

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

**ПРАВОВЫЕ ОТНОШЕНИЯ
ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ
ПОДПИСИ И ОБРАБОТКЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Методические указания

ПЕНЗА 2018

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Пензенский государственный университет» (ПГУ)

Правовые отношения при использовании электронной подписи и обработке персональных данных

Методические указания

С о с т а в и т е л и :

М. А. Катыхева, Ю. Г. Кирюхин, Г. В. Кошелева,
Н. Н. Надеева, Ю. Ю. Фионова, Н. Н. Шокорова

Пенза
Издательство ПГУ
2018

УДК 349.2
П68

Р е ц е н з е н т
кандидат технических наук, доцент кафедры
«Прикладная информатика»
Пензенского государственного технологического университета
Ю. Е. Усачев

П68 **Правовые отношения при использовании электронной подписи и обработке персональных данных** : метод. указания / сост.: М. А. Катышева, Ю. Г. Кирюхин, Г. В. Кошелева, Н. Н. Надеева, Ю. Ю. Фионова, Н. Н. Шокорова. – Пенза : Изд-во ПГУ, 2018. – 20 с.

Издание нацелено на освоение компетенций бакалавра в сфере организации и технологии документационного обеспечения управления.

Подготовлено на кафедре «Информационное обеспечение управления и производства» ПГУ и предназначено для бакалавров направлений подготовки 01.03.01 «Математика»; 01.03.02 «Прикладная математика и информатика»; 01.03.04 «Математическое моделирование в экономике и технике»; 02.03.03 «Математическое обеспечение и администрирование информационных систем»; 09.03.01 «Информатика и вычислительная техника»; 09.03.02 «Информационные системы и технологии»; 09.03.03 «Прикладная информатика»; 09.03.04 «Программная инженерия»; 46.03.02 «Документоведение и архивоведение».

УДК 349.2

© Пензенский государственный
университет, 2018

Содержание

Практическая работа № 4. Правовые отношения при использовании электронной подписи и обработке персональных данных	4
Библиографический список.....	19

Практическая работа № 4

Правовые отношения

при использовании электронной подписи и обработке персональных данных

Цель работы: закрепить полученный на лекционных занятиях необходимый минимум теоретических знаний в области освоения основных понятий «электронная подпись», «персональные данные»; получить практические навыки, необходимые для поиска правовой информации с помощью правового навигатора, путеводителей СПС «Консультант-Плюс» и использования справочной информации; освоить элементарную деятельностьную компетенцию «Способность получать информацию с помощью СПС «КонсультантПлюс».

Общие сведения

Начнем с изучения паспорта этой элементарной деятельностьной компетенции (ЭДК) (таблица 1). Она является элементарной по отношению к компетенции ОК-04: «Способность использовать основы правовых знаний в различных сферах деятельности».

Таблица 1 – Паспорт осваиваемой ЭДК

Содержание ЭДК	Способен использовать основной инструмент получения правовой информации
Виды деятельности, в рамках которых данная ЭДК востребована	Организационно-управленческая и научно-исследовательская
Задачи, для решения которых владение данной ЭДК необходимо	Задача 1 (связана с организационно-управленческой деятельностью): поиск правовой информации с использованием СПС «КонсультантПлюс». Задача 2 (связана с научно-исследовательской деятельностью): составление рекомендаций по выбору основных источников получения правовой информации
ЗК, на базе которых формируется данная ЭДК	ОК-4 – способность использовать основы правовых знаний в различных сферах деятельности
НК, которые являются необходимыми для овладения данной ЭДК	ОК-4 – способность использовать основы правовых знаний в различных сферах деятельности

Продолжение таблицы 1

Содержание ЭДК	Способен использовать основной инструмент получения правовой информации
Нормативные акты, необходимые для овладения (освоения) данной ЭДК	<ul style="list-style-type: none"> – Конституция Российской Федерации от 12.12.1993; – Гражданский кодекс РФ (ч. 1) от 30.11.1994; – Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006; – Федеральный Закон РФ «Об электронной подписи» № 63-ФЗ от 06.04.2011; – Федеральный закон РФ «О персональных данных» № 152-ФЗ от 27.07.2006; – Федеральный закон «Об обязательном экземпляре документов» № 77-ФЗ от 29.12.1994 (ред. от 05.05.2014); – ГОСТ Р 34.10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметрического криптографического алгоритма»; – ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации, функция хэширования»
Название предмета (дисциплины), для которого эта ЭДК является исходной компетенцией	«Архивное право», «Документационное обеспечение службы маркетинга»
Название предмета (дисциплины), для которого эта ЭДК является целевой компетенцией	Правое обеспечение в профессиональной деятельности
Критерии эффективности	<p>Определен набор основных инструментов ИПС «КонсультантПлюс» для поиска правовой информации.</p> <p>Набор основных инструментов ИПС «КонсультантПлюс» обоснован в зависимости от нормативного документа.</p> <p>Составлен список нормативных законодательных актов, регламентирующих правовое обеспечение в профессиональной деятельности</p>

Электронная подпись

Электронная подпись (ЭП) – это не предмет, который можно взять в руки, а реквизит документа, позволяющий подтвердить принадлежность ЭП ее владельцу, а также зафиксировать состояние информации/данных (наличие либо отсутствие изменений) в электронном документе с момента его подписания.

Значение реквизита получается в результате криптографического преобразования информации.

Использование электронных подписей регулируется Федеральным законом «Об электронной подписи» № 63-ФЗ от 06.04.2011, а также другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия.

Федеральный закон «Об электронной подписи» дает следующие понятия:

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Порядок использования электронной подписи в корпоративной информационной системе устанавливается оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

Основными принципами использования электронной подписи являются:

- право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

- возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

- недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы

только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Существует **простая электронная подпись** и **усиленная электронная подпись**. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Выбор типа электронной подписи зависит от задач, которые необходимо решать с ее помощью. Так, например, выдвигаются требования к выбору электронной подписи при работе с бухгалтерскими первичными документами: электронный счет-фактура является документом основанием для вычета сумм НДС только в том случае, если он подписан квалифицированной электронной подписью. Для сдачи отчетности в государственные органы потребуется использование усиленной квалифицированной электронной подписи.

Для решения задач межкорпоративного электронного документооборота можно использовать усиленную квалифицированную электронную подпись.

Получить сертификат квалифицированной электронной подписи можно в любом аккредитованном Минкомсвязи РФ Удостоверяющем центре.

Удостоверяющий центр:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с Федеральным законом «Об электронной подписи»;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

– осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.

Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки электронной подписи на основании соглашения между удостоверяющим центром и заявителем.

Сертификат ключа проверки электронной подписи должен содержать следующую информацию:

- уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;
- фамилия, имя и отчество (если имеется) – для физических лиц, наименование и место нахождения – для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;
- уникальный ключ проверки электронной подписи;
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;
- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи.

Область применения электронной подписи представлена в таблице 2.

Таблица 2 – Область применения электронной подписи

	Простая	Неквалифицированная	Квалифицированная
Внутренний и внешний документооборот	*	*	*
Арбитражный суд	*	*	*
Документооборот с физическими лицами	*	*	*
Госуслуги	*		*
Контролирующие органы (ФНС, ФСС, ПФР)			*
Электронные торги			*

Самые распространенные на данный момент.

1. Электронный документооборот. Технология ЭП широко используется в системах электронного документооборота различного назначения:

- внешнего и внутреннего обмена;
- организационно-распорядительного;
- кадрового;
- законотворческого;
- торгово-промышленного и пр.

Это продиктовано главным свойством электронной подписи – она может быть использована в качестве аналога собственноручной подписи и/или печати на бумажном документе.

Во внутреннем документообороте ЭП используется как средство визирования и утверждения электронных документов в рамках внутренних процессов. Например, во время согласования договора директор подписывает его ЭП, что значит, что договор утвержден и может быть передан в исполнение.

При построении межкорпоративного документооборота наличие ЭП является критически важным условием обмена, поскольку является гарантом юридической силы. Только в этом случае электронный документ может быть признан подлинным и использоваться в качестве доказательства в судебных разбирательствах. Подписанный усиленной электронной подписью документ также может длительное время храниться в цифровом архиве, сохраняя при этом свою легитимность.

2. Электронная отчетность для контролирующих органов. Многие компании наверняка уже оценили удобство сдачи отчетности в электронном виде.

Современный подход к сдаче отчетности через интернет состоит в том, что клиент может выбрать любой удобный для себя способ:

- отдельное программное обеспечение;
- продукты семейства 1С;
- портал Федеральной налоговой службы;
- портал Фонда социального страхования.

Основа этой услуги – сертификат электронной подписи, который должен быть выпущен надежным удостоверяющим центром, метод же отправки не имеет решающего значения. Такая подпись нужна для придания документам юридической значимости.

3. Государственные услуги. Каждый гражданин Российской Федерации может получить электронную подпись для получения госуслуг.

С помощью ЭП гражданин может заверять документы и заявления, отправляемые в ведомства в электронном виде, а так же получать подписанные письма и уведомления о том, что обращение принято на рассмотрение от соответствующих органов власти.

Пользователь имеет возможность подписать электронной подписью заявление, отправляемое в орган исполнительной власти (при готовности органа исполнительной власти принимать заявления, подписанные электронной подписью).

При реализации этого механизма используются отечественные стандарты ЭП (ГОСТ Р 34.11–94, ГОСТ Р 34.10–2001) и применяются

сертифицированные в системе сертификации ФСБ России средства криптографической защиты информации, такие как «Aladdin e-Token ГОСТ» и «КриптоПро CSP», что дает основания считать данную подпись усиленной квалифицированной электронной подписью (Источник: портал Госуслуги).

4. Электронные торги. Электронные торги проходят на специальных площадках (сайтах). Электронная подпись необходима поставщикам на государственных и коммерческих площадках.

ЭП поставщиков и заказчиков гарантируют участникам, что они имеют дело с реальными предложениями. Кроме того, заключенные контракты приобретают юридическую силу только при его подписании обеими сторонами.

5. Арбитражный суд. При возникновении каких-либо споров между организациями в качестве доказательства в суде могут использоваться электронные документы.

Согласно Арбитражному процессуальному кодексу РФ, полученные посредством факсимильной, электронной или иной связи, подписанные электронной подписью или другим аналогом собственноручной подписи, относятся к письменным доказательствам.

6. Документооборот с физическими лицами. Надо признать, данная сфера применения ЭП весьма специфична и пока редко используется, тем не менее, возможна. С помощью ЭП заверять различные документы могут физические лица. Благодаря этой возможности удаленные работники на основании договоров оказания услуг, например, могут выставлять акты приемки-сдачи работ в электронном виде.

ГОСТ Р 7.0.8–2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» дает следующее определение. Юридическая сила документа – это «свойство официального документа вызывать правовые последствия».

Юридическую силу электронному документу, равно как и бумажному, придает обязательное наличие определенных реквизитов:

- наименование вида документа (за исключением писем);
- регистрационный номер документа;
- наименование организации – автора документа или имя автора документа;
- дата документа;
- место составления (издания) документа;
- отметка об электронной подписи.

Срок действия сертификата электронной подписи составляет один год, а, например, бухгалтерские документы, необходимо хранить пять лет. Но даже после истечения срока действия сертификата, документ не теряет юридической силы, так как в момент подписания ставится штамп времени.

Штамп времени – это аналог даты на подписываемом документе. Он подтверждает, что сертификат электронной подписи был действителен на момент подписания документа.

Так, в момент подписания документа проставляется штамп времени и результат проверки сертификата.

Подтвердить тот факт, что на момент подписания сертификат был действующим, можно также обратившись к списку отозванных сертификатов на сайте удостоверяющего центра.

Непосредственно хранение электронных документов можно организовать двумя способами:

- локальное хранение (документы хранятся на локальных серверах компании, например, в системе электронного документооборота (СЭД));
- хранение в облаке (документы хранятся на серверах компании, услугами которой вы воспользовались).

Персональные данные

Необходимость обеспечения безопасности персональных данных в наше время – объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим несколько примеров из повседневной жизни, когда нарушаются права человека на конфиденциальность персональных данных.

Бывает так, что при оформлении дисконтной карты в магазине покупатель указывает следующие сведения: фамилию, номер телефона, электронный адрес, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал, т.е. магазин без согласия покупателя передал его данные третьим лицам.

Если газета печатает ФИО и суммы выигрыша победителей лотереи без их ведома, или ТСЖ вывешивает на подъезде списки должников и сумму их долга. Это примеры «безобидных» утечек.

Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке.

Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг).

На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту.

Законодательство Российской Федерации в области защиты персональных данных основывается на Конституции РФ, международных договорах Российской Федерации, Федеральном законе РФ № 152-ФЗ от 27.07.2006 «О персональных данных», Федеральном законе № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» и других определяющих случаи и особенности обработки персональных данных федеральных законах.

В соответствии с ФЗ «О персональных данных» персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

К персональным данным в связи с этим могут относиться:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- семейное, социальное, имущественное положение;
- образование;
- профессия;
- доходы;
- другая информация.

Операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включающие:

- сбор;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- использование;
- распространение (в том числе передачу);
- обезличивание;
- блокирование;
- уничтожение персональных данных.

Информационная система персональных данных (ИСПД) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Регуляторами называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона.

В ФЗ «О персональных данных» установлены три регулятора:

- Роскомнадзор (защита прав субъектов персональных данных);
- Федеральная служба безопасности (ФСБ) (требования в области криптографии);
- Федеральная служба по техническому и экспортному контролю России (ФСТЭК) (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

ФЗ «О персональных данных» выделяет следующие категории персональных данных.

Общедоступные персональные данные – данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности.

Общедоступные источники персональных данных создаются в целях информационного обеспечения (например, справочники и адресные книги).

В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Важно отметить, что сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных, и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

Они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

Обработка биометрических персональных данных без согласия субъекта персональных данных может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Определение биометрических данных в российском законодательстве предоставляет оператору персональных данных возможность принятия самостоятельного решения об отнесении тех или иных данных к биометрическим.

Это породило немало споров. Рассмотрим пример с фотографией.

С одной стороны, она характеризует физиологические особенности человека. Но человек с течением времени может сильно измениться или злоумышленник может подделать внешние признаки под законного субъекта. Так ли однозначно в данном случае установление личности? В настоящее время представители регуляторов подтверждают, что фотография и видеоизображения относятся к биометрическим данным.

Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Задания к практической работе

1 Изучить общие сведения.

2 Произвести запуск СПС «КонсультантПлюс» и в созданной ранее группе папок создать группу папок с названием «Практическая работа № 4».

2.1 С помощью **Словаря терминов** в СПС «КонсультантПлюс» найти определения:

- «Документированная информация»;
- «Закрытый ключ ЭЦП»;
- «Открытый ключ ЭЦП»;
- «Удостоверяющий центр»
- «Обязательный экземпляр документа»;
- «Персональные данные».

2.2 Сохранить в папку «Термины и определения по электронной подписи и персональным данным».

2.3 Найти все нормативные документы, в которых закреплены принципы электронной подписи и персональных данных. Все найденные документы поместить в папку «*Нормативные документы по персональным данным*».

3 Решить примеры

Пример 1. М.Ю. Иванову при устройстве на работу к индивидуальному предпринимателю предложили заполнить анкету, в которой он должен был указать свое социальное положение, доход, жилищные условия.

Вопрос: являются ли указанные сведения, в контексте трудового законодательства, персональными данными работника?

Пример 2. В анкету для заполнения соискателями, устраивающимися на работу в охранное агентство, принадлежащее индивидуальному предпринимателю, были включены графы, предусматривающие представление информации о родственниках, осужденных к лишению свободы.

Вопрос: являются ли указанные сведения, в контексте трудового законодательства, персональными данными работника?

4 Для защиты практической работы продемонстрировать преподавателю результаты работы и ответить на контрольные вопросы

Контрольные вопросы

- 1 Дайте определение «Документированная информация», в каком нормативном документе используется данное понятие?
- 2 Дайте определение «Электронно-цифровая подпись» », в каком нормативном документе используется данное понятие?
- 3 Дайте определение «Закрытый ключ ЭЦП», в каком нормативном документе используется данное понятие?
- 4 Дайте определение «Открытый ключ ЭЦП», в каком нормативном документе используется данное понятие?
- 5 Дайте определение «Удостоверяющий центр», в каком нормативном документе используется данное понятие?
- 6 Дайте определение «Обязательный экземпляр документа», в каком нормативном документе используется данное понятие?
- 7 Дайте определение «Персональные данные», в каком нормативном документе используется данное понятие?

Библиографический список

- 1 Конституция Российской Федерации от 12.12.1993 // Российская газета. – 1993. – № 237. – 25 декабря.
- 2 Гражданский кодекс РФ (часть первая) № 51-ФЗ от 30.11.1994 : [в ред. от 31.01.2016] // Собрания законодательства РФ. – 1994. – № 32. – Ст. 3301.
- 3 Об информации, информационных технологиях и о защите информации : федер. закон РФ № 149-ФЗ от 27.07.2006 // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 03.03.2018).
- 4 Об электронной подписи : федер. закон РФ № 63-ФЗ от 06.04.2011 // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 03.03.2018).
- 5 О персональных данных : федер. закон РФ № 152-ФЗ от 27.07.2006 // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 03.03.2018).
- 6 Об обязательном экземпляре документов : федер. закон № 77-ФЗ от 29.12.1994 : [в ред. от 05.05.2014] // СПС «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 03.03.2018).
- 7 ГОСТ Р 34.10–94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. – М., 1994.
- 8 ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации, функция хэширования. – М., 1994.
- 9 Камынин, В. Л. КонсультантПлюс: учимся на примерах : учеб.-метод. пособие для студентов, обучающихся по направлению «Юриспруденция» / В. Л. Камынин, Н. Б. Ничепорук, С. Л. Зубарев, М. П. Пшеничнов. – М. : Консультант : АСУ, 2015. – 112 с. – URL: <https://infopedia.su/14xda65.html/>
- 10 Камынин, В. Л. Методические рекомендации для преподавателей, ведущих занятия по обучению работе со справочно-правовой системой «КонсультантПлюс» (направление «Юриспруденция») / В. Л. Камынин, Н. Б. Ничепорук, С. Л. Зубарев, М. П. Пшеничнов. – М. : Консультант : АСУ, 2015. – 107 с. – URL: <https://studfiles.net/preview/7042806/>
- 11 Румынина, В. В. Правовое обеспечение профессиональной деятельности / В. В. Румынина. – М. : Академия, 2007. – 186 с. – URL: <http://college-balabanovo.ru/Student/Bibl/Econ/POPD.pdf>
- 12 Куминова, В. Н. Правовое обеспечение профессиональной деятельности : учеб. пособие / В. Н. Куминова. – СПб. : Санкт-Петербургский колледж управления и экономики «Александровский лицей», 2010. – 124 с. – URL: <http://uchebana5.ru/cont/1310880.html>

Учебное издание

Правовые отношения
при использовании электронной подписи
и обработке персональных данных

С о с т а в и т е л и :

Катышева Марина Александровна, **Кирюхин** Юрий Григорьевич,
Кошелева Галина Викторовна, **Надеева** Наталья Николаевна,
Фионова Юлия Юрьевна, **Шокорова** Нина Николаевна

Редактор *Е. Г. Акимова*
Технический редактор *М. Б. Жучкова*
Компьютерная верстка *М. Б. Жучковой*

Подписано в печать 06.12.2018.
Формат 60×84¹/₁₆. Усл. печ. л. 1,16.
Тираж 100. Заказ № 700.

Издательство ПГУ.
440026, Пенза, Красная, 40.
Тел./факс: (8412) 56-47-33; e-mail: iic@pnzgu.ru

