Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.
ЧЕРНЫШЕВСКОГО»

Кафедра уголовного,
экологического права
и криминологии

Защита персональных данных в Российской Федерации: теоретико-правовой анализ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 431 группы
направления подготовки 40.03.01 – «Юриспруденция»
юридического факультета

Савина Александра Сергеевича

Научный руководитель
профессор кафедры _____ В.Г. Громов
уголовного, экологического
права и криминологии
д. ю. н., профессор

Зав.кафедрой
профессор, д. ю. н., профессор _____ Н.Т. Разгельдеев

Саратов 2018

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Сведения о гражданах собираются и аккумулируются различными государственными структурами (органы внутренних дел, бюро технической инвентаризации, органы актов гражданского состояния, медицинские учреждения, органы регистрации прав на недвижимое имущество и сделок с ним, органы регистрации юридических лиц и др.) и частными корпорациями (сотовые компании, частные образовательные, медицинские, юридические организации и т.д.) при рождении и получении документов, удостоверяющих личность, при поступлении на работу, при обращении в медицинские учреждения, при покупке недвижимого имущества (квартир, машин), при создании частных предприятий, в иных случаях. Совершая покупки в интернет- магазинах, потребитель вынужден сообщать свои персональные данные. В связи с этим встает вопрос о необходимости защиты персональных данных.

Тема дипломной работы является актуальной на сегодняшний день. Основная проблема обусловлена развитием автоматизированных средств обработки информации, с которым также растет вероятность возникновения утечки различных данных, в том числе и содержащих информацию персонифицированного характера. Содержание бакалаврской работы отражает этапы становления законодательства в области защиты персональных данных. Рассматриваются способы защиты информации с использованием обще социальных и обще специальных методов.

Объектом исследования в работе являются общественные отношения, возникающие по поводу нарушения законодательства в области защиты персональных данных в российском праве.

Предметом исследования выступают нормативно-правовые и иные руководящие документы в области защиты персональных данных.

Целью бакалаврской работы изучение становления правового института персональных данных в России, а также способы и формы реализации методов защиты данных.

Для достижения указанной цели поставлены следующие **задачи**:

1. Изучить тезис и тип персональных данных;
1. Становление законодательства в области персональных данных в России;
2. Изучения мер ответственности за нарушения законодательства в области защиты персональных данных в административном и уголовном праве.
3. Рассмотрение обще социальных и обще специальных методов защиты персональных данных.
4. Рассмотрение конкретного административного дела о преступлении, совершенном в области информационного права.

Методологическая основа исследования построена на таких методах как диалектический, сравнительно-правовой и аналитический методы.

Теоретическую основу исследования составили труды таких ученых как: Е.О. Алексеева, С.А. Борисова, Д.М. Ветров, А.С. Долгов и других авторов.

Нормативной базой исследования является: Конституция РФ, Федеральный закон в области персональных данных, действующее административное законодательство Российской Федерации, нормативно-правовые акты в области Защиты информации и международно-правовые акты.

Структура работы соответствует поставленным целям и задачам и состоит из теоретического и практического разделов. Теоретический раздел включает в себя 3 главы, заключения и списка используемой литературы. Практическая часть содержит макет уголовного дела о преступлении.

СОДЕРЖАНИЕ РАБОТЫ

Работа состоит из 2 частей: теоретической и практической.

В теоретической части глава 1 «Персональные данные: понятие и правовое регулирование» состоит из параграфов «Понятие и виды персональных данных» и «Становление законодательства о защите персональных данных в России».

Вторая глава «Ответственность за нарушение законодательства о защите персональных данных» включает в себя параграфы «Административная ответственность» и «Уголовная ответственность».

В третью главу «Основные направления совершенствования защиты персональных данных в РФ» включены параграфы «Общесоциальные меры защиты персональных данных» и «Специальные меры защиты персональных данных».

Практическая часть представляет собой макет уголовного дела по ч.1 ст.137, ч.1 ст.138 Уголовного кодекса Российской Федерации.

Российский законодатель закрепил достаточно ясное определение персональных данных, главным смысл которого является понятие "определение" (или "идентификация"). Именно ключевое свойство как идентификации (определения) позволяет выделить из общего количества сведений о субъекте, только те данные, с помощью которых данного субъекта можно определить. Телефонные разговоры, опросы и социальные мероприятия, которые охватывают понятие «личная жизнь», не позволяют установить личность субъекта, а значит, не могу быть отнесены к персональным данным.

Информация, при использовании которой, возможно определение (идентификация) субъекта, является персональными данными:

- фамилия, имя, отчество,
- год, месяц, дата и место рождения,

- адрес, семейное, социальное и имущественное положение,
- образование, профессия, доходы и
- другая информация.

К "другой» информации может относиться страница в сети интернет (фотография, сведения о детях, супруги и т.п.). Перечень данных относящихся к персональным данным утвержден Указом Президента.

Субъектом персональных данных может являться только физическое лицо. Сведения о юридическом лице, не являются персональными данными, так как согласно ст. 3 ФЗ №152: «В целях настоящего Федерального закона используются следующие основные понятия»: «персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу»[1].

Федеральный закон «О персональных данных» подразделяет персональные данные на следующее категории:

- **общедоступные персональные данные** — персональные данные, доступ к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- **специальные категории персональных данных** — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Обработка таких данных возможна только в случаях, прямо указанных в законе, в частности:

- если субъект персональных данных в письменной форме дал свое согласие;
- если обработка персональных данных необходима в связи с осуществлением правосудия;

---

1 О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. 29.07.2017) / Справочно-правовая система «Консультант-Плюс» (дата обращения 08.12.2017).

• если обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

биометрические персональные данные — сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. К таким персональным данным относится, в частности, дактилоскопическая информация, порядок сбора, хранения и использования которой регулируется Федеральным законом от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»[2].

Дела об административных правонарушениях, предусмотренных законами субъектов РФ, рассматриваются в пределах полномочий, установленных этими законами: мировыми судьями; комиссиями по делам несовершеннолетних и защите их прав; уполномоченными органами и учреждениями органов исполнительной власти субъектов РФ; административными комиссиями, иными коллегиальными органами, создаваемыми в соответствии с законами субъектов РФ.

Общественные отношения, связанные с защитой персональных данных, относятся преимущественно к сфере государственного управления, что обусловливает потенциально большое число составов административных правонарушений в этой сфере в будущем. В настоящее время гл.13 "Правонарушения в области связи и информации" Особенной части КоАП РФ содержит несколько составов административных правонарушений, объектом которых являются отношения, связанные с оборотом и защитой персональных данных граждан[3].

---

2 О государственной дактилоскопической регистрации в Российской Федерации: Федеральный закон от 25.07.1998 № 128-ФЗ (ред. 05.12.2017) /Справочно-правовая система «Консультант-Плюс» (дата обращения 08.12.2017).

3 Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 г. № 195-ФЗ (ред. от 31.12.2017) / Справочно-правовая система «Консультант-Плюс» (дата обращения 08.12.2017).

Уголовно-правовые санкции, связанные с информацией прямо или опосредованно, установлены в отношении таких деяний, как нарушение неприкосновенности частной жизни (ст. 137 УК РФ). Сбор, хранение, а также использование, распространение информации о частной жизни лица без согласия лица не допускаются. Данный запрет является одной из гарантий лица на частную жизнь. В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит не противоправный характер.

К сведениям, составляющим личную или семейную тайну, относятся не подлежащие оглашению данные, по мнению лица, которого эти сведения касаются. В то же время не могут составлять тайну сведения, ранее уже опубликованные тем или иным способом. Создание специальной штатной службы или штатной единицы, ответственной за информационную безопасность, является одним из этапов построения эффективного функционирования защиты информации в автоматизированных системах организации.

Основные функции службы заключаются в следующем:

- формирование требований к системе защиты в процессе создания автоматизированных систем;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования автоматизированных систем;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;

- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках несанкционированного доступа к информации и при нарушениях правил функционирования системы защиты.

Эффективное функционирование комплекса мер по защите компьютерной информации должно быть строго регламентировано. Для этих целей необходимо создание организационно-распорядительных документов. Данные документы должны содержать:

- Порядок и правила обработки информации в автоматизированных системах
- Порядок обеспечения бесперебойного функционирования информационных систем
- Правила восстановления информации в случаях сбоя
- Порядок действия информационного обмена
- Ответственность лиц, осуществляющих обработку, хранение и передачу персональных данных
- План защиты информационных систем персональных данных.

Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения, в руках инсайдера – в товар для продажи конкуренту. Именно поэтому персональные данные нуждаются в самой серьезной защите.

В соответствии со статьей 19 Федерального Закона «О персональных данных» оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Согласно постановлению № 781 от 17 ноября 2007 г. оператор персональных данных, должен назначить должностное лицо и (или) работника, ответственного за обеспечение безопасности персональных данных. Защита Персональных данных при осуществлении пользователями информационных систем голосового ввода данных в ИСПДн или их воспроизведении акустическими средствами ИСПДн обеспечивается путем звукоизоляции помещений, в которых устанавливаются аппаратные средства ИСПДн, систем инженерного обеспечения (вентиляции, отопления и кондиционирования), а также ограждающих конструкций помещений (стены, пол, потолок, окна, двери).

Звукоизоляция обеспечивается с помощью архитектурных и инженерных решений, применением специальных звукопоглощающих строительных и отделочных материалов, виброизолирующих опор, которыми разделяют друг от друга различные ограждающие конструкции. Исключение посторонних предметов на внешней стороне конструкций помещений и выходящих коммуникаций позволит снизить вероятность перехвата.
Применение активных мер защиты (создание систем, способных маскировать акустические и вибрационные типы помех) применимо при отсутствие технической возможности.

Защита персональных данных от несанкционированного доступа, включают в себя мероприятия по анализу защищенности, целостности, а также регистрации и учета. Для полноценной защиты в данные мероприятия включают, подсистемы защиты, такие ка антивирусная защита, межсетевое экранирование и обнаружение вторжений.

К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики (тестирование файловой системы), регистрации (журналирование действий и операций), сигнализации (предупреждение об обнаружении фактов несанкционированных действий или нарушения штатного режима функционирования ИСПДн).

Подсистема обеспечения целостности также реализуется преимущественно средствами самих операционных систем и СУБД. Работа данных средств основана на расчете контрольных сумм, уведомлении о сбое в передаче пакетов сообщений, повторе передачи непринятых пакетов.

Для обеспечения безопасности Персональных данных и программно-аппаратной среды ИСПДн, обеспечивающей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты (подсистема антивирусной защиты). К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации (происходящие, например, в ходе модернизации ИСПДн), предусмотренных указанными правилами, согласовывается с ФСТЭК и ФСБ.

Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации.

Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

В практической части приводится макет уголовного дела по ст. 137 УК РФ.

В заключении говорится о том, что персональные данные это очень важные документы потому, что они представляют собой любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, другую информацию. Персональные данные должны быть, очень хорошо защищены. Несмотря на осознанное понимание поднятой проблемы как законодательными, так и государственными и коммерческими организациями, персональные данные все же подвержены утечкам информации, ущерб от которых подчас оценивается весьма впечатляющими цифрами.

Многократно возрастающий объем информации ограниченного доступа, в том числе и персональных данных, требуют особой ответственности при решении вопросов регулирование соответствующих правоотношений. Увеличение штрафных санкций при совершении административных правонарушений, должно подтолкнуть недобросовестных операторов персональных данных к соблюдению законодательства.