МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

К Г Э У

Кафедра «Экономика и организация производства»

Отчет по Контрольной работе
по дисциплине «Информационная безопасность»

Персональные данные

Выполнила: студент 3 курса Дементьева Е.В.
Преподаватель: доц. Исмагилов И.Р.

КАЗАНЬ 2023

Цель работы: изучение видов информации, для которых соблюдение конфиденциальности является обязательным согласно законодательным требованиям РФ в области информационной безопасности, а также ознакомление с ответственностью за их разглашение.

В данном отчете рассматривается такой вид информации с ограниченным доступом, как персональные данные.

Перечень законодательных, нормативных правовых актов, регулирующих взаимоотношения в обществе, связанных с персональными данными, представлен в таблице:

№ п/п	Вид нормативного правового акта	Наименование нормативного правового акта	Статься, пункт, в котором упоминается вид информации с ограниченным доступом
1	Федеральный закон	Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"	ст. 1 ст. 5-16 ст. 18, 20-22.1 ст. 25
2	Федеральный закон	Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ	Гл.14 ст. 86-89
3	Федеральный закон	Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации"	ст. 24, 26 ст. 42-44 ст. 64
4	Указы Президента Российской Федерации	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации	П. 4-15
5	Указы Президента Российской Федерации	Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных	П. 1-2

		Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами	
6	Нормативные правовые акты и нормативные документы федеральных органов исполнительной власти	Требования и методы по обезличиванию персональных данных	П. 1-15

Термины и определения, касающиеся персональных данных, представлены в таблице:

Термин	Определение
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
Блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных)
Информационная система персональных данных	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Обезличивание персональных данных	действия, в результате которых

	невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных
Обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Персональные данные	— любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных

	данных)
Предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом
Уничтожение персональных данных	действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

К персональным данным могут относиться следующие сведения:

- фамилия, имя, отчество;
- место, дата рождения;
- место постоянной или временной регистрации;
- фотография или видеозапись человека, позволяющие идентифицировать человека;

- сведения о детях, родственниках, семейном положении;
- сведения о заработной плате;
- оценка навыков, личностных качеств;
- индивидуальные личные данные (раса, национальность, политические или религиозные взгляды, философские убеждения; состояние здоровья);
- информация о судимостях, или их отсутствии;
- номер телефона, адрес электронной почты, иные идентификаторы в соц. сетях или мессенджерах;
- паспортные данные, СНИЛС, ИНН;
- биометрические данные.

К персональным данным НЕ могут относиться следующие сведения:

- личные сведения родственников
- сведения об автомобиле
- переписки

Описание порядка предоставления доступа оформление допуск к персональным данным представлено ниже:

Субъект персональных данных имеет право:

− получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные законодательством о персональных данных;

− требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении субъектом персональных данных согласия на обработку персональных данных;

− принимать предусмотренные законом меры по защите своих прав;

− отозвать свое согласие на обработку персональных данных;

− иные права, предусмотренные законодательством о персональных данных.

Оператор имеет право:

− обрабатывать персональные данные субъекта персональных данных в соответствии с заявленной целью;

− требовать от субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, идентификации субъекта персональных данных, а также в иных случаях, предусмотренных законодательством о персональных данных;

− ограничить доступ субъекта персональных данных к его персональным данным в случае, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц, а также в иных случаях, предусмотренных законодательством Российской Федерации;

− обрабатывать общедоступные персональные данные физических лиц;

− осуществлять обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации;

− поручить обработку персональных данных другому лицу с согласия субъекта персональных данных;

− иные права, предусмотренные законодательством о персональных данных.

За правонарушения, ввязанные с разглашением сведений, относящихся к персональным данным предусмотрены виды юридической ответственности, представлены в таблице:

Вид юридической ответственности	Правонарушение/преступление	Основание (ссылка на статью, пункт НПА)
Административная	Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой	Статья 5.39 КоАП РФ

	предусмотрено законом, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации	
	Обработка персональных данных в случаях, не предусмотренных законом, либо обработка, несовместимая с целями сбора персональных данных	Часть 1 ст. 13.11 КоАП РФ
	Обработка персональных данных без письменного согласия субъекта, когда это необходимо, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	Часть 2 ст. 13.11 КоАП РФ
	Невыполнение оператором обязанности по опубликованию или обеспечению иным образом неограниченного доступа к политике обработки персональных данных	Часть 3 ст. 13.11 КоАП РФ

	Невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Часть 4 ст. 13.11 КоАП РФ
	Невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки)	Часть 5 ст. 13.11 КоАП РФ
	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении них	Часть 6 ст. 13.11 КоАП РФ
	Невыполнение оператором, являющимся государственным или	Часть 7 ст. 13.11 КоАП РФ

	муниципальным органом, обязанности по обезличиванию персональных данных либо несоблюдение установленных для этого требований или методов	
	Непредставление или несвоевременное представление в государственный или иной уполномоченный орган сведений, представление которых предусмотрено законом либо предоставление таких сведений в неполном объеме или в искаженном виде	Статья 19.7 КоАП РФ
Уголовная	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ	Статья 137 Уголовного кодекса
	То же деяние, совершенное с	

	использованием служебного положения	
	Незаконное публичное распространение информации, указывающей на личность лица, не достигшего 16 лет, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий	
	Неправомерный отказ должностного лица в предоставлении документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление ему неполной или заведомо ложной информации, если это причинило вред правам и законным интересам граждан	Статья 140 УК РФ
	Неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование	Статья 272 УК РФ
Гражданско-правовая	Причинение лицу убытков в результате нарушения правил обработки его персональных данных. Под убытками при этом понимаются: • расходы, которые лицо произвело или должно будет произвести для восстановления нарушенного права; • утрата или повреждение его	Статья 15 Гражданского кодекса

	имущества; • неполученные доходы, которые лицо получило бы, не будь его право нарушено.	
	Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных	Статья 24 закона о персональных данных, ст. 151 ГК РФ
Дисциплинарная	Разглашение одним работником персональных данных другого, если они стали известны ему в связи с исполнением трудовых обязанностей	Подпункт "в" п. 6 ч. 1 ст. 81 Трудового кодекса
	Иные нарушения в области персональных данных при их обработке	Статья 90, ст. 192 ТК РФ

Пример из судебной практики, относящийся к делу, связанному нарушением норм, регулирующих взаимоотношения в обществе, связанных с персональными данными представлен:

Вид юридической ответственности	Решение суда	Основание	Краткое описание правонарушения/преступления	Ссылка на источник
Административная	Взыскать с ООО «Свобода от долгов» в пользу Разина Евгения Сергеевича компенсацию морального вреда в размере 3 000 (три тысячи) рублей, почтовые расходы в размере 123	Защита и распространение персональных данных	Ответчик незаконно обрабатывал персональные данные истица, чем, безусловно, причинил последнему моральный вред, поскольку затронул его личные неимущественные права.	https://sudact.ru/regular/doc/6FzFUMECKnoO/

	рубля, расходы по уплате государственной пошлины в размере 300 рублей, а всего 3 423 (три тысячи четыреста двадцать три) рубля.			

Примеры известных случаев несанкционированных воздействий на персональные данные представлены в таблице:

№ п/п	Краткое описание инцидента	Негативные последствия	Возможные причины инцидента
1	На данный момент эта утечка считается крупнейшей в российском банковском секторе. База, содержащая информацию о десятках миллионов держателей кредитных карт, оказалась в продаже в сети «Интернет». Ориентировочно утечка произошла во второй половине августа 2019 г., а в продажу база поступила в конце сентября того же года.	Содержание базы включает уникальные идентификаторы держателей карт, такие как паспортные данные и Ф. И. О., а также сведения о лимитах карт и операциях по ним.	Основная версия инцидента – умышленные преступные действия одного из сотрудников, так как внешнее проникновение в базу данных невозможно в силу ее изолированности от внешней сети.
2	"Матерь всех утечек": в открытом доступе оказались 560 миллионов адресов электронной почты и паролей О находке в мае 2017 года сообщил Центр изучения безопасности MacKeeper.	1. Персональные данные 198 миллионов избирателей США хранились на "облаке" Amazon в открытом доступе 2. В Индии из государственно	Среди причин — старый "человеческий фактор" и новые инсайдерские трюки, непреходящая угроза уязвимости.

	Упорядоченную и удобную для чтения базу весом 75 гигабайт назвали "матерью всех утечек" из-за данных, которые уже были скомпрометированы ранее. Эксперты установили, что речь идет как минимум о десяти известных утечках данных пользователей MySpace, LinkedIn, Last.fm, Dropbox, Tumblr и других популярных ресурсов.	й системы биометрической идентификации Aadhaar "утекли" уникальные ID-номера 135 миллионов граждан 3. Данные медстраховок всех жителей Австралии выставили на продажу 4. Базу с данными "почти каждого" жителя Малайзии предложили за один биткоин	
3	В начале декабря 2020 года случилась утечка личных данных примерно 100 тыс. жителей Москвы, переболевших коронавирусом.	Размер «слитого» архива — примерно 1 ГБ, он содержит 362 файла различных форматов. В файлах записано более 100 тыс. строк, которые включают в себя Ф. И. О., номера полисов ОМС, контактные телефоны и другие сведения. Первоначальный анализ утечки позволил понять, что в архиве присутствуют личные данные заболевших в период с апреля по июль этого года.	Слабая защита базы данных с персональной информацией личности

Основные организационные и технические меры, направленные на обеспечение безопасности, учитывающие специфику обработки персональных данных представлены ниже:

− назначение ответственного за организацию обработки персональных данных;

− назначение ответственных за обеспечение мер по сохранности персональных данных и исключению несанкционированный к ним доступа;

− назначение ответственного за обеспечение безопасности персональных данных в информационных системах;

− ограничение состава лиц, допущенных к обработке персональных данных;

− ознакомление субъектов с требованиями федерального законодательства и нормативных документов Оператора по обработке и защите персональных данных;

− организация учета, хранения и обращения носителей, содержащих информацию с персональными данными;

− определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;

− разработка на основе модели угроз системы защиты персональных данных;

− проверка готовности и эффективности использования средств защиты информации;

− разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации;

− регистрация и учет действий пользователей информационных систем персональных данных;

− использование антивирусных средств и средств восстановления системы защиты персональных данных;

− применение в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации;

− организация пропускного режима на территорию Оператора, охраны помещений с техническими средствами обработки персональных данных.

Выводы: согласно предоставленным сведеньям за разные года количество инцидентов информационной безопасности, связанных с несанкционированным воздействием на персональные данные в период с 2017 по 2023 годы возрастает, несмотря на принимаемые меры безопасности, из-за проблем в адаптации законодательства современным вызовам в информационном пространстве. Причинами данных инцидентов являются ненадежная защита баз данных и появление новых обходов шифрования и защиты. Несанкционированные воздействия на персональные данные могут повлечь за собой административное или уголовное наказание.

Считаю, что создание новой шифровальной системы может снизить количество правонарушений, связанных с защитой персональной информацией, так как хакерам нужно будет время на освоение новой защиты.

Библиографические ссылки:

1. https://sudact.ru/regular/doc/6FzFUMECKnoO/
2. https://www.anti-malware.ru/analytics/Threats_Analysis/Top-10-data-leakage-in-Russia#part22
3. https://ria.ru/20171228/1511885539.html
4. https://www.anti-malware.ru/analytics/Threats_Analysis/Top-10-data-leakage-in-Russia#part210
5. https://www.forbes.ru/tekhnologii/487747-cislo-utecek-personal-nyh-dannyh-v-2022-godu-vyroslo-v-2-7-raza