Чернов В.И.

ПОСТАНОВЛЕНИЕ
АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО РАЙОНА "ЧЕРНЯНСКИЙ РАЙОН" БЕЛГОРОДСКОЙ ОБЛАСТИ

18 апреля 2013 года № 344

Об утверждении Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет»

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в администрации муниципального района «Чернянский район» Белгородской области **п о с т а н о в л я е т:**

1. Утвердить Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет».

2. Контроль исполнения настоящего постановления оставляю за собой.

Первый заместитель главы администрации района по экономическому развитию **Т.П.Круглякова**

Утверждено

постановлением администрации
муниципального района
«Чернянский район»

от_____ 2013 г. № _____

Положение
по организации и проведению работ
по обеспечению безопасности персональных данных при их обработке
в ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет»
администрации Чернянского района

1. Общие положения

1.1. Назначение.

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Кадровый учет» и информационной системе персональных данных «Бухгалтерский учет» администрации Чернянского района (далее – Положение) разработано с целью определения перечня мероприятий по организации и техническому обеспечению безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн), определения необходимости создания системы защиты персональных данных (далее – СЗПДн), определения стадий создания СЗПДн, определения перечня и содержания организационно-распорядительной документации, решения вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты.

Положение разработано на основе ФЗ №152-ФЗ «О персональных данных», Постановления Правительства РФ №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК, ФСБ, Мининформсвязи России № 55/86/20 «Порядок проведения классификации информационных систем персональных данных», «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утвержденных ФСТЭК России.

1.2. Нормативно-правовые акты по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

При организации и проведении работ по обеспечению безопасности ПДн при их обработке в ИСПДн необходимо руководствоваться следующими нормативно-правовыми актами:

- Конституция Российской Федерации от 12 декабря 1993г.;
- Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»;
- Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании»;
- Закон Российской Федерации от 8 августа 2001г. № 128-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 30.12.01г. №197-ФЗ «Трудовой кодекс Российской Федерации»;
- Федеральный закон от 13.06.96г. №63-ФЗ «Уголовный кодекс Российской Федерации»;
- Федеральный закон от 30.12.01г. №195-ФЗ «Кодекс Российской Федерации об административных правонарушениях»;
- Федеральный закон №98-ФЗ от 29.07.04г. «О коммерческой тайне»;
- Указ Президента Российской Федерации от 16 августа 2004г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
- Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 26 января 2006г. № 45 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства Российской Федерации от 15 августа 2006г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 31 августа 2006г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;
- Постановление Правительства РФ от 17.11.07г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 05 декабря 1991г. №35 «О перечне сведений, которые не могут составлять коммерческую тайну»;
- Постановление Правительства РФ 06.07.08г. №512 от «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства РФ от 15.09.08г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Указ Президента РФ от 17.03.08г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Постановление Правительства РФ от 26.06.95г. №608 «О сертификации средств защиты информации»;

– Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002г. № 282;

– Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994г.;

– Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Приказ Гостехкомиссии России, 1992г.;

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992г.;

– Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992г.;

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997г.;

– Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Приказ Гостехкомиссии России от 4 июня 1999г. № 114;

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Приказ Гостехкомиссии России от 19.06.2002г. № 187;

– Порядок проведения классификации информационных систем персональных данных, ФСТЭК, ФСБ, Мининформсвязи России, 13.02.2008г. № 55/86/20;

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России, 14.02.2008г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России, 15.02.2008г.;

– Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России, 15.02.2008г.;

– Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, ФСТЭК России, 15.02.2008г.;

– Приказ Россвязьохранкультуры от 28.03.08г. №154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных»;

– Приказ Россвязькомнадзора от 17.07.08г. №08 «Об утверждении образца формы уведомления об обработке персональных данных»;

– Приказ ФСБ Российской Федерации от 09.02.05г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– Приказ ФАПСИ от 13.06.01г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– «Положение о сертификации средств защиты информации по требованиям безопасности информации», приказ Председателя Гостехкомиссии России от 27.10.95г. №199;

– Приказ ФСТЭК РФ от 28.08.07г. №181 «Об утверждении административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации»;

– Приказ ФСТЭК РФ от 28.08.07г. №182 «Об утверждении административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

– «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», ФСБ России;

– «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», ФСБ России;

– «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или)

передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, 2002г.;

–«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, 2002г.;

и другими нормативно-правовыми актами.

2. Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн

2.1. Перечень мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн.

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационных системах информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

2.2. Необходимость создания СЗПДн.

Необходимость создания СЗПДн в администрации района определяется требованиями действующего законодательства Российской Федерации, а именно:

–в соответствии с пунктом 3 статьи 19 Федерального закона №152-ФЗ: «Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

–в пункте б статьи 12 Постановления Правительства РФ №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» определяется:

«12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

к) описание системы защиты персональных данных»;

–пункт 2.6 «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» определяет: «Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ по созданию ИСПДн и должны осуществляться в виде создаваемой системы (подсистемы) защиты персональных данных».

2.3. Стадии создания СЗПДн.

Рекомендуются следующие стадии создания СЗПДн:

–предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

–стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

–стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

2.3.1. Предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание.

На предпроектной стадии по обследованию ИСПДн рекомендуются следующие мероприятия:

–устанавливается необходимость обработки ПДн в ИСПДн;

–определяется перечень ПДн, подлежащих защите от несанкционированного доступа (далее – НСД);

–определяются условия расположения ИСПДн относительно границ контролируемой зоны (далее - КЗ);

–определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

–определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

–определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;

–определяется класс ИСПДн;

–уточняется степень участия персонала в обработке ПДн, характер их взаимодействия между собой;

–определяются (уточняются) угрозы безопасности ПДн к конкретным условиям функционирования (разработка частной модели угроз).

По результатам предпроектного обследования на основе настоящего документа, с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

2.3.2. Стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн.

На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

–разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

–разработка раздела технического проекта на ИСПДн в части защиты информации;

–строительно-монтажные работы в соответствии с проектной документацией;

–использование серийно выпускаемых технических средств обработки, передачи и хранения информации;

–разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

–использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

–сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

–разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

–определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности ПДн;

–разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

–выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

2.3.3. Стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:

–выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

–опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн;

–приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

–организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

–оценка соответствия ИСПДн требованиям безопасности ПДн.

2.4. Организационно-распорядительная документация, разрабатываемая в администрации района.

2.4.1. Перечень организационно-распорядительных документов, разрабатываемых в администрации района.

Во исполнение требований Постановления Правительства РФ №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», «Специальных требований и рекомендаций по технической защите конфиденциальной информации», «Порядка проведения классификации

информационных систем персональных данных», «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» на объекте информатизации необходимо разработать следующие организационно - распорядительные документы (далее ОРД):

- Локальный нормативный акт (положение, инструкция) о персональных данных.
- Перечень сведений конфиденциального характера.
- Положение о маркировке.
- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн.
- Требования по обеспечению безопасности ПДн при обработке в ИСПДн.
- Технический паспорт.
- Частное техническое задание на разработку СЗПДн.
- Постановление о создании комиссии по классификации ИСПДн.
- Акт классификации ИСПДн.
- Журналы учета и хранения документов и магнитных носителей с информацией ограниченного доступа (Журнал регистрации носителей информации).
- Обязательство о неразглашении конфиденциальной информации (персональных данных).
- Должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.
- Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации (администратору, пользователям, по работе с СЗИ, антивирусному контролю).
- Постановление о допуске сотрудников к работе с персональными данными.
- Постановление о назначении администратора безопасности ИСПДн.
- Список лиц, имеющих доступ в помещение, где обрабатываются ПДн.
- Список лиц, допущенных обработке ПДн.
- Постановление о вводе в эксплуатацию объекта информатизации.

2.4.2. Требования к содержанию ОРД

Технический паспорт должен содержать:

1) Общие сведения об объекте информатизации для работы с ИСПДн.
   - Наименование объекта.

- Расположение объекта.
- Класс АС, номер и дата акта классификации АС.

2) Состав оборудования объекта информатизации.

- Состав основных технических средств и систем (далее – ОТСС).
- Состав вспомогательных технических средств и систем (далее – ВТСС) объекта.
- Структуру, топологию и размещение ОТСС относительно границ контролируемой зоны объекта (структурная (топологическая) схема с указанием информационных связей между устройствами; схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны, схема прокладки линий передачи конфиденциальной информации с привязкой к границам контролируемой зоны объекта и др.).
- Системы электропитания и заземления.
- Состав средств защиты информации.
- Состав используемых в АС программных средств.

3) Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации.

4) Результаты периодического контроля.

5) Лист учета изменений и дополнений.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

1) обоснование разработки СЗПДн;

2) исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

3) класс ИСПДн;

4) ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

5) конкретизацию мероприятий и требований к СЗПДн;

6) перечень предполагаемых к использованию сертифицированных средств защиты информации;

7) обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

8) состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

3. Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты

Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты является важным аспектом поддержания требуемого уровня безопасности ПДн. К основным вопросам управления обеспечением безопасности ПДн относятся:

-распределение функций управления доступом к ПДн и их обработкой между должностными лицами;

-определение порядка изменения правил доступа к защищаемой информации;

-определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

-определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

-определение порядка проведения контрольных мероприятий и действий по его результатам.

4. Контроль за обеспечением безопасности ПДн

Контроль за обеспечением безопасности ПДн заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться оператором или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.