**АДМИНИСТРАЦИЯ**

**ЗДВИНСКОГО РАЙОНА НОВОСИБИРСКОЙ ОБЛАСТИ**

**ПОСТАНОВЛЕНИЕ**

от 17.04.2025 № 163-па

О внесении изменений в постановление администрации Здвинского района Новосибирской области от 25.09.2024 № 402-па

Администрация Здвинского района Новосибирской области

п о с т а н о в л я е т:

1. Внести в постановление администрации Здвинского района Новосибирской области от 25.09.2024 № 402-па «О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Здвинского района Новосибирской области» следующие изменения:

пункт 8 приложения 1 постановления администрации Здвинского района Новосибирской области от 25.09.2024 № 402-па «О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Здвинского района Новосибирской области» изложить в редакции, прилагаемой к настоящему постановлению.

2. Опубликовать настоящее постановление в муниципальной газете «Информационный вестник Здвинского района» и разместить на официальном сайте администрации Здвинского района Новосибирской области в информационно-телекоммуникационной сети Интернет.

Глава Здвинского района

Новосибирской области Э.В. Щербаков

Данилко Е.Ю.

8 (383 63) 21 041

|  |  |
| --- | --- |
|  | Приложение  к постановлению  администрации Здвинского района Новосибирской области  от 17.04.2025 № 163-па |

1. **Обеспечение защиты информации в ходе эксплуатации информационной системы**
   1. Обеспечение защиты информации в ходе эксплуатации ИС осуществляется администрацией района в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает следующие мероприятия:

* планирование мероприятий по защите информации;
* анализ угроз безопасности информации в ИС;
* управление (администрирование) системой защиты информации (ЗИ) ИС;
* выявление инцидентов и реагирование на них;
* управление конфигурацией ИС и ее системы ЗИ;
* контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС.
  1. В ходе планирования мероприятий по защите информации в ИС осуществляются:
* определение лиц, ответственных за планирование и контроль мероприятий по защите информации в ИС;
* определение лиц, ответственных за выявление инцидентов и реагирование на них;
* разработка, утверждение и актуализация плана мероприятий по защите информации в ИС;
* определение порядка контроля выполнения мероприятий по обеспечению защиты информации в ИС, предусмотренных утвержденным планом.

План мероприятий по защите информации в ИС администрации района (далее – План мероприятий по защите информации) определяет перечень мероприятий по защите информации, условия и периодичность, а также лиц, ответственных за их проведение (Приложение № 1 к настоящему Положению).

Контроль выполнения мероприятий, предусмотренных Планом мероприятий по защите информации, проводится в рамках внутреннего контроля соответствия обработки персональных данных в администрации района установленным требованиям с периодичностью не реже одного раза в 2 года.

В целях документирования процедур и результатов контроля составляется Протокол контроля соответствия обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в администрации района установленным требованиям.

Пересмотр и корректировка (при необходимости в случае изменения состава мероприятий по защите информации и процедур проведения контроля за их выполнением) Плана мероприятий по защите информации проводится лицом, ответственным за планирование и организацию проведения контроля мероприятий по защите информации в ИС администрации района, не реже одного раза в 2 года.

* 1. В ходе анализа угроз безопасности информации в ИС в ходе ее эксплуатации осуществляются:
* выявление, анализ и устранение уязвимостей ИС;
* анализ изменения угроз безопасности информации в ИС;
* оценка возможных последствий реализации угроз безопасности информации в ИС.
  + 1. Мероприятия по анализу угроз безопасности информации в ИС администрации района проводятся с периодичностью не реже одного раза в год.
    2. Общий порядок проведения процедур выявления, анализа и устранения уязвимостей, источники получения информации об уязвимостях, периодичность проведения мероприятий по выявлению и анализу уязвимостей, средства для выявления и меры по устранению выявленных уязвимостей, а также перечень лиц, имеющих доступ к функциям выявления (поиска) уязвимостей, должны быть определены в ОРД по защите Информации.
    3. В администрации района периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе их эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации с учетом оценки рисков по результатам оценки возможных последствий реализации угроз безопасности информации в ИС администрации района проводится ответственным за защиту информации в администрации района, уполномоченными сотрудниками администрации района или сотрудниками сторонних организаций, привлекаемых к выполнению работ на договорной основе.
    4. В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.
    5. При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИС, включающие структуру и состав ИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в ИС и в ее отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности ее функционирования.
    6. По результатам анализа изменения угроз безопасности информации в ИС администрации района при необходимости лицами, проводившими анализ изменения угроз безопасности информации, разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации, на основании которых проводятся следующие мероприятия:
* осуществляется актуализация модели угроз безопасности информации: корректировка описания ИС администрации района и их структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации;
* обеспечивается корректировка организационно-распорядительных документов по защите информации.
  + 1. В ходе проведения контроля выполнения мероприятий, проводимых в рамках анализа угроз безопасности информации в ИС, проверяется реализация п. 8.3.1 – 8.3.6 настоящего Положения.
  1. В ходе управления (администрирования) системой ЗИ ИС осуществляются:
* заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;
* управление средствами защиты информации в ИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
* установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
* централизованное управление системой защиты информации ИС (при необходимости);
* регистрация и анализ событий в ИС, связанных с защитой информации;
* информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИС и отдельных средств защиты информации, а также их обучение;
* сопровождение функционирования системы ЗИ ИС в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.
  + 1. В ходе проведения контроля выполнения мероприятий, проводимых в рамках управления (администрирования) системой ЗИ администрации района, проверяется:
* закрепление правил и процедур проведения мероприятий по управлению (администрированию) систем ЗИ ИС администрации района, а также обязанностей уполномоченных лиц по осуществлению мероприятий по управлению (администрированию) систем ЗИ ИС администрации района в соответствующих ОРД по защите информации администрации района и инструкциях уполномоченных лиц;
* реализация правил генерации и смены паролей пользователей, в соответствии с ОРД по защите информации, регламентирующими правила и процедуры идентификации и аутентификации субъектов доступа и объектов доступа в ИС администрации района;
* реализация процедур заведения и удаления учетных записей пользователей, правил разграничения доступом и полномочий пользователей в соответствии с организационно-распорядительными документами, регламентирующими правила и процедуры управлении доступом субъектов доступа к объектам доступа в ИС администрации района;
* актуальность и полнота перечня событий безопасности, подлежащих регистрации;
* поддержание в актуальном состоянии (плановое ведение, своевременное внесение необходимых изменений) эксплуатационной документации на систему ЗИ и ОРД по защите информации.
  + 1. По результатам контроля принимаются необходимые меры по устранению выявленных нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.
  1. В ходе выявления инцидентов и реагирования на них осуществляются:
* определение лиц, ответственных за выявление инцидентов и реагирование на них;
* обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
* своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;
* анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
* планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
* планирование и принятие мер по предотвращению повторного возникновения инцидентов.
  + 1. В ходе проведения контроля выполнения мероприятий, проводимых в рамках реагирования на инциденты, проверяется:
* определение (назначение) лиц, ответственных за осуществление мероприятий по выявлению инцидентов и реагированию на них, закрепление в ОРД по защите информации порядка обнаружения инцидентов и информирования ответственных лиц о возникновении инцидентов безопасности, а также порядок реагирования на инциденты безопасности;
* соблюдение установленного в организационно-распорядительной документации по защите информации порядка обнаружения и реагирования на инциденты безопасности;
* наличие отчетной документации по результатам расследований инцидентов (в случае их обнаружения), планированию и принятию мер по их устранению и предотвращению повторного возникновения.
  1. В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются:
* поддержание конфигурации ИС и ее системы защиты информации в соответствии с эксплуатационной документацией на систему защиты информации;
* определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;
* управление изменениями базовой конфигурации ИС и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;
* анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС;
* определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и ее системы защиты информации;
* внесение информации (данных) об изменениях в базовой конфигурации ИС и ее системы защиты информации в эксплуатационную документацию на систему защиты информации ИС.
  1. В ходе информирования и обучения персонала ИС осуществляются:
* информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС;
* доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;
* обучение персонала ИС правилам эксплуатации отдельных средств защиты информации;
* проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты;
* контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.
  + 1. Мероприятия по обучению персонала и контролю осведомленности персонала должны проводиться с периодичностью не реже одного раза в 2 года.
    2. Контроль выполнения ответственными лицами мероприятий по обучению и контролю осведомленности персонала по вопросам обеспечения защиты информации осуществляется путем проверки ведения Журнала обучения и проверок осведомленности сотрудников администрации района в сфере обработки и защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.
  1. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:
* контроль за событиями безопасности и действиями пользователей в ИС;
* контроль (анализ) защищенности информации, содержащейся в ИС;
* анализ и оценка функционирования системы ЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании системы ЗИ ИС;
* периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
* документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;
* принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС.
  + 1. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС администрации района, осуществляется в рамках контроля выполнения мероприятий по защите информации, предусмотренных Планом мероприятий по защите информации, с периодичность не реже одного раза в 2 года.
    2. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС, проводится администрацией района самостоятельно и (или) с привлечением организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации.
    3. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС администрации района, организуется ответственным за защиту информации, содержащейся в ИС администрации района, и проводится с привлечением (при необходимости) иных сотрудников администрации района.
    4. В ходе проведения контроля за обеспечением уровня защищенности информации, содержащейся в ИС, проводятся проверки реализации мероприятий согласно Плану мероприятий по защите информации.