерной информации» приводятся методы и средства защиты

компьютерной информации, а также приводятся рекомендации по решению проблем в сфере компьютерной информации. Глава состоит из одной части.

Необходимо решение проблем по совершенствованию нормативно-правовой базы, недостаточная развитость которой, с точки зрения права, пока не позволяет в полной мере противостоять криминальным действиям в области компьютерной информации.

Существуют определенные недостатки в Уголовном кодексе Российской Федерации: все компьютерные преступления охватываются тремя составами, существенно не дополнявшиеся с момента его принятия. Притом признаки преступлений, которые предусмотрены в статьях 272 и 274 УК РФ, весьма похожи с технической точки зрения.

В заключении работы подводятся итоги проведенного исследования, формулируются основные выводы, положения, а также практические предложения по совершенствованию государственно-правового механизма обеспечения охраны и защиты компьютерной информации, вытекающие из результатов работы.

Работу завершает библиографический список использованной литературы и нормативно-правовых актов, включающий 38 наименований.

ЗАКЛЮЧЕНИЕ

Прогресс дал человечеству множество достижений, однако он же породил и массу проблем. Человеческий разум, решая одни проблемы, обязательно сталкивается при этом с другими, новыми. Вечная проблема - защита информации. На разных этапах развития человечество решало эту проблему с присущей данному периоду характерностью. Изобретение компьютера, а также последующее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. Основная тенденция, которая характеризует развитие современных информационных технологий – это рост количества компьютерных преступлений и связанных с ними хищений конфиденциальной и другой информации и материальных потерь.

В настоящее время, возможно, ни один человек не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это можно объяснить, в первую очередь, отсутствием желания у пострадавших компаний оглашать информацию о своих потерях, а кроме того тем, что не всегда потери от хищения информации возможно оценить точно в денежном эквиваленте.

Причин активизации компьютерных преступлений и, как следствие, связанных с ними финансовых потерь достаточно много. Из них существенными являются:

- переход от классической "бумажной" технологии хранения и передачи данных в электронную, а также недостаточное при этом развитие технологии защиты информации в таких технологиях;

- объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

- увеличение сложности программных средств и, как следствие, связанное с этим уменьшение их надежности и увеличением числа уязвимостей.

Компьютерные сети, в силу своей специфики, попросту не могут нормально функционировать и развиваться, пренебрегая при этом проблемами защиты информации.

В первой главе моей работы были рассмотрены теоретические основы охраны компьютерной информации, было дано понятие компьютерной информации и что ее отличает от других видов информации. Так же было описано понятие охраны и защиты компьютерной информации. Защиту информации следует рассматривать как систему мер по созданию, обеспечению или способствованию обеспечению создания оптимальных условий прохождения всех информационных процессов (хранения, обработки, распространения), связанных с этой информацией.

Во второй главе было подробно рассмотрено правовое регулирование охраны компьютерной информации, а именно дана характеристика и проведен анализ основных правовых документов по охране компьютерной информации. Так же подробно рассмотрен Федеральный Закон «О персональных данных». Так же одним из основных документов в этой области является ст.159.6 «Мошенничество в сфере компьютерной информации». Мной был проведен анализ российской практики нарушений законодательства в сфере компьютерной информации, даны примеры данных нарушений, в том числе и по г. Саратову.

Проанализировав рассматриваемые правовые документы, регулирующие охрану компьютерной информации, в третьей главе моей работы были выявлены следующие проблемы в сфере компьютерной информации:

- все компьютерные преступления охватываются тремя составами, которые существенно не дополнялись с момента его принятия. При этом признаки преступлений, предусмотренных в статьях 272 и 274 УК РФ, с технической точки зрения весьма похожи. Различие заключается в правомерности или неправомерности доступа к ЭВМ, системе ЭВМ или их сети.

- в связи с повсеместным распространением сети Интернет, требуется принять упреждающие меры уголовно-правового характера, заключающиеся в издании норм, пресекающих компьютерные посягательства с учетом ее специфики;

- существуют проблемы при сборе доказательств и первичной проверочной информации при проведении первоначальных оперативно-розыскных мероприятий;

- необходимо внести изменения в п. 1 ч. 5 ст. 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ. К основаниям для внесения в Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено, необходимо добавить сайты и интернет ресурсы, где предоставлены вредоносные компьютерные программы и программные средства, предназначенные для нарушения систем защиты информации, информационно-телекоммуникационных устройств, их систем и сетей.

- необходима разработка, стандартизация и унификация законодательства и программных средств, позволяющих определять местонахождение и установление личности преступников, противоправно использующих компьютерные сети и глобальные телекоммуникационные системы;

- необходимо акцентировать внимание и на решении проблемы унификации законодательства стран, участвующих в информационном обмене. Без единых требований к доказательствам ни один суд, ни одной страны не признает доказательством данные, если они будут собраны в другой стране по законам, противоречащим законам запрашивающей страны.

Таким образом, устранение изъянов и недоработок в законодательстве Российской Федерации – процесс трудоемкий и сложный, но крайне необходимый для борьбы с преступлениями в сфере компьютерной информации.