МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
"ЦЕНТРАЛИЗОВАННАЯ БУХГАЛТЕРИЯ
ДИНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ"

ПРИКАЗ

от 22.06.2026

№ 06-01-01

станица Динская

Об организации защиты персональных данных.

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», приказываю:

1. Утвердить Положение об обработке и защите персональных данных в муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения» (приложение №1).

2. Утвердить Политику информационной безопасности информационных систем персональных данных в Муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения» (приложение №2).

3. Утвердить Концепцию информационной безопасности информационных систем персональных данных в Муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения (приложение №3).

4. Утвердить Перечень персональных данных, подлежащих защите в Муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения (приложение №4).

5. Утвердить Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных в

Муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения (приложение №5).

6. Отменить приказ № 41-01-01 от 17 ноября 2023 года «Об организации защиты персональных данных»

7. Контроль за выполнением приказа оставляю за собой.

Руководитель МКУ "ЦБ ДСП" Ковальчук Р.П

Согласованно главный специалист Виноградов В.А

С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г
С приказом ознакомлен(а)_____ «__»_____2026 г

Приложение №1
к приказу руководителя
МКУ «ЦБ ДСП» от 22.06.2026
№ 06-01-01

Положение
о защите, хранении, обработке и передаче персональных данных работников муниципального казенного учреждения «Централизованная бухгалтерия Динского сельского поселения»

1. Общие положения

1.1. Настоящее положение разработано в соответствии с положениями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных) и определяет порядок сбора, учета, обработки, накопления, использования, распространения и хранения персональных данных работников муниципального казенного учреждения «Централизованная бухгалтерия Динского сельского поселенения» (далее - организация, работодатель).

1.2. Целью настоящего положения является обеспечение защиты персональных данных работников организации от несанкционированного доступа и разглашения.

1.3. В целях настоящего положения под персональными данными понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных.

1.4. К персональным данным относятся:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- сведения о знании иностранных языков;
- данные об образовании (наименование учебного заведения, год окончания, документ об образовании, квалификация, специальность);
- профессия;
- стаж работы (общий, непрерывный, дающий право на выслугу лет);
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- паспорт (номер, дата выдачи, кем выдан);
- адрес места жительства (по паспорту, фактический), дата регистрации по месту жительства;
- номер телефона (домашний, сотовый);
- сведения о воинском учёте;
- сведения о состоянии здоровья работника, необходимые работодателю для определения пригодности для выполнения поручаемой работы и предупреждения профессиональных заболеваний, предусмотренные действующим законодательством Российской Федерации;
- содержание заключенного с работником контракта или трудового договора;
- сведения об аттестации, повышении квалификации, профессиональной переподготовке

работника;

- сведения об использованных отпусках;
- сведения об имеющихся наградах (поощрениях), почётных званиях;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения о социальных льготах (в соответствии с действующим законодательством Российской Федерации);
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения);
- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

1.5. Все персональные данные работника работодатель может получить только от него самого. В случаях когда работодатель может получить необходимые персональные данные работника только у третьего лица, работодатель в обязательном порядке уведомляет об этом работника и получает от него письменное согласие.

1.6. Работодатель в обязательном порядке сообщает работнику о целях, способах и источниках получения персональных данных, а также о перечне подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

1.7. При изменении персональных данных работник письменно уведомляет работодателя о таких изменениях в срок, не превышающий 7 рабочих дней.

1.8. Персональные данные работника являются конфиденциальной информацией и не могут быть использованы работодателем или любым иным лицом в личных целях.

1.9. При определении объема и содержания персональных данных работника работодатель руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

1.10. Работодатель, работник и его представители совместно разрабатывают меры защиты персональных данных работника.

1.11. Работник не должен отказываться от своих прав на сохранение и защиту тайны.

2. Обработка, передача и хранение персональных данных работника

2.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя.

2.2. Работодатель обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных:

Цель обработки персональных данных: ведение бухгалтерского учета подведомственных организаций.

Категория персональных данных	Перечень персональных данных	Категория работников	Тип угрозы	Уровень защищенности
только общие персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения; - адрес; - семейное положение; - образование; - профессия; - социальное положение; - доходы.	Руководитель Главный бухгалтер Зам. Главного бухгалтера Главный специалист Ведущий специалист Специалист 1й категории	угрозы первого типа	Высокий уровень защищенности
общие и специальные персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения; - адрес; - семейное положение; - образование; - профессия; - социальное положение; - доходы; - расовая, национальная принадлежности; - политические взгляды; - религиозные или философские убеждения; - состояние здоровья, интимной жизни; - сведения о судимости.	Руководитель Главный бухгалтер Зам. Главного бухгалтера Главный специалист Ведущий специалист Специалист 1й категории	угрозы первого типа	Высокий уровень защищенности

2.3. При 4-м уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

2.4. При 3-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пункте 2.3 настоящего положения, назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

2.5. При 2-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пунктах 2.3, 2.4 настоящего положения, ограничивает доступ к содержанию электронного журнала сообщений, за исключением для должностных лиц (работников), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

2.6. При 1-м уровне защищенности персональных данных работодатель дополнительно к мерам, перечисленным в пунктах 2.3-2.5 настоящего положения:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным, содержащимся в информационной системе;

- создает структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности.

2.7. Работодатель обрабатывает без использования средств автоматизации следующие категории персональных данных работника, обеспечивает их защиту, которые хранятся на бумажных носителях:

Цель обработки персональных данных: ведение бухгалтерского учета подведомственных организаций..

Категория персональных данных	Перечень персональных данных	Категория работников
только общие персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения; - адрес; - семейное положение; - образование; - профессия; - социальное положение; - доходы.	Руководитель Главный бухгалтер Зам. Главного бухгалтера Главный специалист Ведущий специалист Специалист 1й категории
общие и специальные персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения; - адрес; - семейное положение;	Руководитель Главный бухгалтер Зам. Главного бухгалтера Главный специалист Ведущий специалист

	- образование; - профессия; - социальное положение; - доходы; - расовая, национальная принадлежности; - политические взгляды; - религиозные или философские убеждения; - состояние здоровья, интимной жизни; - сведения о судимости.	Специалист 1й категории
общие и биометрические персональные данные	- фамилия, имя, отчество; - год, месяц, дата рождения; - место рождения; - адрес; - семейное положение; - образование; - профессия; - социальное положение; - доходы;	Руководитель Главный бухгалтер Зам. Главного бухгалтера Главный специалист Ведущий специалист Специалист 1й категории

2.8. Работодатель при обработке персональных данных работника на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников.

2.9. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками ответственными за обработку персональных данных.

2.10. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

2.11. Специалист бухгалтерии в праве использовать персональные данные работника в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.

2.12. Руководитель организации может передавать персональные данные работника третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных законодательством.

2.13. При передаче персональных данных работника специалист бухгалтерии и руководитель организации предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

2.14. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работника, определяются должностными инструкциями.

2.15. Все сведения о передаче персональных данных работника учитываются для контроля правомерности использования данной информации лицами, ее получившими.

2.16. Руководитель отдела кадров обязан предоставлять персональную информацию в пенсионный фонд, фонд обязательного медицинского страхования (ФОМС), фонд социального страхования (ФСС) по форме, в порядке и объеме, установленных законодательством Российской Федерации.

2.17. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.18. Передача информации, содержащей сведения о персональных данных работников, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

2.19. Персональные данные работника, в сейфе на бумажных носителях: трудовая книжка, личная карточка, личное дело и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным работника имеют:

- руководитель организации;
- специалисты орагнизации;

3. Требования к помещениям, в которых производится обработка персональных данных

3.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

3.3. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

3.4. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

4. Обязанности работодателя по хранению и защите персональных данных работника

4.1. Работодатель за свой счет обеспечивает защиту персональных данных работника от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации.

4.2. Работодатель принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. Работодатель самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, относятся:

1) назначение работодателем ответственного за организацию обработки персональных

данных;

2) издание работодателем документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на работодателя не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике работодателя в отношении обработки персональных данных, локальным актам работодателя;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых работодателем мер, направленных на обеспечение выполнения обязанностей, предусмотренных названным Федеральным законом;

6) ознакомление работников работодателя, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику работодателя в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.3. Работодатель знакомит работника и его представителей с настоящим положением и их правами в области защиты персональных данных под расписку.

4.4. Работодатель осуществляет передачу персональных данных работника только в соответствии с настоящим положением и законодательством Российской Федерации.

4.5. Работодатель предоставляет персональные данные работника только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим положением и законодательством Российской Федерации.

4.6. Работодатель не вправе получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать персональные данные работника о его личной жизни, только с письменного согласия работника.

4.7. Работодатель не вправе получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.8. Работодатель не вправе предоставлять персональные данные работника в коммерческих целях без письменного согласия работника.

4.9. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий работника на обработку его персональных данных. Работодатель обеспечивает работнику возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных работником для распространения.

4.10. В согласии на обработку персональных данных, разрешенных работником для

распространения, работник вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных работодателем неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ работодателя в установлении работником запретов и условий, предусмотренных настоящим пунктом, не допускается.

Установленные работником запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных им для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

4.11. Работодатель обеспечивает работнику свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством.

4.12. Работодатель по требованию работника предоставляет ему полную информацию о его персональных данных и обработке этих данных.

5. Права работника на защиту его персональных данных

5.1. Работник в целях обеспечения защиты своих персональных данных, хранящихся у работодателя, имеет право:

- получать полную информацию о своих персональных данных, их обработке, хранении и передаче;

- определять своих представителей для защиты своих персональных данных;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями настоящего положения и законодательства Российской Федерации.

При отказе работодателя исключить или исправить персональные данные работника работник вправе заявить работодателю в письменном виде о своем несогласии с соответствующим обоснованием;

- требовать от работодателя извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2. Если работник считает, что работодатель осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы, работник вправе обжаловать действия или бездействие работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6. Порядок уничтожения, блокирования персональных данных

6.1. В случае выявления неправомерной обработки персональных данных при обращении работника работодатель осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому работнику, с момента такого обращения на период проверки.

6.2. В случае выявления неточных персональных данных при обращении работника работодатель осуществляет блокирование персональных данных, относящихся к этому работнику, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы работника или третьих лиц.

6.3. В случае подтверждения факта неточности персональных данных работодатель на основании сведений, представленных работником, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает

блокирование персональных данных.

6.4. В случае выявления неправомерной обработки персональных данных, осуществляемой работодателем, работодатель в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

6.5. В случае если обеспечить правомерность обработки персональных данных невозможно, работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

6.6. Об устранении допущенных нарушений или об уничтожении персональных данных работодатель уведомляет работника.

6.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав работника, работодатель с момента выявления такого инцидента работодателем, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав работника, и предполагаемом вреде, нанесенном правам работника, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном работодателем на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.8. В случае достижения цели обработки персональных данных работодатель прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором.

6.9. В случае отзыва работником согласия на обработку его персональных данных работодатель прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором.

6.10. В случае обращения работника к работодателю с требованием о прекращении обработки персональных данных работодатель в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления работодателем в адрес работника мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.10 настоящего положения, работодатель осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.12. После истечения срока нормативного хранения документов, содержащих персональные данные работника, или при наступлении иных законных оснований документы подлежат уничтожению.

6.13. Работодатель для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

6.14. По результатам экспертизы документы, содержащие персональные данные работника и подлежащие уничтожению:

- на бумажном носителе – сдаются в специализированную утилизирующею организацию.

- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

8. Заключительные положения

8.1. Настоящее положение вступает в силу с момента его утверждения.

8.2. Работодатель обеспечивает неограниченный доступ к настоящему документу.

8.3. Настоящее положение доводится до сведения всех работников персонально под роспись.

С положением ознакомлены:

N п/п	Ф. И. О. работника	Дата	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

Приложение №2
к приказу руководителя
МКУ «ЦБ ДСП» от 22.06.2026
№ 06-01-01

Политика информационной безопасности информационных систем персональных данных в муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения»

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с положениями **Федерального закона** от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее - Закон об информации, информационных технологиях и о защите информации), **Федерального закона** от 27 июля 2006 г. N 152-ФЗ "О персональных данных", **постановления** Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", **приказа** Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений" (далее - Требования о защите информации), **приказа** Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

1.2. В рамках настоящей Политики под информационной системой понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.3. Оператор обеспечивает защиту информации на всех стадиях (этапах) обработки и хранения информации, создания и развития (модернизации), эксплуатации и вывода из эксплуатации информационной системы в рамках функций, выполняемых им в соответствии с **Законом** об информации, информационных технологиях и о защите информации.

1.4. Действие настоящей Политики распространяется на всех работников учреждения, информационные системы, материальные и цифровые активы оператора, а также внешних пользователей, работающих с его данными.

Настоящая Политика обязательна для исполнения всеми работниками оператора в части, их касающейся.

1.5. Перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите, определен в приложении к настоящей Политике.

2. Цели и задачи защиты информации

2.1. Цели защиты информации определяются оператором исходя из ожидаемых результатов, направленных на недопущение или снижение негативных последствий от

реализации угроз безопасности.

2.2. Основные цели защиты информации включают:

- обеспечение защиты (некриптографическими методами) информации;

- предотвращение несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, блокирования доступа к информации;

- недопущение (снижение возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее - нарушение безопасности информации);

- недопущение (снижение возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

2.3. Основными задачами защиты информации являются:

- защита от несанкционированного доступа к информации, содержащейся в информационной системе;

- предотвращение утечки информации;

- мониторинг и обнаружение угроз;

- создание безопасной цифровой среды.

3. Принципы защиты информации

3.1. Защита информации, содержащейся в информационной системе оператора, основывается на следующих принципах:

- конфиденциальность: информация доступна только авторизованным пользователям, что создает защиту от утечек;

- целостность: защита данных от случайного или намеренного изменения, подмены или удаления;

- доступность: обеспечение бесперебойного доступа к информации авторизованных пользователей в нужное время;

- законность и обоснованность защиты: защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством;

- системность: необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления, во всех структурных элементах, при всех режимах функционирования;

- комплектность: согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках ее компонентов;

- непрерывность защиты: принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования;

- разумная достаточность: стоимость защиты должна соответствовать потенциальному ущербу от потери данных;

- персональная ответственность: каждый субъект доступа несет ответственность за свои действия.

4. Объекты защиты

4.1. Объектами защиты информации являются программные, программно-аппаратные средства, информационные системы, сети и подсети, образующие информационно-телекоммуникационную инфраструктуру оператора.

4.2. Перечень объектов защиты определен в приложении к настоящей Политике.

5. Организация и управление деятельностью по защите информации

5.1. Оператор организует деятельность по защите информации и управляет ею в соответствии с **Требованиями** о защите информации и настоящей Политикой.

5.2. Организация деятельности по защите информации включает:

- разработку и утверждение настоящей Политики;
- определение лиц, ответственных за защиту информации;
- применение программных, программно-аппаратных средств, предназначенных для защиты информации;
- разработку и утверждение внутренних стандартов по защите информации;
- разработку и утверждение внутренних регламентов по защите информации;
- выделение организационных, технических и иных ресурсов, необходимых для защиты информации.

5.3. Защиту информации организовывает руководитель оператора или по его решению ответственное лицо.

5.4. Обязанности (функции) и полномочия ответственного лица по организации деятельности по защите информации, управлению защитой информации, а также по организации контроля за данной деятельностью у оператора должны быть включены в должностные обязанности (трудовые функции) ответственного лица.

Состав обязанностей (функций) и полномочий ответственного лица должен быть достаточен для организации деятельности по защите информации и управления этой деятельностью в соответствии с **Требованиями** о защите информации и настоящей Политикой, а также организации контроля за данной деятельностью у оператора.

5.5. Руководитель оператора, ответственное лицо **создают** (определяют) структурное подразделение или **назначают** отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации (далее - структурное подразделение (специалисты) по защите информации).

Функции и полномочия по защите информации структурного подразделения по защите информации определяются в **положении** о структурном подразделении или ином документе, в соответствии с которым функционирует структурное подразделение.

Обязанности (функции) и полномочия специалистов по защите информации по проведению мероприятий и принятию мер по защите информации должны быть установлены в их должностных обязанностях (трудовых функциях).

Состав обязанностей (функций) и полномочий по защите информации структурного подразделения (специалистов) по защите информации должен быть достаточен для проведения мероприятий и принятия мер по защите информации в соответствии с **Требованиями** о защите информации и настоящей Политикой.

Примечание. В случае наличия у оператора структурного подразделения, на которое возложены функции по обеспечению информационной безопасности, защита информации может быть возложена на указанное подразделение (**пункт 19** Требований о защите информации).

5.6. Работники структурного подразделения (специалисты) по защите информации должны обладать компетенциями, необходимыми для выполнения возложенных на них

обязанностей (функций) по защите информации в соответствии с **Требованиями** о защите информации и настоящей Политикой.

Не менее 30 процентов работников структурного подразделения по защите информации должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

5.7. Структурное подразделение (специалисты) по защите информации должно (должны) обеспечивать защиту информации во взаимодействии с подразделениями (работниками), использующими информационные системы, и подразделениями (работниками), обеспечивающими эксплуатацию информационных систем.

5.8. Подразделения (работники), использующие информационные системы, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном оператором во внутренних стандартах и регламентах по защите информации.

Подразделения, обеспечивающие эксплуатацию информационных систем, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания информационных систем, поставки комплектующих и иных видов работ по эксплуатации информационных систем в объеме, установленном оператором во внутренних стандартах и регламентах по защите информации.

5.9. Структурным подразделением (специалистами) по защите информации должны применяться программные, программно-аппаратные средства, позволяющие обеспечить выполнение возложенных на них обязанностей (функций) по защите информации, в том числе по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, содержащейся в информационных системах, мониторингу информационной безопасности информационных систем, выявлению уязвимостей, контролю настроек и конфигураций информационных систем, а также средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

Состав программных, программно-аппаратных средств, необходимых структурному подразделению (специалистам) по защите информации для выполнения возложенных на них обязанностей (функций), определяется во внутренних стандартах и регламентах по защите информации.

5.10. Для проведения мероприятий и принятия мер по защите информации оператором могут привлекаться организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации (далее - специализированные организации).

Состав проводимых специализированными организациями мероприятий и принимаемых ими мер по защите информации, используемых при этом программных, программно-аппаратных средств, предназначенных для защиты информации, определяется оператором.

Работники структурного подразделения (специалисты) по защите информации оператора должны привлекаться к приемке результатов работ и услуг, выполняемых (оказываемых) специализированными организациями.

5.11. Оператором разработаны и утверждены:

- внутренние стандарты по защите информации, устанавливающие требования к реализации мер по защите информации применительно к особенностям деятельности оператора и функционирования информационных систем;

- внутренние регламенты по защите информации, содержащие порядок проведения мероприятий или описание реализуемых процессов по защите информации применительно к особенностям деятельности оператора и функционирования информационных систем.

Область действия внутренних стандартов и регламентов по защите информации

определена оператором.

5.12. Внутренние стандарты и регламенты по защите информации доводятся до пользователей, а также подрядных организаций в части, их касающейся.

Внутренние стандарты и регламенты по защите информации подлежат исполнению пользователями в части, их касающейся.

Обязанность подрядной организации по выполнению внутренних стандартов и регламентов по защите информации должна быть определена в документах оператора, на основании которых передается информация, предоставляется доступ к информационным системам оператора или содержащейся в них информации.

5.13. Структурное подразделение (специалисты) по защите информации должно (должны) разрабатывать и представлять руководителю оператора, ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по защите информации, с указанием сведений о целях защиты информации, на достижение которых требуются ресурсы, и перечня негативных последствий (событий), наступление которых прогнозируется в случае отсутствия ресурсов.

Руководитель оператора, ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по защите информации, привлечения при необходимости дополнительных сил и средств для защиты информации в соответствии с **Требованиями** о защите информации и настоящей Политикой на всех этапах жизненного цикла информационных систем.

5.14. Управление деятельностью по защите информации осуществляется в рамках функционирующей организационной системы управления, возглавляемой руководителем оператора или по его решению ответственным лицом.

Управление деятельностью по защите информации включает:

- разработку и планирование мероприятий и мер по защите информации;
- проведение мероприятий и принятие мер по защите информации;
- проведение оценки состояния защиты информации;
- совершенствование мероприятий и мер по защите информации.

5.15. При разработке и планировании мероприятий и мер по защите информации должны быть:

- определены события в информационных системах, наступление которых может привести к нарушению целей защиты информации, установленных в политике защиты информации;

- определены информационные системы, программные, программно-аппаратные средства, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации, установленных в политике защиты информации;

- выявлены и оценены угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению целей защиты информации, установленных в политике защиты информации (далее - угрозы безопасности информации);

- определены состав и сроки проведения мероприятий и принятия мер по защите информации и оценены необходимые для этого ресурсы.

5.16. Проводимые мероприятия и принимаемые меры по защите информации должны быть направлены на блокирование (нейтрализацию) актуальных для информационной системы угроз безопасности информации (далее - актуальные угрозы) в соответствии с целями защиты информации, определенными в настоящей Политике.

В зависимости от целей защиты информации мероприятия и меры по защите информации должны быть направлены на:

- исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

- предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации, обнаружение фактов несанкционированного доступа и реагирование на них;

- предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации и реагирование на них;

- предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены и реагирование на них;

- предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

- исключение или существенное затруднение отказа в обслуживании авторизованным пользователям информационных систем;

- недопущение использования информационных систем и содержащейся в них информации не по назначению;

- исключение или существенное затруднение нарушения функционирования (работоспособности) информационных систем;

- недопущение распространения с использованием информационных систем противоправной информации;

- обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки доступа авторизованных пользователей к информационным системам и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

- обеспечение возможности восстановления в установленные оператором (обладателем информации) сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

5.17. Оценка состояния защиты информации проводится на основе определения оператором:

- показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее - показатель защищенности К зи);

- показателя, который определяет достаточность и эффективность проведения мероприятий по защите информации (далее - показатель уровня зрелости П зи).

Для определения значений и расчета показателя защищенности К зи и показателя уровня зрелости П зи применяются методические документы, утвержденные ФСТЭК России (далее - методические документы ФСТЭК России).

5.18. Расчет и оценка показателя защищенности К зи проводится оператором не реже одного раза в шесть месяцев.

Расчет и оценка показателя уровня зрелости П зи проводится оператором не реже одного раза в два года.

О полученных по результатам оценки значениях показателя защищенности К зи и показателя уровня зрелости П зи в случае их несоответствия нормированным значениям, указанным в методических документах ФСТЭК России, в течение 3 календарных дней со дня завершения такой оценки информируется руководитель оператора для принятия решения о проведении мероприятий по совершенствованию защиты информации и принятии мер по повышению уровня защищенности информации, содержащейся в информационных системах.

Результаты оценки показателя защищенности К зи и показателя уровня зрелости П зи в срок не позднее 5 рабочих дней после дня их расчета направляются оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации и оценки эффективности деятельности по технической защите информации.

5.19. По решению руководителя оператора, ответственного лица структурным подразделением (специалистами) по защите информации с участием подразделений

(работников), использующих информационные системы, подразделений (работников), обеспечивающих эксплуатацию информационных систем, разрабатывается план мероприятий по совершенствованию защиты информации, содержащейся в информационных системах, в котором в том числе указываются наименования мероприятий, сроки их выполнения, подразделения (работники), ответственные за реализацию каждого мероприятия.

План утверждается руководителем оператора, ответственным лицом и доводится до подразделений (работников) оператора в части, их касающейся.

Результатом реализации мероприятий плана должно быть достижение значений показателя защищенности К зи и показателя уровня зрелости П зи не ниже нормированных значений, указанных в методических документах ФСТЭК России.

6. Мероприятия и меры по защите информации

6.1. Для достижения целей защиты информации оператором проводятся следующие мероприятия:

- выявление и оценка угроз безопасности информации;
- контроль конфигураций информационных систем;
- управление уязвимостями;
- управление обновлениями;
- обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;
- обеспечение защиты информации при применении конечных устройств;
- обеспечение защиты информации при применении мобильных устройств;
- обеспечение защиты информации при удаленном доступе пользователей к информационным системам;
- обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;
- обеспечение защиты информации при предоставлении пользователям доступа к информационным системам, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в информационных системах (далее - привилегированный доступ);
- обеспечение мониторинга информационной безопасности;
- обеспечение разработки безопасного программного обеспечения;
- обеспечение физической защиты информационных систем;
- обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;
- повышение уровня знаний и информированности пользователей по вопросам защиты информации;
- обеспечение защиты информации при взаимодействии с подрядными организациями;
- обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;
- обеспечение защиты информации при использовании искусственного интеллекта;
- реализация в информационных системах мер по их защите и защите содержащейся в них информации;
- проведение контроля уровня защищенности информации, содержащейся в информационных системах;
- обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

6.2. Достаточность и эффективность проводимых мероприятий (реализованных

процессов) оцениваются оператором по результатам определения показателя уровня зрелости П зи в соответствии с **пунктами 5.18** и **5.19** настоящей Политики.

6.3. Мероприятия по выявлению и оценке угроз безопасности информации предусматривают определение в ходе создания информационных систем актуальных угроз и разработку в случаях, установленных **требованиями** к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными **постановлением** Правительства Российской Федерации от 6 июля 2015 г. № 676, моделей угроз безопасности информации, а также своевременное выявление актуальных угроз и их оценку в ходе эксплуатации информационных систем.

Модель угроз безопасности информации в случае ее разработки используется в качестве исходных данных для разработки и внедрения мер по защите информации, а также для выбора средств защиты информации и их функциональных возможностей в ходе создания (развития) подсистем защиты информации информационных систем. Решение о необходимости разработки модели угроз безопасности информации в ходе создания негосударственных информационных систем принимается руководителем оператора (обладателя информации), ответственным лицом.

В ходе эксплуатации информационных систем обеспечивается поиск данных и признаков, идентифицирующих наличие актуальных угроз, проведена приоритизация выявленных угроз безопасности информации, осуществлено оповещение подразделений (работников) оператора (обладателя информации) о выявленных актуальных угрозах. При наличии признаков реализации (возникновения) актуальных угроз должны быть приняты меры по их блокированию (нейтрализации).

6.4. Мероприятия по контролю конфигураций информационных систем исключают несанкционированное изменение состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечивать обнаружение фактов несанкционированных изменений и выявление причин изменений.

Контроль конфигураций информационных систем осуществляется на основе анализа результатов учета ИТ-активов и (или) сведений, содержащихся в автоматизированных системах хранения и управления данными об информационных системах и их конфигурациях (при наличии систем инвентаризации ИТ-активов).

Структурному подразделению (специалистам) по защите информации должен быть обеспечен доступ к указанным сведениям.

6.5. Мероприятия по управлению уязвимостями включают выявление уязвимостей информационных систем, оценку их критичности, определение методов и приоритетов устранения уязвимостей, а также контроль за устранением уязвимостей.

Устранение уязвимостей, которые могут быть использованы нарушителями, или исключение возможности их использования за счет применения компенсирующих мер проводится оператором:

- в отношении уязвимостей критического уровня опасности - в срок не более 24 часов;

- в отношении уязвимостей высокого уровня опасности - в срок не более 7 календарных дней.

В отношении уязвимостей среднего и низкого уровней опасности сроки и порядок их устранения определяются во внутреннем регламенте по защите информации исходя из особенностей функционирования информационных систем.

При выявлении уязвимостей информационных систем, сведения о которых отсутствуют в банке данных угроз безопасности информации ФСТЭК России, оператор в срок не более 5 рабочих дней с даты такого выявления направляет информацию об уязвимости в ФСТЭК России для оценки необходимости включения выявленной уязвимости в банк данных угроз безопасности информации ФСТЭК России.

6.6. Мероприятия по управлению обновлениями включают проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестирования обновлений до их применения в контурах промышленной эксплуатации информационных систем, выдачу разрешения подразделениям (работникам) оператора на применение обновлений программных, программно-аппаратных средств в контурах промышленной эксплуатации информационных систем с использованием безопасных настроек и конфигураций, установленных во внутренних стандартах по защите информации.

Бесконтрольная установка обновлений программных, программно-аппаратных средств не допускается.

Сроки применения обновлений программных, программно-аппаратных средств, предназначенных для устранения уязвимостей, устанавливаются во внутреннем регламенте по защите информации в зависимости от сроков устранения уязвимостей соответствующих уровней опасности и рисков, связанных с применением обновлений программных, программно-аппаратных средств.

6.7. Мероприятия по защите информации при обработке, хранении и обращении с информацией ограниченного доступа должны исключать:

- неправомерное распространение информации ограниченного доступа вне зависимости от формы ее представления, в том числе с использованием информационно-телекоммуникационных сетей и сети "Интернет";
- доступ к информации ограниченного доступа лиц, для которых информация не предназначена и (или) для которых такой доступ запрещен.

Проводимые мероприятия включают определение информации ограниченного доступа и предназначенных для ее хранения программно-аппаратных средств, а также контроль и регистрацию всех фактов доступа пользователей к программно-аппаратным средствам, в которых хранится информация ограниченного доступа.

Контроль обработки, хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи осуществляется в соответствии с внутренним регламентом по защите информации.

О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам ее обработки и хранения незамедлительно информируется руководитель оператора, ответственное лицо.

6.8. Мероприятия по обеспечению защиты информации при применении конечных устройств информационных систем исключают возможность несанкционированного доступа к информационным системам и конечным устройствам или воздействия на них через интерфейсы и порты, непосредственно взаимодействующие с сетью "Интернет" и (или) доступные из сети "Интернет".

Защита конечных устройств информационных систем включает реализацию в них мер по защите информации от несанкционированного доступа и проведению на них мониторинга и анализа процессов и событий с целью выявления актуальных угроз, а также предупреждении о произошедших событиях безопасности.

Контроль использования конечных устройств осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.9. Посредством проведения мероприятий по обеспечению защиты информации при применении мобильных устройств исключается возможность несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними мобильным устройствам и содержащейся в них информации через каналы передачи мобильных данных, мобильные сервисы, интерфейсы и порты мобильных устройств.

При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператор принимает меры по защите информационных систем и

содержащейся в них информации, в том числе:

- обеспечивает защиту каналов передачи данных;
- осуществляет доступ пользователей с применением строгой аутентификации.

Пользователем должен быть исключен несанкционированный доступ к мобильному устройству.

6.10. Применение пользователями личных мобильных устройств для доступа к информационным системам и содержащейся в них информации с целью выполнения своих обязанностей (функций) допускается в случае соответствия мобильных устройств **Требованиям** о защите информации и наличия у оператора возможности контроля использования мобильных устройств.

6.11. Контроль использования мобильных устройств осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.12. При применении пользователями мобильных устройств для доступа к информационным системам и содержащейся в них информации, не связанного с выполнением пользователем своих обязанностей (функций), в том числе для доступа к общедоступной информации, оператором принимаются меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечивается защита каналов передачи данных, используемых для осуществления доступа.

6.13. Посредством проведения мероприятий по обеспечению защиты информации при удаленном доступе пользователей исключается возможность несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации, а также к взаимодействующим с ними программно-аппаратным средствам пользователей через каналы передачи данных, интерфейсы и порты удаленно подключаемых программно-аппаратных средств.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором принимаются меры по защите информационных систем и содержащейся в них информации, обеспечивается защита каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется удаленный доступ, исключается несанкционированный доступ к удаленно подключаемому программно-аппаратному средству пользователя.

Удаленный доступ пользователей в целях выполнения своих обязанностей (функций) осуществляется с использованием программно-аппаратных средств, выделенных оператором и соответствующих **Требованиям** о защите информации. По согласованию со структурным подразделением (специалистами) по защите информации допускается предоставление удаленного доступа к информационным системам с использованием личных программно-аппаратных средств пользователя оператора при условии применения для удаленного доступа сертифицированных средств обеспечения безопасной дистанционной работы, средств антивирусной защиты и иных средств защиты информации, исключающих угрозы безопасности информации, связанные с удаленным доступом.

Удаленный доступ пользователей к информационным системам в целях выполнения своих обязанностей (функций) осуществляется с использованием сетей связи, расположенных на территории Российской Федерации, посредством применения средств защиты канала передачи данных, и строгой аутентификации пользователей.

При удаленном доступе пользователей к информационным системам и содержащейся в них информации, не связанном с выполнением пользователями своих обязанностей (функций), в том числе при доступе к общедоступной информации, оператором принимаются меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечивается защита каналов передачи данных, используемых для осуществления удаленного доступа.

Контроль удаленного доступа пользователей к информационным системам

осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.14. Посредством проведения мероприятий по обеспечению защиты информации при беспроводном доступе пользователей к информационным системам исключается возможность несанкционированного доступа (воздействия) к информационным системам и содержащейся в них информации за счет несанкционированного подключения к точкам беспроводного доступа и доступа к беспроводным каналам передачи данных, подмены взаимодействующих с ними программно-аппаратных средств или доступа к ним.

При беспроводном доступе пользователей к информационным системам и содержащейся в них информации в целях выполнения своих обязанностей (функций) оператором принимаются меры по защите информационных систем и содержащейся в них информации, обеспечивается защита беспроводных каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется беспроводной доступ. Посредством формирования конфигурации и настроек, уровней сигналов точек беспроводного доступа, используемых для подключения пользователей к информационным системам в целях выполнения своих обязанностей (функций), исключается возможность подключения к ним лиц, не имеющих прав доступа к информационным системам. Указанные точки беспроводного доступа должны быть однозначно идентифицированы в информационных системах, а также определены места их размещения.

Точки беспроводного доступа и построенные на их основе беспроводные сети связи, используемые для доступа пользователей к информационным системам и содержащейся в них информации в целях выполнения ими своих обязанностей (функций), должны быть изолированы от беспроводных сетей связи, предназначенных для доступа к сети "Интернет" и (или) общедоступной информации оператора (обладателя информации).

6.15. Посредством проведения мероприятий по обеспечению защиты информации при предоставлении привилегированного доступа исключается возможность получения привилегированного доступа к информационным системам лицами, для которых такой доступ должен быть исключен, а также использования повышенных прав доступа с нарушением внутренних стандартов и регламентов по защите информации.

Для получения привилегированного доступа создаются привилегированные учетные записи. Привилегированные учетные записи должны иметь права доступа, минимально необходимые для выполнения пользователями возложенных на них обязанностей (функций), в соответствии с принятыми в информационных системах моделями доступа пользователей. Привилегированные учетные записи, имеющие права по созданию других привилегированных учетных записей, должны быть персонифицированными.

Привилегированный доступ осуществляется с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации - с использованием усиленной многофакторной аутентификации.

Не допускается объединение в рамках одной привилегированной учетной записи или одной группы привилегированных учетных записей ролей по системному администрированию, ролей по разработке и тестированию программных, программно-аппаратных средств, ролей администраторов безопасности.

Неиспользуемые привилегированные учетные записи должны быть заблокированы и удалены в соответствии с внутренними стандартами и регламентами по защите информации.

Встроенные привилегированные учетные записи должны быть отключены или, в случае невозможности отключения, переименованы после завершения настройки и установки конфигураций, заданных внутренними стандартами по защите информации. Аутентификационная информация встроенных привилегированных учетных записей должна быть изменена в соответствии с внутренними стандартами и регламентами по

защите информации.

Все действия по доступу пользователей с использованием привилегированных учетных записей подлежат регистрации. Контроль использования привилегированных учетных записей осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

6.16. Мероприятия по осуществлению мониторинга информационной безопасности предусматривают сбор данных о событиях безопасности, их обработке и анализе, а также выявление признаков реализации угроз безопасности информации и (или) нарушений требований внутренних стандартов и регламентов по защите информации. Мероприятия по осуществлению мониторинга информационной безопасности проводятся в отношении всех информационных систем, за исключением локальных и изолированных информационных систем, в которых должен обеспечиваться контроль журналов регистрации событий безопасности.

Мероприятия по мониторингу информационной безопасности осуществляются в соответствии с разделами 4 и 5 **ГОСТ Р 59547-2021**.

В ходе проведения мониторинга информационной безопасности для анализа зафиксированных событий безопасности и выявленных в них признаков реализации актуальных угроз допускается использование доверенных технологий искусственного интеллекта.

Структурное подразделение (специалисты) по защите информации оператора с периодичностью и в сроки, установленные внутренним регламентом по защите информации, разрабатывает и представляет руководителю оператора, ответственному лицу отчет о результатах мониторинга, который в том числе должен содержать типы событий безопасности, обнаруженные по результатам мониторинга, и связанные с ними компьютерные инциденты (при их наличии), а также рекомендации по их анализу и (или) устранению. Последний в текущем году отчет о результатах мониторинга или итоговый отчет за текущий год (в случае его разработки) после представления руководителю оператора направляется оператором в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации.

6.17. Мероприятия по разработке безопасного программного обеспечения направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом оператором программном обеспечении. Мероприятия по разработке безопасного программного обеспечения проводятся в случае осуществления оператором самостоятельной разработки программного обеспечения, применяемого в информационных системах.

В случае самостоятельной разработки оператором программного обеспечения, предназначенного для использования в информационных системах, реализуются меры, предусмотренные разделами 4 и 5 **ГОСТ Р 56939-2024**.

В случае привлечения оператором для разработки программного обеспечения подрядной организации по решению руководителя (ответственного лица) в техническое задание на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с **ГОСТ Р 56939-2024**.

6.18. Посредством проведения мероприятий по обеспечению физической защиты информационных систем исключается возможность несанкционированного физического доступа к программно-аппаратным средствам обработки и хранения информации.

Физический доступ к программно-аппаратным средствам информационных систем, предназначенным для обработки и хранения информации, предоставляется пользователям, которым указанный доступ необходим для выполнения возложенных на них обязанностей (функций). Программно-аппаратные средства информационных систем, предназначенные для хранения информации, должны быть установлены в помещениях (зонах помещений, шкафах, футлярах, корпусах), несанкционированный физический доступ в которые должен быть исключен.

Контроль физического доступа к программно-аппаратным средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений, шкафы, футляры, корпуса), в которых они установлены, осуществляется в соответствии с внутренними регламентами по защите информации.

Съемные машинные носители информации, разрешенные для использования в информационных системах, подлежат учету и контролю использования. В информационных системах должны использоваться съемные машинные носители информации, выдаваемые оператором. В случае обнаружения пользователем съемного машинного носителя информации, принадлежность которого или владельца которого установить не удалось, такой съемный машинный носитель информации должен быть передан в структурное подразделение (специалистам) по защите информации для анализа содержащейся на нем информации, программ и при необходимости дальнейшего уничтожения. Подключение обнаруженного съемного машинного носителя информации к информационным системам запрещается.

6.19. Посредством проведения мероприятий по обеспечению непрерывности функционирования информационных систем при возникновении нештатных ситуаций обеспечивается возможность восстановления выполнения функций (процессов, видов работ) информационных систем, для которых оператором установлены требования к непрерывному режиму функционирования (далее - значимые функции), в пределах интервалов времени восстановления, установленных внутренними стандартами и регламентами по защите информации.

6.20. Интервалы времени восстановления функционирования информационных систем, их сегментов, выполняющих значимые функции, устанавливаются оператором в соответствии с актами, на основании которых осуществляется создание, эксплуатация информационных систем, или требованиями обладателя информации в зависимости от значимости функций для обеспечения его деятельности, классов защищенности информационных систем, устанавливаемых оператором в соответствии с **приложением** к Требованиям о защите информации, и должны составлять:

- для информационных систем 1 класса защищенности - не более 24 часов с момента обнаружения нарушения функционирования;

- для информационных систем 2 класса защищенности - не более 7 календарных дней с момента обнаружения нарушения функционирования;

- для информационных систем 3 класса защищенности - не более 4 недель с момента обнаружения нарушения функционирования.

6.21. Программные, программно-аппаратные средства, позволяющие обеспечить выполнение значимых функций, должны быть развернуты в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный оператором во внутренних стандартах и регламентах по защите информации интервал времени восстановления.

6.22. Оператором обеспечивается:

- создание достаточного количества резервных копий программных, программно-аппаратных средств и их конфигураций, обеспечивающих выполнение значимых функций, необходимых для восстановления выполнения значимых функций в установленный во внутренних стандартах и регламентах по защите информации интервал времени восстановления, и периодическое тестирование таких средств на работоспособность;

- создание достаточного количества резервных копий информации, необходимой для обеспечения выполнения значимых функций, а также их хранение на разных типах машинных носителей информации в местах, обеспечивающих исключение несанкционированного доступа к резервным копиям информации.

Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации

определяются во внутренних стандартах и регламентах по защите информации.

Оператор проводит периодические, но не реже одного раза в два года, проверки, в том числе в форме тренировок, возможности восстановления выполнения значимых функций с использованием резервных копий программных, программно-аппаратных средств и информации, необходимой для их выполнения, с привлечением работников, задействованных в проведении работ по восстановлению функционирования информационных систем.

В случае проведения мероприятий по восстановлению функционирования информационных систем, их сегментов, выполняющих значимые функции, с превышением интервалов времени их восстановления должна обеспечиваться возможность выполнения пользователями значимых функций, в том числе в неавтоматизированном режиме, в соответствии с внутренними регламентами по защите информации.

6.23. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации включают:

- доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;
- проведение лекций, семинаров, обучающих игр по вопросам защиты информации;
- проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;
- проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

6.24. Применяемые оператором способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний определяются во внутренних регламентах по защите информации. Оценка уровня знаний проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора. Для пользователей, у которых отсутствуют знания по вопросам защиты информации, организуется повторное прохождение обучающих курсов по вопросам защиты информации.

6.25. Посредством проведения мероприятий по защите информации при взаимодействии оператора с подрядными организациями исключается возможность несанкционированного доступа или воздействий на информационные системы и содержащуюся в них информацию через взаимодействующие с информационными системами программно-аппаратные средства подрядных организаций или каналы передачи данных и интерфейсы, используемые для доступа подрядных организаций к информационным системам.

Оператором в отношении подрядной организации устанавливаются требования по обеспечению защиты информации, к которой получен доступ.

Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в документах оператора, на основании которых подрядным организациям предоставлен доступ к информационным системам.

В информационных системах, отдельных программно-аппаратных средствах подрядных организаций, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации. Состав информации, цели ее защиты и классы защищенности, в соответствии с которыми подрядными организациями должны быть приняты меры по защите информации во взаимодействующих информационных системах, устанавливаются оператором во внутренних стандартах и регламентах по защите информации.

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в эксплуатируемых информационных системах оператора

не допускается. Для проведения работ по разработке (развитию) и (или) тестированию программного обеспечения работникам подрядных организаций предоставляется доступ к выделенным для проведения таких работ стендам разработки и (или) тестирования, которые должны быть изолированы от эксплуатируемых информационных систем оператора. Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования осуществляется в соответствии с внутренними регламентами по защите информации.

6.26. Посредством проведения мероприятий по организации и проведению защиты от компьютерных атак, направленных на отказ в обслуживании, исключается возможность блокирования авторизованным пользователям доступа к информационным системам и (или) содержащейся в них информации вследствие несанкционированных воздействий на интерфейсы, порты, сервисы, к которым должен быть обеспечен постоянный доступ из сети "Интернет".

Оператором обеспечивается взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также взаимодействие в автоматизированном режиме с Центром мониторинга и управления сетью связи общего пользования.

Мероприятия, предусмотренные настоящим пунктом, осуществляются с привлечением провайдеров хостинга или организаций, предоставляющих услуги связи, или организаций, оказывающих услуги по контролю, фильтрации и блокированию сетевых запросов, обладающих признаками компьютерных атак, направленных на отказ в обслуживании. Программно-аппаратные средства, используемые для контроля, фильтрации и блокирования сетевых запросов, обладающих признаками атак, направленных на отказ в обслуживании, должны быть расположены на территории Российской Федерации.

Обеспечение доступности из сети "Интернет" интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, осуществляется в соответствии с внутренними регламентами по защите информации по согласованию со структурным подразделением (специалистами) по защите информации после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с перечнем ресурсов сети "Интернет", с которыми может взаимодействовать информационная система, включающим исходящий и входящий сетевые потоки, их характеристики и используемые протоколы.

6.27. Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта обеспечивается возможность исключения несанкционированного доступа к информации или воздействия на информационные системы, несанкционированного распространения и модификации информации, а также использования информационных систем не по их назначению за счет воздействия на наборы данных, применяемые модели искусственного интеллекта и их параметры, процессы и сервисы по обработке данных и поиску решений.

Не допускается передача лицу, разработавшему модель искусственного интеллекта, информации ограниченного доступа, содержащейся в информационных системах, в том числе для улучшения функционирования модели искусственного интеллекта.

6.28. При взаимодействии пользователей в целях выполнения ими своих обязанностей (функций) с сервисами на основе искусственного интеллекта посредством направления запроса и получения ответа должны быть:

- при взаимодействии в формате строго заданных шаблонов запросов и ответов:

определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам;

определены шаблоны ответов искусственного интеллекта и обеспечен контроль

соответствия ответов установленным оператором шаблонам;

- при взаимодействии в формате свободной текстовой формы запросов и ответов:

определены для направляемых в искусственный интеллект запросов пользователей допустимые тематики и обеспечен контроль соответствия запросов допустимым тематикам;

определены форматы ответов искусственного интеллекта в соответствии с допустимыми тематиками и обеспечен контроль соответствия ответов установленным оператором форматам и допустимым тематикам;

- разработаны статистические критерии для выявления недостоверных ответов искусственного интеллекта для последующего сбора и анализа недостоверных ответов;

- обеспечено реагирование на недостоверные ответы искусственного интеллекта посредством ограничения области принимаемых решений и (или) реализации функций информационной системы на основе недостоверных ответов искусственного интеллекта.

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование информационных систем.

Непосредственно в состав информационных систем должны включаться доверенные технологии искусственного интеллекта или их компоненты.

6.29. Мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации включают:

- реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором;

- адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

- верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

6.30. В информационных системах реализованы следующие базовые меры защиты информационных систем и содержащейся в них информации:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- защита виртуализации и облачных вычислений;
- защита технологий контейнерных сред и их оркестрации;
- защита сервисов электронной почты;
- защита веб-технологий;
- защита программных интерфейсов взаимодействия приложений;
- защита конечных устройств;
- защита мобильных устройств;
- защита технологий интернета вещей;
- защита точек беспроводного доступа;
- антивирусная защита;
- обнаружение и предотвращение вторжений на сетевом уровне;
- сегментация и межсетевое экранирование;
- защита от компьютерных атак, направленных на отказ в обслуживании;
- защита каналов передачи данных и сетевого взаимодействия.

6.31. Реализация мер по защите информационных систем и содержащейся в них информации, подлежащие реализации, обеспечивает защиту от нарушителей со следующими уровнями возможностей:

- в информационных системах 3 класса защищенности - от нарушителей с базовым уровнем возможностей;

- в информационных системах 2 класса защищенности - от нарушителей с повышенным уровнем возможностей;

- в информационных системах 1 класса защищенности - от нарушителей с высоким уровнем возможностей.

Оператором может быть принято решение о применении мер защиты информационных систем и содержащейся в них информации от нарушителей с более высоким уровнем возможностей.

6.32. С целью подтверждения достаточности принятых мер защиты информационных систем и содержащейся в них информации до начала обработки и (или) хранения информации в информационных системах может быть проведена их аттестация на соответствие **Требованиям** о защите информации.

Решение о необходимости аттестации информационных систем принимается руководителем оператора, ответственным лицом.

6.33. Мероприятия по контролю уровня защищенности информации, содержащейся в информационных системах, обеспечивают включение проведения оценки возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями.

Контроль уровня защищенности информации проводится в соответствии с внутренними регламентами по защите информации одним или совокупностью следующих методов:

- автоматизированное и (или) ручное выявление уязвимостей информационных систем с последующей экспертной оценкой возможности их использования нарушителем для нарушения безопасности информации и (или) нарушения функционирования информационных систем;

- выявление несанкционированных подключений устройств к информационным системам;

- тестирование информационных систем путем моделирования реализации актуальных угроз с целью оценки возможностей несанкционированного доступа к ним (воздействий на них) или повышения привилегий при реализованных мероприятиях и мерах по защите информационных систем и содержащейся в них информации;

- проведение в соответствии с планом тренировок по отработке работниками оператора действий по обеспечению уровня защищенности информации, содержащейся в информационных системах, в условиях реализации актуальных угроз.

6.34. Контроль уровня защищенности информации проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора. Методы контроля уровня защищенности информации и периодичность его проведения определяются оператором во внутреннем регламенте.

По результатам проведения контроля уровня защищенности информации разрабатывается отчет, который подписывается лицами, проводившими контроль. Отчет должен быть представлен в течение 3 рабочих дней с даты завершения контроля уровня защищенности информации руководителю оператора, ответственному лицу для принятия при необходимости решения руководителя оператора о выделении ресурсов с целью повышения уровня защищенности информации. Отчет направляется оператором в ФСТЭК России в течение 5 рабочих дней с даты завершения контроля уровня защищенности информации в целях мониторинга текущего состояния технической защиты информации.

6.35. Мероприятия и меры по защите информации, предусмотренные **Требованиями** о защите информации и настоящей Политикой, реализуются оператором с использованием методических документов ФСТЭК России.

6.36. При отсутствии возможности реализации отдельных мероприятий и (или) принятия мер по защите информации оператором разрабатываются и внедряются

компенсирующие меры, позволяющие обеспечить блокирование (нейтрализацию) актуальных угроз. При этом оператором должно быть обосновано применение компенсирующих мер на этапе создания информационных систем, а при аттестации информационных систем - подтверждена их эффективность для блокирования (нейтрализации) актуальных угроз.

6.37. Технические меры по защите информации принимаются на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре при ее наличии. На аппаратном и системном уровнях защита информации обеспечивается посредством применения встроенных в аппаратное обеспечение и системное программное обеспечение средств защиты информации. На прикладном и сетевом (инфраструктурном) уровнях защита информации обеспечивается применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.

6.38. Для защиты информации применяются сертифицированные средства защиты информации в соответствии с инструкциями (правилами) по их эксплуатации, установленными разработчиками в эксплуатационной документации. Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

Средства защиты информации применяются с соблюдением запретов, установленных **пунктом 6** Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

6.39. Применяемые сертифицированные средства защиты информации должны соответствовать:

- для защиты информационных систем 1 класса защищенности - не ниже чем 4 классу защиты и уровню доверия;
- для защиты информационных систем 2 класса защищенности - не ниже чем 5 классу защиты и уровню доверия;
- для защиты информационных систем 3 класса защищенности - 6 классу защиты и уровню доверия.

6.40. На стадиях жизненного цикла информационных систем меры по защите информации принимаются оператором в соответствии с разделом 5 национального стандарта Российской Федерации **ГОСТ Р 51583-2014** "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования", утвержденного и введенного в действие **приказом** Росстандарта от 28 января 2014 г. № 3-ст.

7. Обработка информации, содержащей персональные данные

7.1. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с **частью 5 статьи 19** Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных).

7.2. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

7.3. Оператор обеспечивает безопасность персональных данных при их обработке в информационной системе.

7.4. Оператор осуществляет выбор средств защиты информации для системы защиты персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

7.5. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

7.6. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда.

7.7. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

7.8. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.9. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.10. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.11. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

7.12. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

7.13. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных **пунктом 7.12** настоящей Политики, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

7.14. Для обеспечения 2-го уровня защищенности персональных данных при их

обработке в информационных системах помимо выполнения требований, предусмотренных **пунктом 7.13** настоящей Политики, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

7.15. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных **пунктом 7.14** настоящей Политики, необходимо выполнение следующих требований:

- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;
- создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

7.16. Контроль за выполнением указанных в настоящем разделе требований организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором.

8. Ответственность

8.1. Нарушение требований **Закона** об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение №3
к приказу руководителя
МКУ «ЦБ ДСП» от 22.06.2026
№ 06-01-01

Концепция информационной безопасности информационных систем персональных данных в муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения»

Введение

Настоящая Концепция информационной безопасности ИСПДн учреждения разработана Муниципальным казенным учреждением «Централизованная бухгалтерия Динского сельского поселения», является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности Учреждения.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Учреждениях, при обработке информации вообще, и персональных данных в частности.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждений, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Учреждения;

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

5.12 Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

5.13 Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Учреждения.

5.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

6 Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

6.1 Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

6.3 Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн,

деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Учреждения в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а так же их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

В организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;
- порядок допуска сотрудников к использованию ресурсов ИСПДн Учреждения;
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
- инструкций пользователей ИСПДн (администратора ИСПДн, администратора

безопасности, оператора ИСПДн);

- инструкция пользователя при возникновении внештатных ситуаций.

6.4 Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5 Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Учреждения;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн Учреждения разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами Учреждения осуществляется непрерывное управление и административная

поддержка функционирования средств защиты.

7 Контроль эффективности системы защиты ИСПДн Учреждения

Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

8 Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель Учреждения. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

- Планирование и реализация мер по обеспечению безопасности ПДн;
- Анализ угроз безопасности ПДн;
- Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- Контроль защищенности ИТ инфраструктуры Компании от угроз ИБ путем;
- Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организациями должно быть заключено "Соглашение о конфиденциальности", либо "Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн". Подготовка типовых вариантов этих соглашений осуществляется совместно с Юридическим отделом.

9 Модель нарушителя безопасности

Под нарушителем в Учреждении понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10 Модель угроз безопасности

Для ИСПДн Учреждения выделяются следующие основные категории угроз безопасности персональных данных:

1) Угрозы от утечки по техническим каналам.

2) Угрозы несанкционированного доступа к информации:

- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

- Угрозы преднамеренных действий внутренних нарушителей.

- Угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

11 Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;

- постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСТЭК России;

- потребностей ИСПДн в средствах обеспечения безопасности информации.

12 Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к

ИСПДн;

- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

13 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1. **Федеральный закон** от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - ФЗ "О персональных данных"), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. "**Положение** об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденное **Постановлением** Правительства РФ от 17.11.2007 г. N 781.
3. **Постановление** Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
4. "**Положение** об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденное **Постановлением** Правительства РФ от 15.09.2008 г. N 687.
5. "**Требования** к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", утвержденные **Постановлением** Правительства РФ от 06.07.2008 г. N 512.

Приложение №4
к приказу руководителя
МКУ «ЦБ ДСП» от 22.06.2026
№ 06-01-01

Перечень
персональных данных, подлежащих защите в информационных системах персональных данных в муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения»

Введение

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных (ИСПДн) (далее - Перечень) в муниципальном казенном учреждении «Централизованная бухгалтерия Динского сельского поселения» (далее – Учреждения).

Перечень разработан в соответствии со списком объектов защиты, изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

1 Общие положения

Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень объектов защиты определен по результатам Отчета о результатах проведения внутренней проверки.

Объекты защиты каждой ИСПДн включают:

1) Обрабатываемая информация:
- персональные данные субъектов ПДн (раздел 2.1);
- персональные данные сотрудников (**раздел** 2.1.1);
2) Технологическая информация (**раздел 2.2**).
3) Программно-технические средства обработки (**раздел 2.3**).
4) Средства защиты ПДн (**раздел 2.4**).
5) Каналы информационного обмена и телекоммуникации (**раздел 2.5**).
6) Объекты и помещения, в которых размещены компоненты ИСПДн (**раздел 2.6**).

2. Обрабатываемая информация

2.1 Перечень персональных данных субъектов ПДн

Персональные данные субъектов ПДн включают:

- ФИО;
- Дата рождения;
- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;
- Паспортные данные;

2.1.1 Перечень персональных данных сотрудников Учреждения

Персональные данные сотрудников Учреждения включают:
- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (N трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, N и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;

2.2 Технологическая информация

Технологическая информация, подлежащая защите, включает:
- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная

информация, ключи и атрибуты доступа и др.);

- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

2.3 Программно-технические средства обработки

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4 Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

2.5 Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6 Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

Приложение №5
к приказу руководителя
МКУ «ЦБ ДСП» от 22.06.2026
№ 06-01-01

Модель угроз безопасности информации

1. Общие положения

1.1. Модель угроз безопасности информации **сервера 1С** (далее - Модель угроз безопасности информации) разработана в целях реализации Муниципальным казенным учреждением «Централизованная бухгалтерия Динского сельского поселения» требований Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Методического документа "Методика оценки угроз безопасности информации", утвержденного Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.

1.2. Модель угроз безопасности информации применяется в **сервере 1С** для решения следующих задач:

- определения требуемого уровня защищенности персональных данных;
- разработки системы защиты персональных данных;
- выбора технических и организационных мер по обеспечению безопасности персональных данных;
- проведения мероприятий по предотвращению несанкционированного доступа к персональным данным;

1.3. Муниципальным казенным учреждением «Централизованная бухгалтерия Динского сельского поселения» использует для оценки угроз безопасности информации Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановление правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Методического документа "Методика оценки угроз безопасности информации", утвержденного Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.

1.4. Ответственными за обеспечение защиты информации в Муниципальным казенным учреждением «Централизованная бухгалтерия Динского сельского поселения» назначается: главный специалист Виноградов В.А.

1.5. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

1.6. Изменение модели угроз безопасности информации осуществляется в случаях:

- изменения требований нормативных правовых актов Российской Федерации, методических документов Федеральной службе по техническому и экспортному контролю (далее - ФСТЭК) России, регламентирующих вопросы оценки угроз безопасности информации;
- изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;

- выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;

- включения в банк данных угроз безопасности информации ФСТЭК России сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

2. Описание систем и сетей и их характеристика как объектов защиты

2.1. Модель угроз безопасности разработана для **сервера 1С**.

2.2. Модель угроз безопасности персональных данных при их обработке в ИСПДн строится на основании Отчета о результатах проведения внутренней проверки в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

2.3. Сервер 1С используются в целях ведения бухгалтерского учета.

Муниципальным казенным учреждением «Централизованная бухгалтерия Динского сельского поселения» обрабатывается следующая информация:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (N трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, N и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;

2.6. На сервере 1С существует 10 учетных записей пользователей с разграниченными правами доступа

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

3.1. К негативным последствиям, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба), относятся: нарушение законодательства РФ;

потеря или хищение денежных средств;

утечка конфиденциальной информации;

несанкционированный доступ к компонентам системы и данным;

нарушение функционирования программно-аппаратных средств обработки, передачи и хранения информации;

несанкционированное использование вычислительных ресурсов систем и сетей для решения несвойственных им задач;

4. Классификация угроз безопасности персональных данных

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.);

средства защиты информации;

вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее – служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн (рисунок 1) являются:

источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;

среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

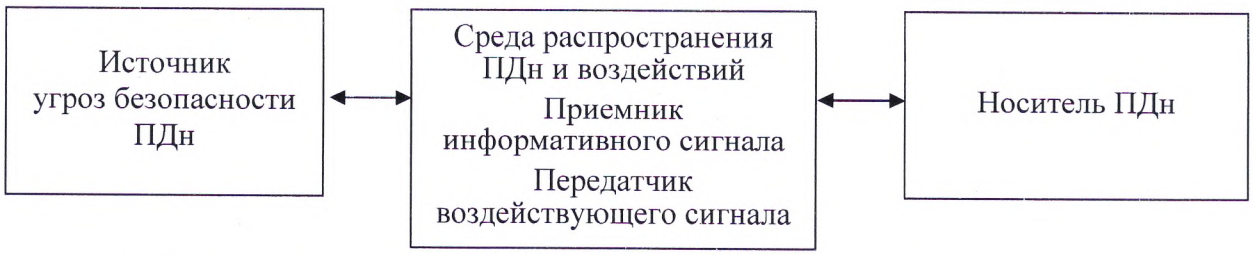


Рисунок 1. Обобщенная схема канала реализации угроз безопасности персональных данных

Носители ПДн могут содержать информацию, представленную в следующих видах:

акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

видовая информация (ВИ), представленная в виде текста и изображений различных

устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками (рисунок 2):

по виду защищаемой от УБПДн информации, содержащей ПДн;

по видам возможных источников УБПДн;

по типу ИСПДн, на которые направлена реализация УБПДн;

по способу реализации УБПДн;

по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

по используемой уязвимости;

по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей
ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

Классификация угроз безопасности персональных данных

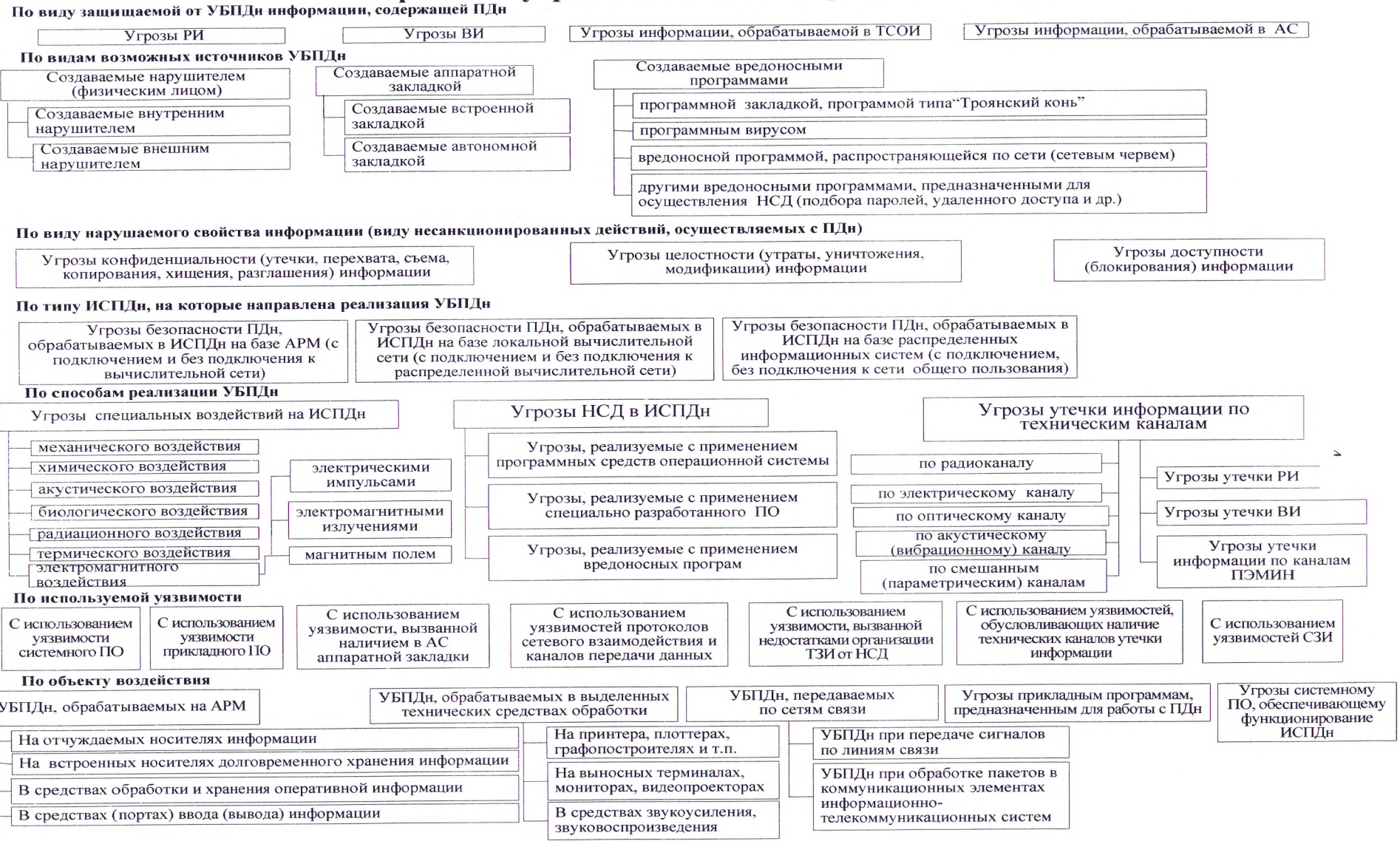


Рисунок 2. Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);

угрозы утечки ПДн по техническим каналам утечки информации;

угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

угрозы, реализуемые с использованием уязвимости системного ПО;

угрозы, реализуемые с использованием уязвимости прикладного ПО;

угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых на АРМ;

угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

угрозы безопасности ПДн, передаваемых по сетям связи;

угрозы прикладным программам, с помощью которых обрабатываются ПДн;

угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для
субъектов ПДн:

значительным негативным последствиям для субъектов ПДн;

негативным последствиям для субъектов ПДн;

незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД) (далее – угрозы НСД в ИСПДн), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов

реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

5. Угрозы утечки информации по техническим каналам

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

угроз утечки акустической (речевой) информации;

угроз утечки видовой информации;

угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

6. Угрозы несанкционированного доступа к информации в информационной системе персональных данных

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и

т.п.;

угрозы внедрения вредоносных программ (программно-математического воздействия).

Состав элементов описания угроз НСД к информации в ИСПДн приведен на рисунке 3.

Кроме этого, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду компьютера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств – это угрозы «Отказа в обслуживании». Как правило, данные угрозы рассматриваются применительно к ИСПДн на базе локальных и распределенных информационных систем вне зависимости от подключения

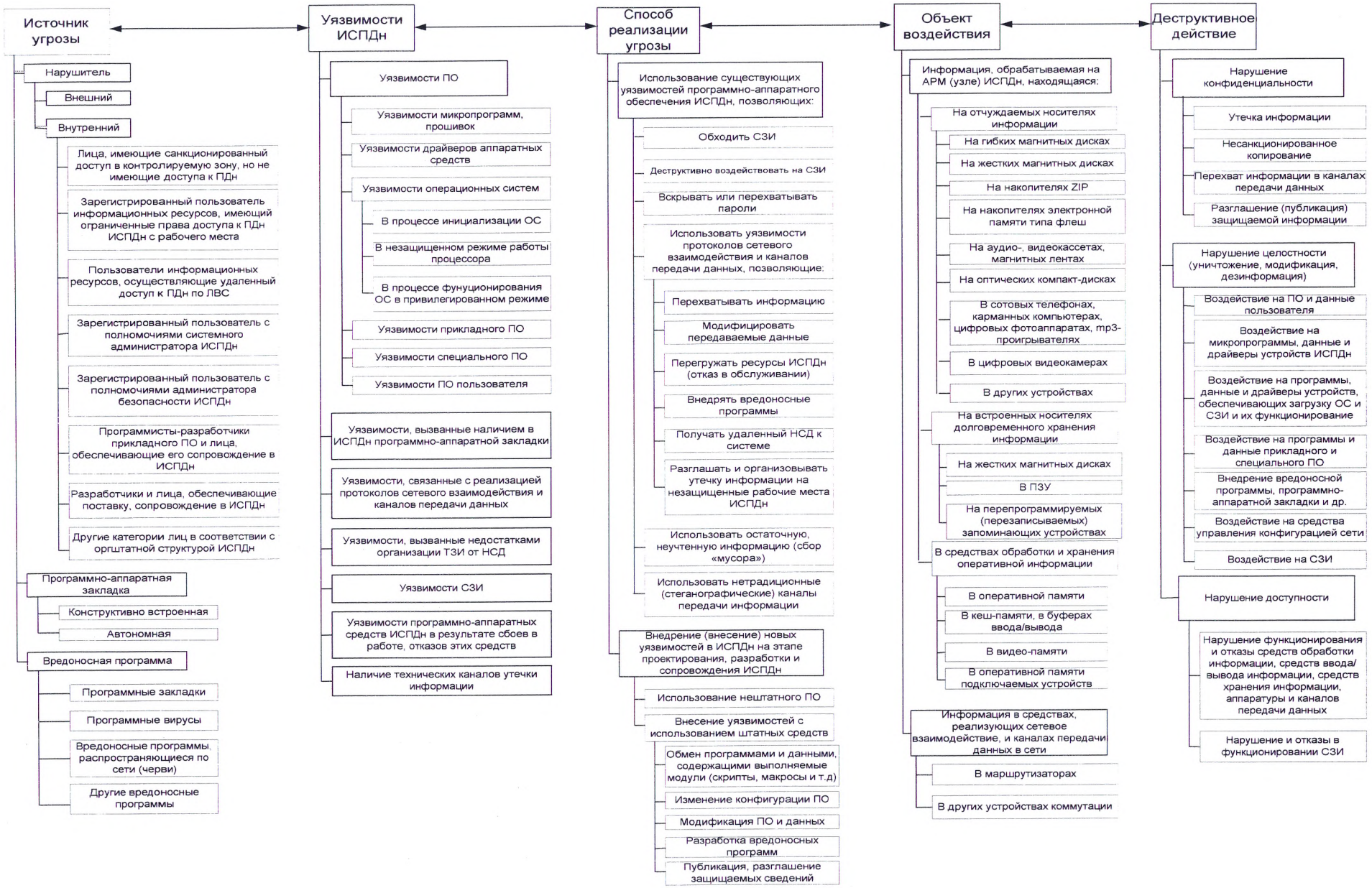


Рисунок 3. Элементы описания угроз НСД к информации в ИСПДн

информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

содержания служебной информации в пакетах сообщений, передаваемых по сети;

условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);

форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

программного обеспечения обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др. Описание таких угроз формально может быть представлено следующим образом:

угроза «Отказа в обслуживании»: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, «зацикливание» обработки и т.п.)>.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что,
во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации
на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования). В связи с этим угрозы программно-математического воздействия (ПМВ) формально могут быть представлены следующим образом:

угроза ПМВ в ИСПДн: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор,
файл и т.п.)>, <описание возможных деструктивных действий>,<дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Ниже дается общая характеристика источников угроз безопасности информации, уязвимостей, которые могут быть использованы при реализации угроз НСД, и характеристика результатов несанкционированного или случайного доступа. Характеристика способов реализации угроз дается
при описании угроз доступа (проникновения) в операционную среду компьютера, угроз отказа в обслуживании и угроз ПМВ.

7. Общая характеристика источников угроз несанкционированного доступа в информационной системе персональных данных

Источниками угроз НСД в ИСПДн могут быть:

нарушитель;

носитель вредоносной программы;

аппаратная закладка.

Угрозы безопасности ПДн, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) ИСПДн нарушители подразделяются на два типа:

нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;

нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, – внутренние нарушители.

Внешними нарушителями могут быть:

разведывательные службы государств;

криминальные структуры;

конкуренты (конкурирующие организации);

недобросовестные партнеры;

внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

осуществлять несанкционированный доступ к информации
с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят
от действующих в пределах контролируемой зоны режимных
и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости

от способа доступа и полномочий доступа к ПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории, может:

иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;

располагать именами и вести выявление паролей зарегистрированных пользователей;

изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн
с рабочего места.

Лицо этой категории:

обладает всеми возможностями лиц первой категории;

знает, по меньшей мере, одно легальное имя доступа;

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лицо этой категории:

обладает всеми возможностями лиц первой и второй категорий;

располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;

имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;

обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;

имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

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

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации УБПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной

программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;

встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

пакеты передаваемых по компьютерной сети сообщений;

файлы (текстовые, графические, исполняемые и т.д.).

8. Общая характеристика уязвимостей информационной системы персональных данных

Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

9. Источники угроз безопасности информации

9.1. Источники угроз безопасности информации делятся на антропогенные и технологические источники

Антропогенные источники исходят от людей и включают как случайные ошибки, так и

умышленные действия.

К случайным ошибкам относятся:

непреднамеренные действия сотрудников (ошибки при работе с данными, случайное удаление файлов);

использование слабых или повторно используемых паролей;

потеря или кража физических носителей информации (ноутбуков, флешек, смартфонов) без должного уровня защиты (отсутствие шифрования, блокировки экрана);

несоблюдение правил безопасности (например, не выход из учётной записи, что позволяет несанкционированный доступ к компьютеру другим лицам).

К умышленным действиям относятся:

Кража данных. Сознательное копирование, передача или использование конфиденциальной информации (финансовых данных, клиентской базы, интеллектуальной собственности) в личных целях или для продажи конкурентам.

Саботаж. Намеренное нанесение ущерба: уничтожение данных, нарушение работы систем, внедрение вредоносного ПО.

Мошенничество. Манипуляции с данными для сокрытия ошибок или получения личной выгоды (например, искажение финансовых отчётов).

Технологические источники угрозы связаны с недостатками в работе оборудования, программного обеспечения и сетевых коммуникаций к ним относятся:

Уязвимости в программном обеспечении и аппаратной части. Устаревшие версии ПО или не обновляемая «прошивка» часто содержат бреши, которые злоумышленники могут эксплуатировать.

Ошибки в конфигурации систем. Некорректные настройки сетевых экранов, баз данных, сервисов создают «ворота» для атак.

Сбои и отказы оборудования. Поломка серверов, жёстких дисков, каналов связи может привести к потере данных или простою.

Отсутствие или неэффективность резервного копирования. Повышает риск безвозвратной

Угрозы в облачных вычислениях. Виртуальные хранилища не гарантируют полную безопасность, если не приняты соответствующие меры.

10. Актуальные угрозы безопасности информации

1. Атаки с использованием искусственного интеллекта (ИИ). ИИ становится мощным инструментом в руках атакующих. С его помощью автоматизируют массовые рассылки фишинговых писем, создают дипфейки, проводят глубокий OSINT-анализ для персонализации атак. Также существует риск компрометации знаний, на которых обучаются ИИ-ассистенты и чат-боты.

2. Целевые атаки (APT — Advanced Persistent Threats). Это сложные, многоэтапные атаки, которые злоумышленники тщательно планируют. Их цель — незаметно проникнуть в инфраструктуру, закрепиться в ней и получить доступ к конфиденциальным данным или внутренним ресурсам. В 2026 году отмечается рост доли таких атак, особенно на промышленные предприятия.

3. Атаки на цепочки поставок (supply chain attacks). Злоумышленники атакуют не саму организацию напрямую, а её доверенных поставщиков услуг: облачных провайдеров, интеграторов, сервисных компаний. Компрометация одного звена может привести к масштабному инциденту для всей организации.

4. Фишинг и социальная инженерия. Злоумышленники рассылают поддельные письма, создают сайты-клоны, звонят от имени «службы безопасности», чтобы обманом заставить жертву раскрыть логины, пароли, данные банковских карт или другую конфиденциальную информацию.

Социальная инженерия остаётся одним из самых эффективных способов получения доступа к системам.

5. Вредоносное программное обеспечение (ВПО). В арсенале атакующих — шифровальщики (программы-вымогатели), стилеры (для кражи учётных данных), трояны удалённого доступа (RAT), загрузчики и ПО для майнинга. В 2026 году эксперты отмечают смещение акцента с простого шифрования данных на их кражу с последующим шантажом.

6. DDoS-атаки. Эти атаки направлены на нарушение доступности сервисов путём перегрузки системы большим объёмом запросов. Хотя их доля в общем числе инцидентов может снижаться, они по-прежнему способны парализовать работу критически важных систем.

7. Утечки данных. Неконтролируемое распространение конфиденциальной информации (персональных данных, коммерческой тайны, интеллектуальной собственности) в результате взломов, ошибок сотрудников или потери носителей.

8. Уязвимости в ПО и конфигурации систем. Эксплуатация уязвимостей «нулевого дня» (ранее неизвестных) и недостатков в настройке сетевого оборудования, прав доступа, использовании паролей по умолчанию.

9. Инсайдерские угрозы. Риски, связанные с действиями сотрудников: от случайных ошибок (например, отправка данных на личную флешку) до умышленных действий (кража данных, саботаж).