Муниципальное бюджетное учреждение «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги»

ПРИКАЗ

от 24.02.2016 г. № 17

об утверждении Политики
информационной безопасности

Во исполнение:

– п.2, п.4, п.6 ч.1 и ч.2 ст.18.1 Федерального закона РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ;

– ст.2 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 г. № 211;

– раздела 5.5. Методических рекомендаций для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, согласованные с начальником 2 управления ФСТЭК России 22.12.2009 г., утвержденных директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009 г., а также Приложением 5 к указанным Методическим рекомендациям

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику информационной безопасности в МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» (далее - Политика).
2. Контроль за выполнением настоящего приказа возложить на ответственного за организацию работ и обеспечение безопасности персональных данных заместителя директора по административно-хозяйственной части Якименко О.А.
3. Приказ довести до заинтересованных лиц под роспись в листе ознакомления.

Директор МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» С.В. Колышкина

УТВЕРЖДЕНА
приказом директора МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги»
от 24.02.2016 г. № 17

ПОЛИТИКА
информационной безопасности в МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги»

1. Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность информации (данных) - состояние защищенности информации (данных); при котором обеспечены ее (их) конфиденциальность, доступность и целостность; состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

Доступность (санкционированная доступность) информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Замысел защиты информации - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Компьютерный вирус (КВ) - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Криптографическое средство защиты информации – средства шифрования (аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении); средства имитозащиты (аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации); средства электронной цифровой подписи (аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой

подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи); средства кодирования (средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций); средства изготовления ключевых документов (независимо от вида носителя ключевой информации); ключевые документы (независимо от вида носителя ключевой информации).

Межсетевой экран (МЭ) (средство межсетевого экранирования) - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС.

Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

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.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Оператор персональных данных (оператор ПДн) - 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.

Ответственный за организацию обработки персональных данных - должностное лицо оператора ПДн, осуществляющее:

- внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Политика безопасности (информации в организации) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

СЗПДн – система (подсистема) защиты персональных данных.

Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

Цель защиты информации - заранее намеченный результат защиты информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

2. Общие положения

2.1. Настоящая Политика информационной безопасности в МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» (далее – Политика) определяет общую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации.

2.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Концепции информационной безопасности информационных систем персональных данных МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» (далее – Учреждение).

2.3. Целью настоящей Политики является определение основных правил обеспечения безопасности объектов защиты персональных данных Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба от возможной реализации угроз безопасности персональных данных.

2.4. 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.

2.5. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения персональных данных.

2.6. В Политике определены: общий замысел защиты информации Учреждения, требования к пользователям информационных систем персональных данных, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности должностных лиц, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных Учреждения.

2.7. Требования Политики обязательны для всех работников, представителей контрольно-надзорных органов, допущенных к защищаемой информации на законных основаниях, а также работников иных организаций, допущенных к защищаемой информации для проведения работ по гражданско-правовым договорам.

2.8. В соответствии с ч.2. ст.18.1 Федерального закона РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ Учреждение обязано опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящей Политике.

3. Система защиты персональных данных Учреждения

3.1. Система защиты персональных данных строится на основании:

- законодательства Российской Федерации в области защиты персональных данных, руководящих документов Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России;
- организационно-распорядительных документов Учреждения в сфере защиты персональных данных (Приложение к Политике).

3.2. На основании указанных документов определяется необходимый уровень защищенности персональных данных каждой информационной системы персональных данных МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги».

3.3. На основании анализа актуальных угроз безопасности персональных данных, описанного в Моделях угроз безопасности при их обработке в информационных системах

Учреждения и Отчете о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах Учреждения, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных.

3.4. Для каждой информационной системы персональных данных должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке персональных данных, на всех элементах информационных систем:

- персональные компьютеры пользователей;
- система управления базами данных – СУБД;
- граница локальной вычислительной сети;
- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются персональные данные.

3.5. В зависимости от уровня защищенности информационных систем и актуальных угроз система защиты персональных данных может включать в себя следующие технические средства:

- антивирусные средства для персональных компьютеров пользователей;
- средства межсетевого экранирования;
- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

3.6. Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки персональных данных: операционной системой, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать в себя:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- осуществление обнаружения вторжений.

4. Требования к подсистемам защиты персональных данных

4.1. В соответствии с реализуемыми функциями защиты система защиты персональных данных включает в себя следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

4.2. Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от уровня защищенности персональных данных при их обработке в информационных системах персональных данных, определенного в Актах определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

4.3. Подсистема управления доступом предназначена для реализации следующих функций:

- идентификации и проверки подлинности субъектов доступа при входе в информационную систему;
- идентификации узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю.

4.4. Подсистема регистрации и учета предназначена для реализации следующих функций:

- регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее останова;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрация попыток доступа программных средств к каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема регистрации и учета может быть реализована с помощью организационных мер защиты информации. Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по регистрации действий, осуществляемых в информационной системе.

4.5. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем, а также средств защиты при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов информационных систем.

4.6. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты персональных компьютеров пользователей. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную (удаленную установку) деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы информационных систем.

4.7. Подсистема межсетевого экранирования предназначена для реализации следующий функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема может быть реализована внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальной вычислительной сети.

4.8. Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационных систем, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

4.9. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путем внедрения криптографических программно-аппаратных комплексов.

5. Категории пользователей информационных систем

5.1. В Концепции информационной безопасности информационных систем Учреждения определены основные категории пользователей информационных систем персональных данных.

5.2. Для определения требований к пользователям информационных систем, степени ответственности, уровня защищенности, должностным обязанностям сотрудников, ответственных за обеспечение безопасности персональных данных выделяются следующие группы пользователей информационных систем персональных данных Учреждения, участвующих в обработке и хранении персональных данных:

- администратор информационной системы персональных данных;
- администратор безопасности информации;
- администратор сети;
- пользователь информационной системы персональных данных;
- программист-разработчик информационной системы персональных данных.

Данные о группах пользователей, уровне их доступа и информированности отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных Учреждения.

5.3. Администратор информационной системы персональных данных:

5.3.1. Администратор информационной системы – должностное лицо, ответственное за настройку, внедрение и сопровождение информационной системы персональных данных. Обеспечивает функционирование подсистемы управления доступом информационных систем и уполномоченное осуществлять предоставление и разграничение доступа конечного пользователя к элементам информационных систем, хранящим персональные данные.

5.3.2. Администратор информационной системы персональных данных обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;

– обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных;

– имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;

– обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

5.4. Администратор безопасности информации:

5.4.1. Администратор безопасности информации обладает следующим уровнем доступа:

– обладает правами администратора информационной системы персональных данных;

– обладает полной информацией об информационной системе персональных данных;

– имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов информационной системы персональных данных;

– не имеет прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

5.4.2. Администратор безопасности информации уполномочен:

– реализовывать политики безопасности в части настройки средств криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь информационной системы персональных данных получает возможность работать с элементами информационной системы персональных данных;

– осуществлять аудит средств защиты;

– устанавливать доверительные отношения своей защищенной сети с сетями других участников информационного обмена.

5.5. Администратор сети – должностное лицо, ответственное за функционирование телекоммуникационной подсистемы информационной системы персональных данных. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

5.5.1. Администратор сети обладает следующим уровнем доступа:

– обладает частью информации о системном и прикладном программном обеспечении информационной системы персональных данных;

– обладает частью информации о технических средствах и конфигурации информационной системы персональных данных;

– имеет физический доступ к техническим средствам обработки информации и средствам защиты;

– знает, по меньшей мере, одно легальное имя доступа.

5.6. Пользователь информационной системы:

5.6.1. Пользователь информационной системы - должностное лицо МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги», участвующее в процессе эксплуатации информационной системы персональных данных и осуществляющее обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных в информационную систему персональных данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных. Пользователь информационной системы персональных данных не имеет полномочий для управления подсистемами обработки данных и безопасности.

5.6.2. Пользователь информационной системы персональных данных обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;

– располагает конфиденциальными данными, к которым имеет доступ.

5.7. Программист-разработчик информационной системы персональных данных:

5.7.1. Программист-разработчик информационной системы – специалист, осуществляющий разработку прикладного программного обеспечения, обеспечивающий его сопровождение на защищаемом объекте. К данной группе могут относиться как специалисты Учреждения, так и сотрудники сторонних организаций.

5.7.2. Программист-разработчик информационной системы обладает следующим уровнем доступа:

– обладает информацией об алгоритмах и программах обработки информации на информационной системе Учреждения;

– обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии информационной системы Учреждения и технических средствах обработки и защиты персональных данных.

6. Требования к пользователям информационных систем по обеспечению защиты персональных данных

6.1. Все пользователи информационных систем персональных данных Учреждения должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

6.2. Все сотрудники Учреждения должны быть ознакомлены с настоящей Политикой и документами, регламентирующими требования по защите персональных данных в Учреждении, а также обучены навыкам выполнения процедур, необходимых для санкционированного использования информационных систем персональных данных.

6.3. Пользователи информационных систем персональных данных, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а так же исключить возможность их утери или использования третьими лицами. Пользователи информационных систем персональных данных Учреждения несут персональную ответственность за сохранность идентификаторов.

6.4. Пользователи информационных систем персональных данных должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации).

6.5. Пользователи информационных систем персональных данных должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица; должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

6.6. Пользователям информационных систем персональных данных запрещается:

- устанавливать постороннее программное обеспечение;
- подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию;
- разглашать защищаемую информацию третьим лицам.

6.7. При работе с персональными данными пользователи информационных систем персональных данных Учреждения обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов персональных компьютеров.

При завершении работы в информационной системе пользователи информационных систем персональных данных обязаны защитить персональный компьютер с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

6.8. Пользователи информационных систем персональных данных должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение.

6.9. Пользователи информационных систем персональных данных обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем, которые могут повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководителю подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

7. Ответственность

Пользователи информационных систем персональных данных Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ПРИЛОЖЕНИЕ
к Политике информационной безопасности в МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги»

ПЕРЕЧЕНЬ
организационно-распорядительных документов МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» в сфере защиты персональных данных

В МБУ «Центр социального обслуживания граждан пожилого возраста и инвалидов города Юрги» (далее – Учреждение) принимаются следующие виды организационно-распорядительных документов в сфере защиты персональных данных, обрабатываемых в информационных системах персональных данных Учреждения:

1) Акт определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
2) Журнал регистрации и учета обращений субъектов персональных данных о выполнении их законных прав;
3) Журнал учета применяемых средств защиты информации информационных систем персональных данных;
4) Журнал учета съемных носителей конфиденциальной информации;
5) Инструкция администратора информационных систем персональных данных;
6) Инструкция администратора по обеспечению безопасности обработки персональных данных;
7) Инструкция о порядке допуска сотрудников со средствами криптографической защиты информации;
8) Инструкция о порядке учета, хранения и уничтожения носителей персональных данных в Учреждении;
9) Инструкция ответственного за выполнение работ по обеспечению безопасности персональных данных;
10) Инструкция ответственного за организацию обработки и обеспечение безопасности персональных данных;
11) Инструкция по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах персональных данных;
12) Инструкция по организации антивирусной защиты информационных систем;
13) Инструкция по организации парольной защиты в информационных системах;
14) Инструкция пользователя информационных систем персональных данных;
15) Инструкция пользователя по обеспечению безопасности обработки персональных данных;
16) Инструкция пользователя при возникновении внештатных ситуаций;
17) Концепция информационной безопасности информационных систем персональных данных Учреждения;
18) Матрица доступа сотрудников к персональным данным;
19) Модель нарушителя в информационных системах персональных данных;
20) Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
21) Отчет о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных;

22) Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

23) Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

24) Перечень информационных систем персональных данных;

25) Перечень персональных данных, подлежащих защите в информационных системах персональных данных;

26) Перечень помещений, предназначенных для обработки персональных данных;

27) Перечень сведений конфиденциального характера;

28) Перечень сотрудников, имеющих доступ к работе с персональными данными;

29) План внутренних проверок;

30) План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных;

31) Политика информационной безопасности;

32) Положение о порядке обработки и обеспечении безопасности персональных данных;

33) Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных;

34) Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;

35) Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных;

36) Правила обработки персональных данных;

37) Правила осуществления внутреннего контроля;

38) Правила работы с обезличенными персональными данными;

39) Правила рассмотрения запросов субъектов персональных данных;

40) Приказ об утверждении состава комиссии по защите информации;

41) Приказ о назначении ответственных за организацию обработки и обеспечение безопасности персональных данных;

42) Приказ о проведении работ по защите персональных данных;

43) Приказ об установлении контролируемой зоны;

44) Список лиц, наделенных правом использования электронной подписи;

45) Список сотрудников, имеющих доступ в помещения, предназначенные для обработки персональных данных;

46) Технический паспорт информационной системы персональных данных.