**РОССИЙСКАЯ ФЕДЕРАЦИЯ ОРЛОВСКАЯ ОБЛАСТЬ
ШАБЛЫКИНСКИЙ РАЙОН
АДМИНИСТРАЦИЯ ТИТОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**ПОСТАНОВЛЕНИЕ**

От 02.05. 2024 года № 15

**Об обеспечении информационной безопасности и назначении ответственных лиц**

В целях обеспечения безопасности информации в администрации Титовского сельского поселения Шаблыкинского района Орловской области и выполнения требований Федеральных законов и нормативно-правовых и нормативно-методических актов в области защиты информации, администрация Титовского сельского поселения

**ПОСТАНОВЛЯЕТ:**

* 1. Назначить ответственным за организацию обработки персональных данных (далее – защищаемая информация) в информационных системах персональных данных администрации Титовского сельского поселения (далее – ИС) главу администрации Захаркину Ольгу Васильевну.
1. Возложить на Захаркину О. В. следующие обязанности:
* оформление (ведение) и своевременное уточнение списка лиц, доступ которых к защищаемой информации, обрабатываемой в ИС, необходим для выполнения служебных обязанностей, а также списка лиц, имеющих право бесконтрольного пребывания в помещениях, в которых производится обработка защищаемой информации;
* контроль выполнения сотрудниками, допущенными к обработке защищаемой информации, предъявляемых требований к безопасности информации;
* контроль эффективности принимаемых организационных мер по обеспечению безопасности защищаемой информации в соответствии с утвержденными документами, определяющими требования к организации обработки защищаемой информации;
* выявление фактов несоблюдения условий хранения носителей защищаемой информации, использования нерегламентированных программных и технических средств, способных привести к нарушению конфиденциальности обрабатываемых данных, а также иных нарушений, приводящих к снижению уровня защищенности;
* доведение до сведения сотрудников, допущенных к обработке защищаемой информации, положений законодательства Российской Федерации о защите информации, локальных актов по вопросам обработки защищаемой информации;
* организация приема, обработки и учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных, осуществление контроля за обработкой таких обращений.
1. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных (приложение 1 к данному Постановлению).
2. Назначить администратором безопасности персональных данных главу сельского поселения Захаркину О.В.
3. Возложить на Захаркину О.В. следующие обязанности:
* организация эксплуатации и контроля работоспособности технических и программных средств ИС, в том числе средств и систем защиты информации в соответствии с установленными организационно-техническими требованиями по защите информации и эксплуатационными документами;
* обслуживание и ремонт технических средств ИС;
* осуществление резервного копирования (восстановления) баз данных и документов, содержащих обрабатываемую защищаемую информацию;
* контроль за работой пользователей ИС, своевременное выявление и регистрация попыток несанкционированного доступа к защищаемой информации;
* обучение лиц, использующих средства защиты информации, применяемые в ИС, правилам работы с ними.
1. Утвердить и ввести в действие Инструкцию администратора безопасности персональных данных (приложение 2 к данному Постановлению).
2. Создать Комиссию по вопросам информационной безопасности (приложение 3 к данному Постановлению).
3. Утвердить и ввести в действие Положение о Комиссии по вопросам информационной безопасности (приложение 4 к данному Постановлению).
4. Комиссии по вопросам информационной безопасности провести работы по выявлению информационных систем администрации Титовского сельского поселения и определению уровня защищенности обрабатываемых персональных данных.
5. Утвердить План мероприятий по контролю за обеспечением безопасности персональных данных (приложение 5 к данному Постановлению).
6. Утвердить Форму Протокола проведения внутренней проверки условий обработки защищаемой информации (приложение 6 к данному Постановлению).
7. Утвердить Форму Журнала проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к защите такой информации (приложение 7 к данному Постановлению). Обязанности по ведению данного журнала возложить на ответственного за организацию обработки персональных данных.
8. Утвердить Перечень программного обеспечения, разрешенного к установке в информационных системах персональных данных администрации Титовского сельского поселения (приложение 8 к данному Постановлению).
9. Утвердить Политику выявления инцидентов информационной безопасности (приложение 9 к данному Постановлению).
10. Контроль за исполнением настоящего Постановления оставляю за собой.

Глава Титовкого сельского поселения О.В.Захаркина

Приложение 1 к Постановлению № 15 от 02.05.2024г

**ИНСТРУКЦИЯ**

**ответственного за организацию обработки персональных данных**

# Обозначения и сокращения по тексту

|  |  |  |
| --- | --- | --- |
| Организация |  | Администрация Титовского сельского поселения  |
| Ответственный (ответственное лицо) |  | Должностное лицо, ответственное за организацию обработки персональных данных; |
| ИС |  | Информационные системы персональных данных; |
| Защищаемая информация |  | Персональные данные (ПДн). |

# Общие положения

* 1. В настоящем документе определяются права, обязанности, а также ответственность должностного лица, ответственного за организацию обработки персональных данных в администрации Титовского сельского поселения.
	2. Лицо, ответственное за организацию обработки персональных данных (далее – лицо, отвечающее за организацию обработки защищаемой информации с использованием средств автоматизации и без использования таких средств, а также доступ защищаемой информации в Организации.
	3. Ответственный назначается приказом руководителя Организации и подотчетен ему.

# Должностные обязанности

* 1. Ответственное лицо обязано осуществлять внутренний контроль соблюдения сотрудниками Организации Законодательства Российской Федерации о защите информации.
	2. Ответственное лицо обязано доводить до сведения сотрудников Организации положения законодательства защите информации, локальные акты по вопросам информационной безопасности, требования к защите данных.
	3. Ответственное лицо разрабатывает и поддерживает в актуальном состоянии список лиц, допущенных к обработке защищаемой информации.
	4. Требования ответственного лица, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками Организации.

# Должностные права

* 1. Ответственное лицо имеет право:
* Запрашивать у сотрудников Организации информацию, необходимую для реализации своих полномочий.
* Требовать от сотрудников Организации, являющихся пользователями информационных систем, выполнения установленной технологии обработки защищаемой информации, инструкций и других локальных актов по обеспечению безопасности защищаемой информации.
* Участвовать в разработке мероприятий по совершенствованию безопасности защищаемой информации.
* Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности.
* Принимать меры по приостановлению или прекращению обработки защищаемой информации, осуществляемой с нарушением требований законодательства Российской Федерации.
* Вносить руководителю Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки защищаемой информации или нарушения режима конфиденциальности.
* Вносить руководителю Организации предложения о совершенствовании правового, технического и организационного регулирования обеспечения защиты информации.

# Ответственность

* 1. Ответственное лицо несет персональную ответственность за качество проводимых им работ, связанных с выполнением им своих должностных обязанностей.
	2. За нарушение настоящей Инструкции Ответственное лицо может быть привлечено к дисциплинарной или иной предусмотренной законодательством ответственности.

# Прием обращений субъектов персональных данных

* 1. Ответственное лицо обязано организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей в журнале учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных и осуществлять контроль приема и обработку таких обращений и запросов.
	2. Запрос может содержать:
* номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя;
* сведения о дате выдачи указанного документа и выдавшем его органе;
* сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словестное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором;
* подпись субъекта ПДн или его законного представителя.
	1. В случае отсутствия в запросе, по крайней мере, одного пункта из п. 3.2, прием обращения производится по усмотрению ответственного лица.

# ЛИСТ ОЗНАКОМЛЕНИЯ

**с инструкцией ответственного за организацию персональных данных**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **ФИО** | **Должность** | **Подпись, дата** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 2 к Постановлению № 15 от 02.05.2024г

**ИНСТРУКЦИЯ**

**администратора безопасности персональных данных**

1. **Обозначения и сокращения по тексту**

|  |  |  |
| --- | --- | --- |
| Организация |  | Администрация Титовского сельского поселения Шаблыкинского района Орловской области |
| Администратор безопасности |  | Администратора безопасности персональных данных; |
| ИС |  | Информационные системы персональных данных; |
| Защищаемая информация |  | Персональные данные (ПДн); |

1. **Общие положения**
	1. Настоящая инструкция определяет права и обязанности должностного лица, ответственного за обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных администрации Титовского сельского поселения
	2. Администратор безопасности назначается постановлением руководителя Организации и отвечает за обеспечение безопасности защищаемой информации при ее обработке в ИС администрации Титовского сельского поселения;
	3. Администратор безопасности по вопросам обеспечения безопасности защищаемой информации подчиняется непосредственно руководителю Организации;
	4. Администратор безопасности отвечает за поддержание установленного уровня защищенности информации;
	5. Администратор безопасности осуществляет методическое руководство деятельности пользователей ИС, допущенных к обработке защищаемой информации;
	6. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИС;
	7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, состояния и поддержания установленного уровня защищенности информации, обрабатываемой в ИС;
	8. Администратор безопасности обеспечивает нормальное функционирование защитных механизмов ИС;
	9. Настоящая инструкция не исключает обязательного выполнения требований других действующих нормативных документов по вопросам обеспечения защиты информации.
2. **Задачи администратора безопасности**
	1. Основными задачами администратора безопасности являются:
* поддержание необходимого уровня защиты ИС от несанкционированного доступа (НСД) к защищаемой информации;
* обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи защищаемой информации;
* установка средств защиты информации и контроль выполнения правил их эксплуатации;
* сопровождение средств защиты информации (СЗИ) и основных технических средств и систем (ОТСС) ИС;
* периодическое обновление СЗИ ИС;
* оперативное реагирование на нарушения требований по информационной безопасности (ИБ) в ИС и участие в их прекращении.
	1. В рамках выполнения основных задач администратор безопасности осуществляет:
* текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
* текущий контроль технологического процесса автоматизированной обработки защищаемой информации;
* участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности защищаемой информации;
* управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;
* управление СЗИ в ИС, в том числе параметрами настройки программного обеспечения (ПО), включая ПО СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;
* установка обновлений ПО, включая ПО СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;
* централизованное управление системой защиты информации;
* регистрация и анализ событий в ИС, связанных с защитой информации (далее – события безопасности);
* информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации и отдельных СЗИ, а также их обучение;
* сопровождение функционирования системы защиты информации ИС в ходе ее эксплуатации;
* поддержание конфигурации ИС и системы защиты информации (структуры системы защиты информации, состава, мест установки и параметров настройки СЗИ, ПО и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС и системы защиты информации);
* управление изменениями базовой конфигурации ИС и системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и системы защиты информации;
* анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность Организации;
* определение параметров настройки ПО, включая ПО СЗИ, состава и конфигурации технических средств и ПО до внесения изменений в базовую конфигурацию ИС и системы защиты информации;
* методическую помощь всем пользователям ИС по вопросам обеспечения безопасности информации.
1. **Администратор безопасности имеет право:**
	1. Отключать от ресурсов ИС работников, осуществивших НСД к защищаемым ресурсам ИС или нарушивших другие требования по ИБ;
	2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ;
	3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИС;
	4. Осуществлять контроль информационных потоков, генерируемых пользователями ИС при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа;
	5. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное ПО и аппаратное обеспечение;
	6. Вырабатывать предложения по дальнейшему усовершенствованию принятой политики безопасности, выбору используемого в ИС ПО и аппаратного обеспечения.
2. **Администратор безопасности обязан:**
	1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок обеспечения безопасности информации, обрабатываемой в ИС;
	2. Управлять конфигурацией системы защиты информации ИС:
* Разграничивать права доступа в ИС;
* Осуществлять управление изменениями конфигурации ИС и системы защиты информации ИС, проводить анализ потенциального воздействия планируемых изменений, осуществлять документирование данных о таких изменениях;
* Осуществлять контроль безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
* Выполнять периодическое резервное копирование защищаемой информации и элементов ИС на резервные машинные носители информации;
* Участвовать в установке, настройке и сопровождении программных СЗИ;
* Участвовать в приемке новых программных средств обработки информации.
* Осуществлять периодический мониторинг (контроль) защищенности ИС:
* Осуществлять обнаружение, идентифицировать и регистрировать инциденты (события безопасности);
* Своевременное информировать лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС;
* Осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
* Выявлять, анализировать уязвимости системы защиты информации ИС и оперативно устранять вновь выявленные уязвимости;
* Осуществлять контроль установки обновлений ПО, включая обновления ПО СЗИ;
* Обеспечивать контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
* Осуществлять контроль состава технических средств, ПО и СЗИ;
* Осуществлять контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей;
* Осуществлять контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов, в том числе по передачи информации;
* Осуществлять контроль выполнения мер по защите технических средств;
* Осуществлять анализ событий во время загрузки ОС;
* Осуществлять отслеживание попыток использования ИС вне установленного рабочего времени;
* Отслеживать изменения в перечне пользователей, допущенных к работе в ИС;
* Осуществлять обнаружение использования ПО, не внесенного в список разрешенного ПО;
* Осуществлять обнаружение новых (неизвестных) устройств;
* Осуществлять проверку соответствия общесистемной программной среды эталону (контроль целостности ПО).
	1. Обеспечить доступ к защищаемой информации пользователям ИС, согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки);
	2. Установленным порядком хранить резервные копии, регистрации фактов нарушения установленного порядка работ и попыток НСД;
	3. Вести журнал создания резервных копий информации и необходимого программного обеспечения;
	4. Контролировать исполнение пользователями ИС введенного режима безопасности, а также правильность работы с элементами ИС и СЗИ;
	5. Контролировать исполнение пользователями правил парольной политики;
	6. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений;
	7. Оказывать помощь пользователям ИС в части применения СЗИ и консультировать по вопросам введенного режима защиты;
	8. В случае отказа работоспособности технических средств и ПО ИС, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
	9. В случае выявления нарушений режима безопасности защищаемой информации, а также возникновения внештатных и аварийных ситуаций, немедленно докладывать об этом ответственному лицу и принимать необходимые меры с целью ликвидации их последствий;
	10. В случае болезни, отпуска и т.п. администратор безопасности передает свои обязанности замещающему его лицу, назначаемому приказом руководителя Организации.
1. **Ответственность администратора безопасности**

Администратор безопасности несет ответственность:

* 1. За качество выполнения обязанностей, установленных данной Инструкцией;
	2. За качество проводимых работ по контролю действий пользователей, состояние и поддержание необходимого уровня защищенности информации, содержащейся в ИС;
	3. За разглашение данных, ставших известными ему по роду работы.
1. **Действия администратора безопасности при обнаружении попыток НСД**
	1. К попыткам НСД относятся:
* сеансы работы с ИС незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;
* действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИС с использованием учетной записи администратора или другого пользователя ИС, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
	1. При выявлении факта/попытки НСД администратор безопасности обязан:
* прекратить доступ к ИС со стороны выявленного участка НСД;
* доложить руководителю и/или ответственному за обеспечение безопасности информации в Организации о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
* проанализировать характер НСД;
* по решению ответственного за обеспечение безопасности персональных данных осуществить действия по выяснению причин, приведших к НСД;
* предпринять меры по предотвращению подобных инцидентов в дальнейшем.

**ЛИСТ ОЗНАКОМЛЕНИЯ**

**с инструкцией администратора безопасности персональных данных**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **ФИО** | **Дата** | **Подпись** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 3 к Постановлению № 15 от 02.05.2024г

**СОСТАВ**

**комиссии по вопросам информационной безопасности**

|  |  |  |
| --- | --- | --- |
| Председатель комиссии:  | Захаркина О.В. | Глава сельской администрации |
| Члены комиссии: | Федотова Е.Н. | Ведущий специалист администрации |
|  | Прудникова Т.Г.  | Депутат с/с (по согласованию) |
|  |  |  |
|  |  |  |
|  |  |  |

Приложение 4 к Постановлению № 15 от 02.05.2024г

**ПОЛОЖЕНИЕ**

**о Комиссии по вопросам информационной безопасности**

1. **Общие положения**
	1. Настоящее Положение определяет структуру, основные задачи и порядок работы Комиссии по вопросам информационной безопасности администрации Титовского сельского поселения (далее – Комиссия).
	2. Комиссия назначается постановлением главы администрации сельского поселения (далее – Организация).
	3. Комиссия создается для достижения следующих целей:
* исполнение положений нормативных правовых актов в сфере информации, информационных технологий и защиты информации;
* укрепление безопасности в организации путем непосредственного участия руководства и выделения необходимых ресурсов;
* координация внедрения мероприятий по управлению информационной безопасностью.
	1. Комиссия осуществляет свою деятельность в соответствии с действующими федеральными законами, постановлениями и решениями Правительства Российской Федерации, методическим и руководящими документами органов уполномоченных в сфере технической защиты информации, приказами и указаниями руководства Организации, данным Положением и иными внутренними организационными распорядительными документами.
	2. Организационно Комиссия состоит из председателя и членов Комиссии.
	3. Решения Комиссии являются обязательными для всех работников Организации и вступают в силу после их утверждения.
1. **Основные задачи Комиссии**
	* Определение концептуальных подходов к обеспечению защиты информации в Организации.
	* Утверждение и пересмотр политики информационной безопасности и соответствующих обязанностей по ее выполнению.
	* Анализ и мониторинг инцидентов нарушения информационной безопасности.
	* Утверждение основных проектов в области информационной безопасности.
	* Согласование конкретных функций и обязанностей в области информационной безопасности в рамках Организации.
	* Согласование конкретных методик и процедур информационной безопасности.
	* Оценка адекватности и координация внедрения конкретных мероприятий по управлению информационной безопасностью для новых систем или услуг.

Примечание: По решению председателя Комиссии могут рассматриваться и другие вопросы, возникшие в ходе работ по защите информации.

1. **Порядок работы Комиссии**
	1. Периодичность созыва Комиссии определяется ее председателем.
	2. Для оперативного решения вопросов связанных с информационной безопасностью могут проводиться внеочередные созывы Комиссии. Инициатива о внеочередном созыве Комиссии может поступать от руководителя Организации, председателя Комиссии, ответственного за организацию обработки персональных данных или администратора безопасности информации.
	3. Решения Комиссии принимаются открытым голосованием и считаются принятыми, если они поддержаны большинством присутствующих членов Комиссии.
	4. Решения Комиссии утверждаются руководителем Организации и доводятся до исполнителей и других заинтересованных лиц в части, их касающейся.
	5. Протоколы и решения Комиссии хранятся у председателя Комиссии, в соответствии с требованиями, предъявленными к защищенному документообороту.

Приложение 5 к Постановлению № 15 от 02.05.2024г

## ПЛАН МЕРОПРИЯТИЙ

## по контролю за обеспечением безопасности персональных данных

**Обозначения и сокращения**

|  |  |  |
| --- | --- | --- |
| Ответственный |  | Должностное лицо, ответственное за организацию обработки персональных данных; |
| Администратор безопасности |  | Администратор безопасности персональных данных |
| ИС |  | Информационные системы персональных данных; |

**План мероприятий**

| **№ п/п** | **Мероприятие** | **Исполнители** | **Сроки проведения** |
| --- | --- | --- | --- |
|  | Уточнение и корректировка списков лиц/должностей, допущенных к обработке защищаемой информации | Ответственный  | На постоянной основе по мере необходимости |
|  | Контроль за соблюдением порядка доступа в помещения, где расположены элементы ИС | Ответственный | На постоянной основе по мере необходимости |
|  | Контроль порядка реагирования на обращения субъектов персональных данных о выполнении их законных прав в области защиты персональных данных | Ответственный | На постоянной основе по мере необходимости |
|  | Проверка знаний пользователями ИС положений законодательства РФ о защите информации, в том числе требований к защите персональных данных, документов, определяющими политику в отношении информационной безопасности, локальных актов по вопросам обработки защищаемой информации, и (или) обучение указанных сотрудников | Ответственный | 1 раз в полгода |
|  | Контроль получения согласий с субъектов персональных данных на обработку его персональных данных; контроль получения соглашений о соблюдении конфиденциальности от пользователей, допущенных к обработке защищаемой информации  | Ответственный  | 1 раз в полгода |
|  | Проверка знания пользователями ИС действий при внештатных ситуациях | Ответственный | 1 раз в полгода |
|  | Контроль за соблюдением антивирусной политики | Администратор безопасности  | Ежемесячно |
|  | Контроль за соблюдением порядка резервирования баз данных и хранения резервных копий | Администратор безопасности | Ежемесячно |
|  | Контроль за работоспособностью средств защиты информации, а также работы пользователей со средствами защиты информации (анализ и мониторинг журналов регистрации событий безопасности) | Администратор безопасности | 1 раз в квартал |
|  | Контроль за соблюдением пользователями ИС правил работы со съемными носителями защищаемой информации | Администратор безопасности | 1 раз в квартал |
|  | Контроль состава основных технических средств и систем | Администратор безопасности  | 1 раз в квартал |
|  | Контроль обновления программного обеспечения ИС, предназначенного для обработки защищаемой информации, а также программного обеспечения установленных средств защиты информации  | Администратор безопасности  | 1 раз в полгода |
|  | Контроль за соблюдением пользователями ИС парольной политики | Администратор безопасности | 1 раз в полгода |
|  | Организация анализа и пересмотра имеющихся угроз безопасности информации (персональных данных), а так же выявление новых, еще не известных угроз | Администратор безопасности | 1 раз в год |

Приложение 6

к Постановлению № 15 от 02.05.2024г

**ФОРМА**

**ПРОТОКОЛ**

**проведения внутренней проверки условий обработки защищаемой информации**

Настоящий Протокол составлен о том, что \_\_\_\_.\_\_\_\_ 20\_\_\_ г. ответственным за организацию обработки персональных данных/администратором безопасности/комиссией проведена проверка\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (тема проверки)

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В ходе проверки проверено:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Выявленные нарушения:

Меры по устранению нарушений:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| *Должность Ответственного* | *Подпись* | *И.О. Фамилия* |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| *Должность Ответственного* | *Подпись* | *И.О. Фамилия* |

Приложение 7

к Постановлению № 15 от 02.05.2024г **ФОРМА**

**ЖУРНАЛ №\_\_\_**

**проведения внутреннего контроля соответствия обработки защищаемой информации требованиям к защите такой информации**

На \_\_\_\_ листах

| **№ п/п** | **Дата проведения** | **Мероприятие** | **Исполнитель** | **Результат** | **Подпись** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Приложение 8

к Постановлению № 15 от 02.05.2024г

**Перечень**

**программного обеспечения, разрешенного к установке в информационных системах персональных данных администрации Титовского сельского поселения Шаблыкинского района Орловской области**

| **Наименование** | **Версия** | **Производитель** | **Место установки** |
| --- | --- | --- | --- |
| *Операционная система семейства ОС Windows* |  |  | *Все ПЭВМ, входящие в состав ИС* |
| *MS Office* |  |  |
| *Файловый архиватор 7-Zip* |  |  |
|  |  |  |
|  |  |  |
|  |  |  | *АРМ Администратора безопасности* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |

Приложение 9

к Постановлению № 15 от 02.05.2024г

**ПОЛИТИКА**

**выявления инцидентов информационной безопасности**

1. **Общие положения**
	1. Настоящая Политика выявления инцидентов информационной безопасности (далее – Политика) определяет общие функции, ответственность, права и обязанности ответственных за обеспечение информационной безопасности в администрации Титовского сельского поселения Шаблыкинского района Орловской области (далее по тексту – Организация).
	2. При осуществлении мониторинга информационной безопасности в Организации должна обеспечиваться возможность получения информации о зарегистрированных событиях безопасности и иных данных от различных источников, таких как средства защиты информации, общесистемное и прикладное программное обеспечение, специальное программное обеспечение и сервисы, телекоммуникационное оборудование, технологическое и (или) производственное оборудование (исполнительные устройства), среда функционирования информационных систем (далее – ИС), персонал, допущенный к работе в ИС и иные источники данных.
2. **Общие положения**
	1. Все сотрудники, взаимодействующие с ИС должны немедленно уведомлять администратора безопасности персональных данных (далее – администратора ИБ, администратор безопасности) о выявленных слабых местах и инцидентах информационной безопасности (далее – инцидент ИБ).
	2. Пользователи не должны использовать имеющиеся уязвимости.
	3. После получения уведомления, а также в случае самостоятельного обнаружения инцидента ИБ администратор безопасности должен отреагировать на инцидент ИБ и принять меры по:

1. Анализу инцидента ИБ.

2. Предотвращению развития инцидента ИБ.

3. Устранению инцидента ИБ.

4. Восстановлению безопасности после инцидента ИБ.

5. Регистрации инцидента ИБ

6. Проведению внутреннего расследования (при необходимости).

7. Формирование рекомендаций по результатам инцидента ИБ по повышению уровня защищенности.

* 1. Информация об инцидентах ИБ, приведших к нарушению безопасности ИС, должна быть задокументирована Администратором ИБ в форме «Отчёта об инциденте ИБ»
1. **Выявление инцидентов**
	1. Основными источниками информации об Инцидентах ИБ являются:
* факты, выявленные сотрудниками организации;
* результаты работы средств мониторинга ИБ, результаты проверок и аудита (внутреннего или внешнего);
* журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
* обращения субъектов с указанием Инцидента ИБ;
* другие источники информации.
	1. Основными видами инцидентов ИБ в являются:
* Разглашение защищаемой информации, либо угроза такого разглашения;
* несанкционированный доступ к ИС и защищаемой информации со стороны лиц, которые не имеют никакого легального доступа к ресурсам ИС и защищаемой информации;
* превышение полномочий - несанкционированный доступ к ИС;
* компрометация учетных записей или паролей;
* вирусная атака или вирусное заражение;
* нарушение или сбой в работе системы резервного копирования;
* нарушение правил использования ИС.
	1. Администратор безопасности, после получения информации о предполагаемом Инциденте ИБ, незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа Администратор безопасности проводит проверку наличия в выявленном факте нарушений.
	2. В случае наличия признаков Инцидента ИБ, приведшего к негативным последствиям, Администратор безопасности классифицирует инцидент, определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства.
	3. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, Администратор безопасности определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.
	4. Целями разбирательства инцидентов ИБ являются:
* выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
* защита прав, установленных законодательством Российской Федерации;
* защита информационных ресурсов ИС Организации;
* обеспечение безопасности защищаемой информации;
* предотвращение несанкционированного доступа к защищаемой информации, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.
	1. Разбирательство Инцидента ИБ, состоит из следующих этапов:
* подтверждение/опровержение факта возникновения Инцидента ИБ;
* классификация инцидента ИБ;
* подтверждение/корректировка уровня значимости Инцидента ИБ;
* уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;
* получение (сбор) доказательств возникновения Инцидента ИБ;
* минимизация последствий Инцидента ИБ;
* информирование и консультирование сотрудников по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
* переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.
	1. В процессе проведения разбирательства Инцидента ИБ обязательными для установления являются:
* дата и время совершения Инцидента ИБ;
* ФИО, должность и подразделение Нарушителя ИБ;
* классификация инцидента;
* уровень критичности Инцидента ИБ;
* обстоятельства и мотивы совершения Инцидента ИБ;
* информационные ресурсы, затронутые Инцидентом ИБ;
* характер и размер реального и потенциального ущерба;
* обстоятельства, способствовавшие совершению Инцидента ИБ.

После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство сотрудник проводит анализ полученных данных.

* 1. Администратор безопасности проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:
* прямой финансовый ущерб;
* репутационный ущерб;
* потенциальный ущерб;
* косвенные потери, связанные с недоступностью сервисов, потерей информации;
* другие виды ущерба или аспекты негативных последствий для ИС, Организации или субъектов персональных данных.
	1. По завершению разбирательства Инцидента ИБ, Администратор безопасности передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю Организации для решения вопроса о целесообразности привлечения нарушителя к дисциплинарной ответственности.
	2. На основании полученных результатов разбирательства Администратор ИБ организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:
* анализ и пересмотр имеющихся прав доступа к информационным ресурсам;
* доведение до сотрудников требований внутренних нормативных документов в части информационной безопасности;
* обсуждение Инцидента ИБ на совещании;
* усиление системы защиты.
1. **Ответственность**
	1. Каждый сотрудник, имеющий доступ к ИС и защищаемой информации несёт персональную ответственность за обеспечение информационной безопасности в соответствии с требованиями настоящей Политики.
	2. Лица, нарушившие требования безопасности, изложенные в настоящей Политике, могут быть привлечены к дисциплинарной или административной ответственности в соответствии с действующим законодательством Российской Федерации.