Р О С С И Й С К А Я Ф Е Д Е Р А Ц И Я
Б Е Л Г О Р О Д С К А Я О Б Л А С Т Ь
МУНИЦИПАЛЬНЫЙ РАЙОН «ВЕЙДЕЛЕВСКИЙ РАЙОН»

АДМИНИСТРАЦИЯ
КЛИМЕНКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

П О С Т А Н О В Л Е Н И Е
с. Клименки

27 марта 2024 года № 14

Об утверждении Положения о политике информационной безопасности администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области

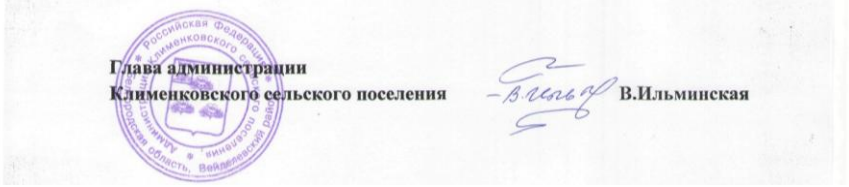
В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации», в целях обеспечения информационной безопасности администрации Клименковского сельского поселения, постановляю:

1. Утвердить прилагаемое Положение о политике информационной безопасности администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области.

2. В месячный срок после вступления в силу настоящего постановления создать комиссию по расследованию и реагированию на инцидент информационной безопасности.

3. Обнародовать настоящее постановление в установленном порядке и разместить на официальном сайте органов местного самоуправления Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области **(**https://klimenkovskoe-r31.gosweb.gosuslugi.ru/**)** в информационно-телекоммуникационной сети «Интернет».

4. Контроль за исполнением настоящего постановления оставляю за собой.



УТВЕРЖДЕНО
постановлением администрации
Клименковского сельского поселения
муниципального района «Вейделевский район»
Белгородской области
от 27 марта 2024 г. № 14

ПОЛОЖЕНИЕ
о политике информационной безопасности администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области

1. Общие положения

1.1. Положение о политике информационной безопасности администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области (далее – Положение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется администрация Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области (далее – администрация поселения) в своей деятельности.

1.2. Основными целями политики информационной безопасности администрации поселения (далее – политика) являются защита информации и обеспечение эффективной работы всей информационно-вычислительной системы администрации поселения.

1.3. Общее руководство обеспечением информационной безопасности администрации поселения осуществляет глава администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области.

1.4. Расследование инцидентов информационной безопасности осуществляет комиссия по расследованию и реагированию на инцидент информационной безопасности, создаваемая постановлением администрации поселения.

1.5. Сотрудники администрации поселения обязаны соблюдать порядок обращения с документами, содержащими защищаемую информацию, ключевыми носителями, следовать требованиям настоящей информационной политики и иных документов, регламентирующих деятельность в области информационной безопасности.

1.6. Настоящее Положение распространяется на всех сотрудников администрации поселения.

2. Основные понятия

2.1. В настоящем Положении используются следующие основные понятия:

- **автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

- **администратор безопасности** – лицо или группа лиц, ответственных за обеспечение безопасности системы, реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты;

- **вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию конфиденциального характера или ресурсы информационной системы;

- **доступ к информации** – возможность получения информации и ее использования;

- **защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

- **информационная система (ИС)** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- **использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- **источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

- **нарушитель** – лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства;

- **несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами;

- **носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов,

количественных характеристик физических величин;

- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

- **организационные меры защиты** – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации;

- **перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

- **персональные данные** – любая информация, относящаяся прямо или косвенно к определенному физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- **пользователь информационной системы** – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования;

- **правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

- **предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- **средства вычислительной техники** – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем;

- **субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа;

- **утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

- **уязвимость** – слабые места в средствах защиты, которые можно использовать для нарушения системы или содержащейся в ней информации;

- **целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Цели и задачи политики

3.1. Основными целями информационной безопасности администрации поселения являются:

- повышение стабильности функционирования администрации поселения в целом;

- достижение адекватности мер по защите от реальных угроз информационной безопасности;

- предотвращение или снижение ущерба от инцидентов нарушения информационной безопасности.

3.2. Основными задачами деятельности по обеспечению информационной безопасности администрации поселения являются:

- выполнение требований действующего законодательства Российской Федерации по обеспечению информационной безопасности;

- контроль за выполнением установленных требований по обеспечению информационной безопасности;

- разработка и совершенствование организационно-распорядительных документов администрации поселения и ее структурных подразделений в области обеспечения информационной безопасности;

- выявление, оценка и прогнозирование угроз информационной безопасности;

- выработка рекомендаций по устранению уязвимых мест системы информационной безопасности;

- организация антивирусной защиты информационных активов;

- защита информации от несанкционированных действий и утечки по техническим каналам связи.

4. Объекты защиты

4.1. Основными объектами системы информационной безопасности в администрации поселения являются:

- управленческий процесс;

- межведомственное взаимодействие;

- финансово-экономическая информация;

- информационный технологический процесс;

- информация ограниченного распространения, не составляющая государственную тайну.

4.2. Информация ограниченного распространения, не составляющая государственную тайну, обрабатываемая в ИС администрации поселения, состоит из:

- сведений, содержащихся в личных делах сотрудников администрации поселения;

- сведений о доходах, имуществе и обстоятельствах имущественного характера сотрудников администрации поселения, если действующим законодательством Российской Федерации они не отнесены к сведениям открытого доступа;

- сведений, раскрывающих систему, средства и методы защиты информации на средствах вычислительной техники от несанкционированного доступа, а также значений действующих кодов и паролей;

- сведений, содержащихся в материалах по аттестации технических

средств и систем, предназначенных для защиты или обработки конфиденциальной информации;

- других служебных сведений, доступ к которым ограничен в соответствии с действующим законодательством Российской Федерации.

5. Основные принципы обеспечения информационной безопасности

5.1. Основными принципами обеспечения информационной безопасности являются:

- постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов администрации поселения;
- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность администрации поселения, корректировка моделей угроз;
- разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом;
- контроль эффективности принимаемых защитных мер.

6. Модель угроз и модель нарушителей

6.1. Модель угроз используется для анализа защищенности ИС администрации поселения и разработки системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз. Возможные угрозы представлены в приложении к настоящему Положению.

6.2. По признаку принадлежности к ИС все нарушители делятся на две группы:

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

6.2.1. Внутренним нарушителем может быть лицо из следующих категорий сотрудников администрации поселения:

- зарегистрированные пользователи информационных систем;
- сотрудники, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем, но имеющие доступ в здания и помещения администрации поселения;
- персонал, обслуживающий технические средства информационной системы;
- сотрудники подразделений, задействованные в разработке и сопровождении программного обеспечения.

6.2.2. Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники;
- представители организаций, взаимодействующих по вопросам

технического обеспечения;

- посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);

- другие лица, заинтересованные в нарушении целостности, доступности и конфиденциальности информации.

7. Формы и средства обеспечения информационной безопасности

7.1. Обеспечение информационной безопасности администрации поселения реализуется следующими формами защиты:

- организационной;

- программно-аппаратной.

7.2. Меры защиты призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

7.3. Организационной формой защиты являются (но не ограничиваются) мероприятия, предусмотренные данной политикой. К ним относятся:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании технической инфраструктуры администрации поселения и других ассоциированных с ней объектов;

- мероприятия по разработке правил доступа пользователей;

- мероприятия по организации парольной защиты;

- мероприятия по разработке правил работы с сетью Интернет;

- мероприятия по организации антивирусной защиты;

- мероприятия, осуществляемые при подборе и подготовке сотрудников на должности в администрации поселения;

- организация охраны и режима допуска к системе;

- организация учета, хранения, использования и уничтожения документов и носителей информации;

- распределение реквизитов разграничения доступа.

7.4. Программными и аппаратными формами защиты являются (но не ограничиваются) мероприятия, предусмотренные данной политикой. К ним относятся:

- идентификация и аутентификация пользователей;

- разграничение доступа к ресурсам;

- регистрация событий;

- криптографические преобразования;

- проверка целостности системы;

- создание физических препятствий на путях проникновения нарушителей.

7.4.1. В целях предотвращения работы с ресурсами информационных

систем администрации поселения посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей).

7.4.1.1. Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

- путем проверки знания ими паролей.

7.4.2. Средства разграничения доступа.

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

7.4.2.1. Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа к:

- компонентам информационной среды и элементам системы защиты информации (физический доступ);

- информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

- активным ресурсам (прикладным программам, задачам и т.п.);

- операционной системе, системным программам и программам защиты.

7.4.3. Средства обеспечения и контроля целостности.

7.4.3.1. Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

7.4.3.2. Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

7.4.3.3. Контроль целостности информации и средств защиты с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, носителям информации, серверам, логическим устройствам и т.п.);

- средствами электронно-цифровой подписи;

- средствами учета.

7.4.4. Средства оперативного контроля и регистрации событий безопасности.

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей и т.п.), которые могут привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

7.4.4.1. Средства контроля и регистрации должны предоставлять

возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);

- получения твердой копии (печати) журнала регистрации событий безопасности;

- упорядочения журналов, а также установления ограничений на срок их хранения;

- оперативного оповещения администратора безопасности о нарушениях.

7.4.5. Криптографические средства защиты информации.

Элементами системы обеспечения безопасности информации информационной системы администрации поселения являются криптографические методы и средства защиты.

7.4.5.1. Конфиденциальность и защита информации при ее передаче по каналам связи должна обеспечиваться также за счет применения в системе шифросредств абонентского шифрования. В информационной системе администрации поселения, являющейся структурой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений.

7.4.6. Создание физических препятствий на путях проникновения нарушителей.

7.4.6.1. Физические меры защиты основаны на применении разного рода механических, электронных 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.

7.4.6.2. 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 них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой зоны технических средств съема информации.

7.4.6.3. Для обеспечения физической безопасности компонентов информационной системы администрации поселения необходимо осуществлять ряд организационных и технических мероприятий, включающих проверку оборудования, предназначенного для обработки защищаемой информации, на:

- наличие специально внедренных закладных устройств;

- побочные электромагнитные излучения и наводки;

- введение дополнительных ограничений по доступу в помещения,

предназначенные для хранения и обработки закрытой информации;

- оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

8. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов информационной безопасности

8.1. К техническим мерам обеспечения непрерывной работы и восстановления ресурсов относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения ИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

8.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

8.3. Все критичные помещения администрации поселения (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

8.5. Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должна использоваться технология резервного копирования. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, применяется дублирование данных, хранимых на дисках.

8.6. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для информации, содержащей сведения ограниченного распространения, - не реже одного раза в месяц;
- для технологической информации – не реже одного раза в три месяца;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС, – не реже одного раза в полгода и каждый раз при внесении изменений в эталонные копии (выход новых версий).

9. Управление информационной безопасностью

9.1. Управление информационной безопасностью администрации поселения включает в себя:

- своевременную актуализацию настоящей политики;
- разработку регламентирующих и методических документов обеспечения информационной безопасности;
- обеспечение штатного функционирования комплекса средств информационной безопасности администрации поселения;
- осуществление контроля за функционированием системы информационной безопасности;
- обучение с целью поддержки (повышения) квалификации персонала администрации поселения;
- оценку рисков, связанных с нарушением информационной безопасности.

9.2. Основными направлениями по обеспечению информационной безопасности являются:

- разработка технических, организационных и административных планов реализации политики информационной безопасности;
- проведение единой технической политики, организация и координация работ по защите информации;
- участие в согласовании проектов всех внутренних документов, затрагивающих вопросы безопасности технологий, используемых администрацией поселения;
- подготовка рекомендаций по выбору средств защиты информации;
- администрирование средств защиты информации администрации поселения в части обеспечения работоспособности прикладного программного обеспечения и их обновления;
- участие в обеспечении бесперебойной работы АС администрации поселения и восстановлении работы после сбоев;
- обучение пользователей безопасной работе с информационными активами;
- контроль за соблюдением требований по использованию антивирусных средств;
- организация аттестации объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности и/или конфиденциальности;
- организация и проведение работ по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;
- разработка предложений по организации и совершенствованию системы защиты информации;
- подготовка отчетов о состоянии работы по защите информации.

9.3. Работники администрации поселения обеспечивают соблюдение положений настоящей политики и иных документов по защите информации в подразделении.

10. Контроль за соблюдением настоящего Положения

10.1 Контроль за соблюдением требований по информационной

безопасности в администрации поселения обеспечивает глава администрации Клименковского сельского поселения муниципального района «Вейделевский район» Белгородской области.

10.2. Общий контроль состояния информационной безопасности осуществляется сотрудниками администрации поселения, ответственными за обеспечение информационной безопасности.

10.3. Контроль осуществляется путем проведения мониторинга и управления инцидентами информационной безопасности администрации поселения по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

10.4. Контроль эффективности средств защиты необходимо осуществлять не реже одного раза в год. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы средств защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ИС.

10.5. Мероприятия по осуществлению контроля включают в себя:

- контроль за соблюдением режима защиты;
- контроль за соблюдением режима обработки информации, содержащей сведения ограниченного распространения;
- контроль за выполнением антивирусной защиты;
- контроль за соблюдением режима защиты при подключении к сетям общего пользования;
- контроль за обновлениями программного обеспечения (ПО) и единообразия применяемого ПО на всех элементах ИС;
- контроль за обеспечением резервного копирования;
- организация анализа и пересмотра имеющихся угроз безопасности ИС, а также предсказание появления новых, еще неизвестных, угроз;
- поддержание в актуальном состоянии нормативно-организационных документов;
- контроль за разработкой и внесением изменений в ПО собственной разработки или в штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.

ПРИЛОЖЕНИЕ
к Положению о политике
информационной безопасности
администрации Клименковского
сельского поселения муниципального района
«Вейделевский район» Белгородской области

ВОЗМОЖНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ОПИСАНИЕ

№ п/п	Название угрозы	Возможные источники угрозы	Используемые уязвимости	Вид активов, потенциально подверженных угрозе	Возможные последствия реализации угрозы
1.	Осуществление несанкционированного доступа (ознакомления) с целевой информацией при ее обработке и хранении в ИС администрации поселения	пользователи ИС администрации поселения	недостатки механизмов разграничения доступа к целевой информации, связанные с возможностью предоставления доступа к целевой информации неуполномоченным на это лицам	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации
2.	Осуществление несанкционированного копирования (хищения) информации, содержащей конфиденциальные сведения	пользователи ИС администрации поселения	недостатки механизмов безопасного взаимодействия автоматизированных рабочих мест (далее - АРМ) пользователей с серверами ИС	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации
3.	Осуществление необнаруженной несанкционированной модификации (подмены) защищаемой информации	пользователи ИС администрации поселения	недостатки механизмов разграничения доступа к защищаемой информации и механизмов аудита, связанные с возможностью необнаруженной модификации (подмены) целевой информации неуполномоченными	защищаемая информация	навязывание должностным лицам модифицированной (ложной) информации; передача по запросам модифицированной (ложной) информации и нарушение режимов

			на это лицами		функционирования ИС
4.	Осуществление необнаруженного несанкционированного блокирования (нарушение доступности) защищаемой информации	пользователи ИС администрации поселения; другие лица, являющиеся внешними по отношению к ИС	недостатки механизмов безопасного администрирования сервисов, предоставляемых ИС, а также механизмов аудита, связанные с возможностью бесконтрольного блокирования доступности защищаемой информации	защищаемая информация	непредставление целевой информации заинтересованным лицам в отведенное время; нарушение штатного режима функционирования ИС
5.	Перехват защищаемой информации в каналах связи с использованием специально разработанных технических средств и ПО	пользователи ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	недостатки механизмов защиты передаваемой информации, связанные с возможностью ее перехвата из каналов связи и последующего с ней ознакомления	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации, используемой в ИС; несанкционированное ознакомление с принципами функционирования механизмов защиты в ИС, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС
6.	Внедрение в ИС компьютерных вирусов	пользователи ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	недостатки механизмов защиты информационных ресурсов ИС от компьютерных вирусов	программное обеспечение	нарушение режимов функционирования ИС; реализация различного рода негативных информационных воздействий на целевую, технологическую информацию и

					программное обеспечение ИС
7.	Осуществление необнаруженных несанкционированных информационных воздействий (направленных на "отказ в обслуживании" для сервисов, модификацию конфигурационных данных программно-аппаратных средств и т.п.) на программно-аппаратные элементы ИС	пользователи ИС администрации поселения; другие лица, являющиеся внешними по отношению к ИС	недостатки механизмов защиты программно-аппаратных элементов ИС от несанкционированных внешних воздействий	защищаемая информация, программное обеспечение	нарушение режимов функционирования ИС; снижение уровня защищенности ИС; подготовка к последующим воздействиям и осуществление несанкционированного доступа к защищаемым информационным ресурсам
8.	Осуществление несанкционированного доступа к информационным активам, основанного на использовании средств защиты информации, телекоммуникационного оборудования с уязвимостями и недокументированными возможностями, внесенными на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств	пользователи ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	наличие не декларированных возможностей, внесенных на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации; нарушение режимов функционирования
9.	Осуществление	пользователи ИС;	недостатки механизмов	защищаемая	несанкционированное

	несанкционированного доступа к защищаемой информации, основанного на восстановлении (в том числе фрагментарном) остаточной информации путем анализа выведенных из употребления, сданных в ремонт, на обслуживание, переданных для использования другим пользователям или для использования за пределами ИС носителей информации	уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	гарантированного уничтожения защищаемой информации, связанные с возможностью ее последующего несанкционированного восстановления	информация	ознакомление и разглашение защищаемой информации
10.	Внедрение в ИС вредоносного программного обеспечения	пользователи ИС; уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	недостатки механизмов защиты информационных ресурсов ИС от вредоносного программного обеспечения	защищаемая информация, программное обеспечение	несанкционированное ознакомление и разглашение защищаемой информации; создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС; нарушение режимов функционирования ИС
11.	Перехват разглашаемых сведений о защищаемой информации, ИС и ее компонентах	сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.)	недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью перехвата разглашаемой защищаемой информации	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации; создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС

12.	Хищение производственных отходов (распечаток, записей, списанных носителей) с целью последующего анализа и несанкционированного ознакомления с целевой и технологической информацией	сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.)	недостатки организационно-технических мер, обеспечивающих гарантированное уничтожение производственных отходов в ИС, связанные с возможностью их несанкционированного хищения и последующего использования для проведения аналитических исследований	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы
13.	Осуществление несанкционированного визуального просмотра защищаемой информации, отображаемой на средствах отображения (экранах мониторов), а также несанкционированное ознакомление с распечатываемыми документами, содержащими защищаемую информацию	сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.)	недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью несанкционированного визуального просмотра защищаемой информации на средствах отображения (экранах мониторов)	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы
14.	Осуществление несанкционированного доступа к защищаемой информации в процессе ремонтных и регламентных работ	уполномоченный персонал разработчиков ИС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС	доступ лиц, имеющих право на техническое обслуживание, к техническим и программным средствам ИС в момент обработки с использованием этих средств защищаемой информации	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы ИС; нарушение режимов функционирования ИС

15.	Осуществление несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам	сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы ИС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.)	недостатки реализации необходимых организационно-режимных мероприятий на объектах ИС, связанные с возможностью несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам	защищаемая информация	несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы