АДМИНИСТРАЦИЯ НОВОСИБИРСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

05.11.2024 г. **г.Новосибирск** № 2390-па

О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Новосибирского района Новосибирской области

Во исполнение требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях защиты информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), и реализации мер защиты информации, обрабатываемой в информационных системах администрации, администрация Новосибирского района Новосибирской области
ПОСТАНОВЛЯЕТ:

1. Утвердить:

1) Положение по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 1;

2) Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 2;

3) Правила управления доступом субъектов доступа к объектам доступа в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 3;

4) Правила по ограничению программной среды в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 4;

5) Правила обращения с машинными носителями информации в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 5;

6) Правила регистрации событий безопасности в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 6;

7) Правила антивирусной защиты информационных систем администрации Новосибирского района Новосибирской области согласно Приложению 7;

8) Правила контроля (анализа) защищенности информации в информационных системах администрации Новосибирского района Новосибирской области согласно Приложению 8;

9) Правила обеспечения целостности и доступности информационных систем и информации в администрации Новосибирского района Новосибирской

области согласно Приложению 9;

10) Регламент выявления инцидентов безопасности и реагированию на них в администрации Новосибирского района Новосибирской области согласно Приложению 10;

11) Положение по управлению конфигурацией информационных систем администрации Новосибирского района Новосибирской области согласно Приложению 11;

12) Положение по защите информации в администрации Новосибирского района Новосибирской области при выводе из эксплуатации информационных систем или после принятия решения об окончании обработки информации ограниченного доступа согласно Приложению 12.

2. Заместителю главы администрации - начальнику управления организационно-контрольной работы администрации Новосибирского района Новосибирской области Полевой И.А. ознакомить уполномоченных работников администрации Новосибирского района Новосибирской области с настоящим постановлением.

3. Контроль за исполнением постановления возложить на заместителя главы администрации - начальника управления организационно-контрольной работы администрации Новосибирского района Новосибирской Полевую И.А.

Глава района А.Г.Михайлов

Д.В.Макогонов
373 45 99

ПРИЛОЖЕНИЕ № 1
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Новосибирского района Новосибирской области (далее – Положение), разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Целью разработки настоящего Положения является определение порядка организации и проведения работ по обеспечению безопасности информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация) на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

1. Термины и определения

1.1. В настоящем Положении используются следующие термины и их определения:

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

– **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

– **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

– **обработка информации** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств

автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение информации;

– **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– **технические средства информационной системы** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, аппаратные средства защиты информации;

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

– **уничтожение информации** – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации;

– **уровень защищенности персональных данных** – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах;

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

2. Порядок организации и проведения работ по обеспечению безопасности информации

2.1. Под организацией обеспечения безопасности информации, обрабатываемой в ИС администрации, понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее – система ЗИ).

2.2. Система ЗИ включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности информации, уровня защищенности информации (в том числе персональных данных), который необходимо обеспечить, класса информационной системы и информационных технологий, используемых в ИС.

2.3. Защита информации, содержащейся в ИС, обеспечивается путем выполнения требований к организации и мерам защиты информации, содержащейся в ИС.

2.4. Для обеспечения защиты информации, содержащейся в ИС,

администрации назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации (далее – Ответственный), содержащейся в ИС.

2.5. Для обеспечения выполнения мер, предусмотренных законодательством Российской Федерации в области персональных данных, администрации назначается ответственный за организацию обработки персональных данных.

2.6. Для обеспечения соблюдения условий использования средств криптографической защиты информации (при их использовании) администрации назначается ответственный за эксплуатацию средств криптографической защиты информации в администрации.

2.7. Для проведения работ по защите информации в ходе создания и эксплуатации ИС обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

2.8. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

2.9. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

2.10. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в ИС, в рамках системы (подсистемы) защиты ИС.

2.11. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации ИС, в зависимости от информации, содержащейся в ИС, целей создания ИС и задач, решаемых этой ИС, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);
- неправомерного блокирования информации (обеспечение доступности информации).

2.12. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИС;
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации (форма оценки эффективности и документов, разрабатываемых по результатам оценки эффективности, принимается администрацией самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности информации) и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации ИС;
- обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

3. Формирование требований к защите информации, содержащейся в информационных системах

3.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется администрацией;

3.2. Формирование требований к защите информации, содержащейся в ИС, включает:

- принятие решения о необходимости защиты информации, содержащейся в ИС;
- определение уровня защищенности персональных данных при их обработке в ИС и (или) классификацию ИС по требованиям защиты информации;
- определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;
- определение требований к системе ЗИ ИС.

3.3. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

- анализ целей создания ИС и задач, решаемых этой ИС;
- определение информации, подлежащей обработке в ИС;
- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;
- принятие решения о необходимости создания системы ЗИ ИС, а также определение целей и задач защиты информации в ИС, основных этапов создания системы ЗИ ИС и функций по обеспечению защиты информации, содержащейся в ИС, оператора и уполномоченных лиц.

3.4. Результаты определения уровня защищенности персональных данных при их обработке в ИС оформляются актом. Результаты классификации ИС оформляются актом классификации.

3.5. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа

возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

3.6. Требования к системе ЗИ ИС определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

4. Разработка системы защиты информации информационной системы

4.1. Разработка системы ЗИ ИС организуется администрацией.

4.2. Разработка системы ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС и включает:

- проектирование системы защиты информации ИС;
- разработку эксплуатационной документации на систему ЗИ ИС;
- макетирование и тестирование системы ЗИ ИС (при необходимости).

4.3. Система ЗИ ИС не должна препятствовать достижению целей создания ИС и ее функционированию.

4.4. При разработке системы ЗИ ИС учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

4.5. При проектировании системы ЗИ информационной системы:

- определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты;
- определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в ИС;
- выбираются меры защиты информации, подлежащие реализации в системе ЗИ ИС;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
- определяется структура системы ЗИ ИС, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС;
- определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации;
- определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

4.6. Результаты проектирования системы ЗИ ИС отражаются в проектной документации на систему ЗИ ИС.

4.7. Разработка эксплуатационной документации на систему ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС.

4.8. При макетировании и тестировании системы ЗИ ИС в том числе осуществляются:

- проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;
- проверка выполнения выбранными средствами защиты информации требований к системе защиты информации ИС;
- корректировка проектных решений, разработанных при создании ИС и (или) системы защиты информации ИС.

5. Внедрение системы защиты информации информационной системы

5.1. Внедрение системы ЗИ ИС организуется администрацией.

5.2. Внедрение системы ЗИ ИС осуществляется в соответствии с проектной и эксплуатационной документацией на систему ЗИ ИС и в том числе включает:

- установку и настройку средств защиты информации в ИС;
- разработку документов, определяющих правила и процедуры, реализуемые администрацией для обеспечения защиты информации в ИС в ходе ее эксплуатации;
- внедрение организационных мер защиты информации;
- предварительные испытания системы ЗИ ИС;
- опытную эксплуатацию системы ЗИ ИС;
- анализ уязвимостей ИС и принятие мер защиты информации по их устранению;
- приемочные испытания системы ЗИ ИС.

5.3. Установка и настройка средств защиты информации в ИС должна проводиться в соответствии с эксплуатационной документацией на систему ЗИ ИС и документацией на средства защиты информации.

5.4. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- управления (администрирования) системой ЗИ ИС;
- выявления инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации, и реагирования на них;
- управления конфигурацией ИС и системы ЗИ ИС;
- контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

- защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

5.5. При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;
- проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и ответственных лиц по реализации организационных мер защиты информации;
- отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

5.6. Предварительные испытания системы ЗИ ИС включают проверку работоспособности системы ЗИ ИС, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС.

5.7. Опытная эксплуатация системы ЗИ ИС включает проверку функционирования системы ЗИ ИС, в том числе реализованных мер ЗИ, а также готовность пользователей и ответственных лиц к эксплуатации системы ЗИ ИС.

5.8. Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем системы ЗИ ИС и предотвращения реализации угроз безопасности информации. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ИС.

5.9. Приемочные испытания системы ЗИ ИС включают проверку выполнения требований к системе ЗИ ИС в соответствии с техническим заданием на создание системы ЗИ ИС.

6. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации

6.1. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации организуется администрацией и включает проведение комплекса организационных и технических мероприятий, в результате которых подтверждается соответствие системы ЗИ ИС требованиям по безопасности информации.

6.2. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации проводится администрацией самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

6.3. По решению администрации оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы в

соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6.4. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, техническое задание на создание системы ЗИ ИС, проектная и эксплуатационная документация на систему ЗИ ИС, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний системы ЗИ ИС. Аттестат соответствия выдается на весь срок эксплуатации ИС.

6.5. В ходе эксплуатации ИС администрация должна обеспечивать поддержку соответствия системы защиты информации аттестату соответствия в рамках реализации мероприятий по защите информации, предусмотренных пунктом 8 настоящего Положения.

7. Обеспечение защиты информации в ходе эксплуатации информационной системы

7.1. Обеспечение защиты информации в ходе эксплуатации ИС осуществляется администрацией 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;
- управление (администрирование) системой 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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.

8. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

8.1. Мероприятия по выводу ИС из эксплуатации включают:

подготовку документов, связанных с выводом ИС из эксплуатации;

работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на программное обеспечение ИС, демонтажу и списанию технических средств ИС (при необходимости), обеспечению хранения и дальнейшего использования информационных ресурсов ИС;

обеспечение защиты информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

8.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности администрации.

8.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

8.4. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации осуществляется в соответствии с эксплуатационной документацией на систему ЗИ ИС и организационно-распорядительными документами по защите информации.

8.5. В ходе проведения контроля выполнения мероприятий по защите Информации при выводе из эксплуатации ИС администрации или после принятия решения об окончании обработки информации, проверяется документальное оформление процедур, предусмотренных организационно-распорядительными документами по защите информации, регламентирующими вышеназванные мероприятия, а также соблюдение требований законодательства об архивном деле в Российской Федерации.

ПРИЛОЖЕНИЕ № 1
к Положению по организации
и проведению работ по обеспечению
безопасности информации, обрабатываемой
в информационных системах
администрации Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па – что это?

ПЛАН МЕРОПРИЯТИЙ
по защите информации в информационных системах администрации Новосибирского района Новосибирской области

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
1.	Анализ угроз безопасности информации в ИС в ходе их эксплуатации		
1.1.	Выявление, анализ и устранение уязвимостей ИС	Не реже одного раза в год	Уполномоченные сотрудники администрации, ответственный за защиту информации, содержащейся в ИС администрации (далее – ответственный за защиту информации)
1.2.	Анализ изменения угроз безопасности информации в ИС	Не реже одного раза в год	
1.3.	Оценка возможных последствий реализации угроз безопасности информации в ИС	В случае выявления новых угроз безопасности	
2.	Управление (администрирование) системой ЗИ ИС		
2.1.	Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.2.	Управление средствами защиты информации ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.3.	Управление обновлениями программных и программно-аппаратных средств, в том числе средств ЗИ	По мере выхода обновлений, с учетом особенностей функционирования ИС	Уполномоченные сотрудники администрации
2.4.	Централизованное управление системой ЗИ ИС (при необходимости)	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.5.	Мониторинг и анализ зарегистрированных событий в ИС, связанных с обеспечением безопасности информации	Постоянно в ходе эксплуатации ИС	Уполномоченный сотрудник администрации
2.6.	Обеспечение функционирования систем ЗИ ИС в ходе их эксплуатации, включая ведение эксплуатационной документации и	Постоянно в ходе эксплуатации ИС	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	организационно-распорядительных документов по защите информации		
3.	Управления конфигурацией ИС и их системами ЗИ		
3.1.	Определение компонентов ИС и их систем ЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю	При создании системы ЗИ ИС, далее при необходимости в случае изменения состава объектов управления конфигурацией	администрация
3.2.	Управление изменениями ИС и их системами ЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в ИС и их систему защиты информации	При создании системы ЗИ ИС и далее при необходимости в ходе эксплуатации ИС	Ответственный за защиту информации
3.3.	Контроль и документирование действий по внесению изменений в ИС и их системы защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
4.	Реагирование на инциденты		
4.1.	Обнаружение инцидентов (в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа,	Постоянно в ходе эксплуатации ИС	Сотрудники администрации (пользователи ИС и уполномоченные ответственные лица)

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов)		
4.2.	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС	Постоянно в ходе эксплуатации ИС	Сотрудники администрации (пользователи ИС и уполномоченные ответственные лица)
4.3.	Идентификация и анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	При возникновении инцидентов безопасности	Уполномоченные сотрудники администрации, ответственный за защиту информации (в пределах своих полномочий в зависимости от характера инцидента)
4.4.	Планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и их 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	При возникновении инцидентов безопасности	Уполномоченные ответственные лица администрация (в пределах своих полномочий в зависимости от характера инцидента)
4.5.	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	При возникновении инцидентов безопасности	
5.	Информирование и обучение персонала ИС по вопросам защиты информации		
5.1.	Информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС	Не реже одного раза в 2 года	Ответственный за защиту информации
5.2.	Доведение до персонала ИС требований по защите	Не реже одного раза в 2 года.	Ответственный за организацию обработки

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	информации, а также положений организационно-распорядительных документов по защите информации	В случае изменения нормативной правовой базы, локальных актов администрации в области защиты информации обучение сотрудников должно быть проведено не позднее одного месяца с момента изменений	персональных данных и ответственный за защиту информации (в пределах своих полномочий)
5.3.	Обучение персонала ИС правилам эксплуатации средств защиты информации от несанкционированного доступа и средств антивирусной защиты	При создании системы защиты информации ИС и далее при необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
5.4.	Проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты	Не реже одного раза в 2 года	Ответственный за защиту информации, уполномоченные сотрудники администрация
5.5.	Контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
6.	Мероприятия по защите информации, проводимые в целях обеспечения и поддержания уровня защищенности информации, содержащейся в ИС		
6.1.	Установка обновлений программного обеспечения (ПО) (общесистемного, прикладного, программных СЗИ), в том числе проверка обновлений баз средств защиты информации (для средств антивирусной защиты и средств анализа защищенности)	В автоматическом режиме при выпуске производителем новой версии ПО либо вручную (при наличии обновлений) не реже одного раза в 3 месяца	Уполномоченные сотрудники администрация (в пределах своих полномочий)
6.2.	Обеспечение работоспособности, правильности функционирования и параметров настройки программного обеспечения и средств защиты информации	Постоянно в ходе эксплуатации ИС	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.3.	Контроль состава технических	Не реже одного раза в	Ответственный за защиту

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	средств, программного обеспечения и средств защиты информации	год	информации
6.4.	Соблюдение установленных правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.5.	Учет и сохранность технической и эксплуатационной документации на технические и программные средства, применяемые в ИС	В процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации
6.6.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за организацию обработки персональных данных и ответственный за защиту информации
6.7.	Учет средств защиты информации, эксплуатационной и технической документации к ним (при необходимости)	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники администрации, ответственный за защиту информации, ответственный за эксплуатацию средств криптографической защиты СКЗИ (в пределах своих полномочий)
6.8.	Учёт машинных носителей информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации
6.9.	Обеспечение безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Непрерывно в процессе эксплуатации ИС и при необходимости в случае возникновения нарушений в функционировании технических средств	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.10.	Поддержание работоспособности средств	Непрерывно в процессе эксплуатации	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
	резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий	ИС	
6.11.	Проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов)	В автоматическом режиме в соответствии с установленным расписанием и вручную по требованию	Пользователи ИС, уполномоченные сотрудники администрации (в пределах своих полномочий)
6.12.	Проверка расположения средств отображения информации	Не реже одного раза в год	Ответственный за защиту информации
6.13.	Документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС	По результатам проведения контроля за обеспечением уровня защищенности информации, содержащейся в ИС	Ответственный за защиту информации
6.14.	Принятие решения о необходимости доработки (модернизации) системы защиты информации		администрация
7.	Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации		
7.1.	Архивирование информации, содержащейся в ИС	При необходимости дальнейшего использования информации в деятельности ГБУ НСО «ЦЗИ НСО»	Ответственный за защиту информации, уполномоченные сотрудники администрация (в пределах своих полномочий)
7.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации	При необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации	Ответственный за защиту информации
7.3.	Физическое уничтожение машинных носителей остаточной информации	При выводе из эксплуатации машинных носителей информации	Ответственный за защиту информации

ПРИЛОЖЕНИЕ № 2
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

ПРАВИЛА
идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер защиты информации по идентификации и аутентификации субъектов доступа к объектам доступа в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор).

1.2. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1 При доступе в ИС администрация должна осуществляться идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

2.2 К внутренним пользователям относятся сотрудники администрация, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС администрации в соответствии с должностными регламентами (инструкциями), утвержденными в администрации, и которым в ИС присвоены учетные записи.

2.3 В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, уполномоченного лица и (или) оператора иной ИС, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с заключенными соглашениями и организационно-распорядительными документами администрации.

2.4 Для каждого внутреннего пользователя в ИС администрации должны быть заведены учетные записи.

2.5 Пользователи ИС администрации должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

2.6 Аутентификация пользователей в ИС администрации должна осуществляться с использованием паролей. Также могут применяться аппаратные средства в случае многофакторной аутентификации.

2.7 В ИС администрации должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

3. **Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов**

3.1 В ИС администрации должны быть реализованы следующие функции управления идентификаторами пользователей и устройств:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;
- блокирование идентификатора пользователя через установленный период времени неиспользования.

3.2 Создание, присвоение и уничтожение идентификаторов пользователей и устройств осуществляют уполномоченные сотрудники администрации.

4. **Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации**

4.1. В ИС администрации должны быть реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации ИС;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации) с последующей сменой пользователями начальной аутентификационной информации;
- установление характеристик пароля: длина пароля не менее восьми символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- обновление аутентификационной информации (замена средств аутентификации) с установленной периодичностью не более, чем через 120 дней;

- защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

4.2. В случае утраты и (или) компрометации личного пароля пользователя ИС администрации должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- внеплановая смена (сброс) личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться уполномоченными сотрудниками администрации после окончания последнего сеанса работы данного пользователя с системой;
- внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) лиц, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС администрация.

4.3. Управление средствами аутентификации (аутентификационной информацией) пользователей ИС и принятие мер в случае утраты и (или) компрометации средств аутентификации (аутентификационной информации) осуществляют уполномоченные сотрудники администрации.

4.4. Руководители структурных подразделений администрации должны обеспечить своевременное доведение информации о прекращении полномочий пользователей ИС до уполномоченных сотрудников администрации.

5. **Защита обратной связи при вводе аутентификационной информации**

5.1. В ИС администрации должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

5.2. Защита обратной связи «система – субъект доступа» в процессе аутентификации должна обеспечиваться исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

6. **Ответственность при организации идентификации и аутентификации**

6.1. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

6.2. Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 3
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

ПРАВИЛА
управления доступом субъектов доступа к объектам доступа в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация) по управлению доступом субъектов доступа к объектам доступа в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор).

1.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в ИС правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

2. Управление учетными записями пользователей

2.1 В ИС администрация должны быть реализованы следующие функции управления учетными записями пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная);
- объединение учетных записей в группы (при необходимости);
- верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с установленной периодичностью (не реже 1 раза в год);
- регламентирование порядка заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей,

предоставленных для однократного выполнения задач в ИС;

- предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС.

2.2 Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИС).

2.3 По истечении установленного срока использования временных учетных записей должно осуществляться автоматическое блокирование временных учетных записей пользователей.

2.4 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей ИС администрации осуществляют уполномоченные сотрудники администрации.

3. Правила разграничения доступа

3.1 В зависимости от особенностей функционирования ИС, с учетом угроз безопасности информации в ИС администрации реализуется один или комбинация следующих методов управления доступом:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа - списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
- ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

3.2 Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

3.3 Оператором должно обеспечиваться разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями (функциями), и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей). Соответствие ролей и функций, выполняемых персоналом, представлено в таблице 1.

Роли и функции персонала, обслуживающего и эксплуатирующего ИС

о 12 пункту выбираем в нмцк минимально предложенную цену

№ п/п	Роль	Уровень доступа	Основные функции
1.	Ответственный за организацию обработки персональных данных	Доступ на правах пользователя к информации, техническим средствам, программному обеспечению, средствам защиты информации. Без доступа на изменение параметров средств защиты информации, программного обеспечения, технических средств	осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных; доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов
2.	Ответственный за защиту информации (обеспечение безопасности персональных данных)	Доступ на правах администратора к средствам защиты информации, на правах пользователя к информации, техническим средствам, программному обеспечению. Без доступа на изменение параметров программного обеспечения, технических средств	организация и обеспечение выполнения требований по защите информации в процессе ее обработки в ИС; планирование и организация контроля мероприятий по защите информации в ИС; обеспечение анализа угроз безопасности информации в ИС; информирование и обучение пользователей ИС об актуальных угрозах безопасности информации, по вопросам обеспечения защиты информации и правилам безопасной эксплуатации ИС; контроль осведомленности пользователей ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации; обнаружение и реагирование на инциденты, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации, и реагирование на них; ведение, пересмотр и доработка документации в области защиты информации, предусмотренной локальными актами администрации; контроль соблюдения правил разграничения доступа; управление (администрирование) системой

№ п/п	Роль	Уровень доступа	Основные функции
			защиты информации ИС; контроль работоспособности (контроль неотключения) и правильности функционирования СЗИ; обеспечение установки обновлений программного обеспечения СЗИ, обеспечение выполнения и контроль результатов выполнения задач обновления баз данных СЗИ; проведение инструктажа персонала по правилам работы с отдельными СЗИ; контроль аппаратной конфигурации защищаемых технических средств (АРМ, серверов) и предотвращение попытки ее несанкционированного изменения
3.	Администратор ИС	Доступ на правах администратора к техническим средствам, программному обеспечению. Без доступа на изменение параметров средств защиты информации	установка, модернизация, настройка и мониторинг работоспособности системного, базового и прикладного программного обеспечения; конфигурирование и управление программным обеспечением и оборудованием ИС; модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций)
4.	Ответственный за выявление инцидентов и реагирование на них	Доступ на правах администратора к средствам защиты информации. Без доступа на изменение к информации, техническим средствам, программному обеспечению	выявление (поиск) уязвимостей ИС администрации с использованием средств анализа (контроля) защищенности (сканеров безопасности); обнаружение и идентификация инцидентов; анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий; планирование и принятие мер по устранению инцидентов; планирование и принятие мер по предотвращению повторного возникновения инцидентов
5.	Ответственный за эксплуатацию средств криптографической защиты информации (СКЗИ)	Доступ на правах пользователя к информации, техническим средствам, прикладному программному обеспечению, средствам защиты информации. Без	поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и локальными актами администрации; учет пользователей криптосредств; надежное хранение эксплуатационной и

№ п/п	Роль	Уровень доступа	Основные функции
		доступа на изменение параметров средств защиты информации, программного обеспечения, технических средств	технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств; проведение расследований и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; разработка и принятие мер по предотвращению возможных негативных последствий нарушений
6.	Пользователь информационной системы	Доступ на правах пользователя к информации, техническим средствам, программному обеспечению, средствам защиты информации. Без доступа на изменение параметров настройки средств защиты информации, программного обеспечения, технических средств	доступ к техническим средствам ИС, программному обеспечению, защищаемой информации (персональным данным); обработка защищаемой информации (персональных данных)

3.4 В ИС администрации должно осуществляться ограничение количества неуспешных попыток входа в ИС (доступа к ИС), а также обеспечиваться блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИС (доступа к ИС) на установленный период времени.

3.5 В ИС администрации должно обеспечиваться блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в ИС или по запросу пользователя ИС.

3.6 Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из ИС).

3.7 Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

3.8 Блокирование сеанса доступа пользователя в ИС должно сохраняться до прохождения им повторной идентификации.

3.9 Пользователям ИС запрещены любые действия до прохождения ими процедур идентификации и аутентификации (кроме необходимых для прохождения процедур идентификации и аутентификации).

4. Управление информационными потоками

4.1 В ИС администрации должно осуществляться управление информационными потоками, обеспечивающее разрешенный (установленный) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между ИС или при взаимодействии с сетью «Интернет» (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

4.2 Управление информационными потоками должно блокировать передачу защищаемой информации через сеть «Интернет» (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС.

5. Правила удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

5.1 В ИС администрации должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

5.2 Защита удаленного доступа должна обеспечиваться для всех видов доступа и включает:

- ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим;
- предоставление удаленного доступа только тем лицам, которым он необходим для осуществления технической поддержки на основании договора;
- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;
- контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации);

- использование ограниченного (минимально необходимого) количества точек подключения к ИС при организации удаленного доступа к объектам доступа ИС;
- исключение удаленного доступа от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

6. **Управление взаимодействием с информационными системами сторонних организаций (внешними ИС)**

6.1 Управление взаимодействием ИС администрации с внешними ИС должно включать в себя определение порядка обработки, хранения и передачи информации с использованием внешних ИС.

6.2 Оператор разрешает обработку, хранение и передачу информации с использованием внешней ИС при выполнении следующих условий:

- при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
- при наличии подтверждения выполнения во внешней ИС предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

7. **Ответственность**

7.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

7.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение
к Правилам управления доступом
субъектов доступа к объектам
доступа в информационных системах
администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

Матрица доступа
субъектов доступа по отношению к защищаемым информационным ресурсам информационных систем администрации Новосибирского района Новосибирской области

Настоящий документ разработан в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17, и устанавливает полномочия субъектов доступа по доступу к защищаемым информационным ресурсам информационных систем (далее – ИС) администрации Новосибирского района Новосибирской области (администрации). Предоставление пользователям прав доступа к объектам доступа информационных систем осуществляется на основании задач, решаемых пользователями в ИС администрации и взаимодействующими с ними информационными системами.

В ИС администрации для управления доступом используются дискреционный и ролевой методы управления доступом.

В ИС администрации обеспечено разделение полномочий (ролей) субъектов доступа ИС, и определены роли пользователей в соответствии с минимально необходимыми правами и привилегиями:

1) Пользователь – имеет непривилегированный доступ к ресурсам АРМ ИС и средствам защиты информации, разрешены действия (операции) по обработке информации в ИС с использованием технологии локального доступа, без права управления (администрирования) ИС и системы защиты ИС;

2) Администратор ИБ – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) системой защиты ИС);

3) Администратор ИС – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) ИС, без права управления (администрирования) средствами защиты информации).

Перечень категорий лиц, имеющих доступ к информационным ресурсам администрации с указанием их роли приведен в таблице 1.

Табло 12 пункту выбираем в нмцк минимально предложенную цену

№	Категория лиц	Роль

п/п		
1.	Сотрудники администрации (пользователи ИС)	Пользователь
2.	Уполномоченный сотрудник администрации	Администратор ИБ
3.	Уполномоченные сотрудники администрации	Администратор ИС

Для субъектов доступа ИС администрации установлены разрешения согласно таблице 2.

Таблица 2 – Разрешения, установленные для субъектов доступа

Разрешения	Разрешить	Запретить
Администратор ИБ/Администратор ИС		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений	+	
Смена владельца	+	
Печать	+	
Управление принтерами	+	
Управление документами	+	
Пользователь		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений		+
Смена владельца		+
Печать	+	
Управление принтерами		+

Управление документами	+	

Наличие доступа к объектам ИС администрации в зависимости от полномочий (роли) отражено в таблице 3.

Таблица 3 – Наличие доступа к объектам ИС администрации

Объект доступа	Роль		
	Администратор ИС	Администратор ИБ	Пользователь
Устройства			
Автоматизированное рабочее место (АРМ)	+	+	+
Сетевое и коммутационное оборудование	+	+	–
Съемные машинные носители (CD/DVD, флеш-накопители и т.д.)	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+
Объекты файловой системы			
Жесткий диск, личный каталог	+	+	+
Жесткий диск, служебные (в том числе системные) каталоги	+	+	–
Запускаемые и исполняемые модули			
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно участвующего в обработке персональных данных	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+ (без права конфигурирования компонентов ИС)
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно не участвующего в обработке персональных данных	+	+	+

Приложение
к Правилам управления доступом
субъектов доступа к объектам
доступа в информационных системах
администрации
Новосибирского района
Новосибирской области
от 05.11.2014 № 2390-па

Матрица доступа
субъектов доступа по отношению
к защищаемым информационным ресурсам
информационных систем
администрации Новосибирского района
Новосибирской области

Настоящий документ разработан в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17, и устанавливает полномочия субъектов доступа по доступу к защищаемым информационным ресурсам информационных систем (далее – ИС) администрации Новосибирского района Новосибирской области (администрации). Предоставление пользователям прав доступа к объектам доступа информационных систем осуществляется на основании задач, решаемых пользователями в ИС администрации и взаимодействующими с ними информационными системами.

В ИС администрации для управления доступом используются дискреционный и ролевой методы управления доступом.

В ИС администрации обеспечено разделение полномочий (ролей) субъектов доступа ИС, и определены роли пользователей в соответствии с минимально необходимыми правами и привилегиями:

1) Пользователь – имеет непривилегированный доступ к ресурсам АРМ ИС и средствам защиты информации, разрешены действия (операции) по обработке информации в ИС с использованием технологии локального доступа, без права управления (администрирования) ИС и системы защиты ИС;

2) Администратор ИБ – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) системой защиты ИС);

3) Администратор ИС – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) ИС, без права управления (администрирования) средствами защиты информации).

Перечень категорий лиц, имеющих доступ к информационным ресурсам администрации с указанием их роли приведен в Таблице 1.

Таблица 1 – Перечень категорий лиц

№ п/п	Категория лиц	Роль
1.	Сотрудники администрации (пользователи ИС)	Пользователь
2.	Уполномоченный сотрудник администрации	Администратор ИБ
3.	Уполномоченные сотрудники администрации	Администратор ИС

Для субъектов доступа ИС администрации установлены разрешения согласно Таблице 2.

Таблица 2 – Разрешения, установленные для субъектов доступа

Разрешения	Разрешить	Запретить
Администратор ИБ/Администратор ИС		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений	+	
Смена владельца	+	
Печать	+	
Управление принтерами	+	
Управление документами	+	
Пользователь		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений		+
Смена владельца		+
Печать	+	

Управление принтерами		+
Управление документами	+	

Наличие доступа к объектам ИС администрации в зависимости от полномочий (роли) отражено в Таблице 3.

Таблица 3 – Наличие доступа к объектам ИС администрации

Объект доступа	Роль		
	Администратор ИС	Администратор ИБ	Пользователь
Устройства			
Автоматизированное рабочее место (АРМ)	+	+	+
Сетевое и коммутационное оборудование	+	+	–
Съемные машинные носители (CD/DVD, флеш-накопители и т.д.)	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+
Объекты файловой системы			
Жесткий диск, личный каталог	+	+	+
Жесткий диск, служебные (в том числе системные) каталоги	+	+	–
Запускаемые и исполняемые модули			
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно участвующего в обработке персональных данных	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+ (без права конфигурирования компонентов ИС)
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно не участвующего в обработке персональных данных	+	+	+

Приложение № 4
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

Правила по ограничению программной среды в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер защиты информации по ограничению программной среды в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор).

1.2. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в ИС программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в ИС программного обеспечения.

2. Установка (инсталляция) только разрешенного к использованию программного обеспечения и его компонентов

2.1. Установка (инсталляция) в ИС администрации программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов должна осуществляться с учетом Перечня программного обеспечения, разрешенного к установке в информационных системах администрации («белый список»).

2.2. Установка (инсталляция) в ИС программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора.

2.3. В ИС администрации должен обеспечиваться периодический контроль установленного (инсталлированного) программного обеспечения на предмет соответствия его Перечню программного обеспечения, разрешенному к установке, а также на предмет соответствия его Перечню программного обеспечения, разрешенного к использованию в информационных системах администрации Новосибирского района Новосибирской области, а также на предмет отсутствия программного обеспечения, запрещенного в ИС администрации.

2.4. Пересмотр Перечня программного обеспечения, разрешенного к использованию в информационных системах администрации, может осуществляться на основании заявки пользователя, согласованной с непосредственным руководителем пользователя.

3. Ответственность

3.1. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

3.2. Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством РФ.

Приложение № 3
к Правилам по ограничению
программной среды в
информационных системах
администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па.

ФОРМА

Перечень программного обеспечения и (или) его компонентов, разрешенного к установке в информационных системах администрации Новосибирского района Новосибирской области

№ п/п	Наименование	Назначение
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		

Приложение № 5
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 №3390-па.

ПРАВИЛА
обращения с машинными носителями информации в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер по защите машинных носителей информации (персональных данных), используемых в информационных системах (далее – ИС) администрации (далее – администрация оператор).

1.2. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

1.3. В качестве машинных носителей информации в настоящих Правилах рассматриваются:

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);
- мобильные технические средства: съемные машинные носители информации (флэш-накопители, CD, внешние накопители на жестких дисках и иные устройства).

1.4. Под использованием машинных носителей информации в ИС администрация понимается их подключение к инфраструктуре ИС администрация с целью обработки, приема/передачи информации между ИС и носителями информации.

2. Использование машинных носителей информации

2.1. В ИС администрации для обработки защищаемой информации допускается использование только учтенных машинных носителей информации, которые являются собственностью администрации и подвергаются регулярной ревизии и контролю.

2.2. При использовании сотрудниками машинных носителей информации необходимо:

- использовать машинные носители информации исключительно для выполнения своих служебных обязанностей;

- бережно относиться к машинным носителям информации;
- обеспечивать физическую безопасность машинных носителей информации;
- извещать ответственного за защиту информации о фактах утраты (кражи) машинных носителей информации;
- перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ.

2.3. При использовании машинных носителей информации запрещено:
- использовать машинные носители информации в личных целях;
- передавать носители информации третьим лицам;
- оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;
- выносить без предварительного согласования с руководителем соответствующего подразделения машинные носители информации из служебных помещений для работы с ними на дому и т. д.

2.4. Ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

3. Защита применяемых в информационных системах мобильных технических средств.

3.1. Защита мобильных технических средств (съемных машинных носителей информации) включает реализацию следующих мер:
- контроль использования в ИС мобильных технических средств информации;
- реализация в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации, управлению доступом, ограничению программной среды, защите машинных носителей информации, регистрации событий безопасности, антивирусной защите, контролю (анализу) защищенности, обеспечению целостности;
- уничтожение съемных машинных носителей информации, которые не подлежат очистке;
- выборочные проверки съемных машинных носителей информации (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);
- запрет возможности автоматического запуска (без команды пользователя) в ИС программного обеспечения на съемных машинных носителях информации.

3.2. Контроль использования мобильных технических средств в ИС а включает:
- использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с настоящими Правилами;

- ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

4. Учет и хранение машинных носителей информации

4.1. В администрации учету подлежат следующие машинные носители информации, используемые в ИС для обработки и хранения защищаемой информации (персональных данных):
- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации;
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

4.2. На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать (регистрационный номер носителя).

4.3. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

4.4. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства ИС нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

4.5. Учет машинных носителей информации (персональных данных), используемых в информационных системах администарции, ведется в соответствующем журнале учета машинных носителей информации (далее – Журнал учета) по форме, приведенной в Приложении № 1 к настоящим Правилам.

4.6. Регистрационные или иные номера подлежат занесению в Журнал учета или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

4.7. При поступлении нового машинного носителя информации, который будет использоваться в ИС администрации, носитель регистрируется в Журнале учета. Перед использованием новый машинный носитель информации в обязательном

порядке должен пройти антивирусную проверку (при наличии технической возможности).

4.8. В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные машинные носители информации изымаются.

4.9. Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

4.10. Необходимо осуществлять хранение отчуждаемых машинных носителей персональных данных в сейфах (металлических шкафах, персональных хранилищах), оборудованных внутренними замками, либо иным образом обеспечить условия хранения машинных носителей информации, исключающие несанкционированный к ним доступ.

5. Управление доступом к машинным носителям информации

5.1. Управление доступом к машинным носителям информации, используемым в ИС администрации должно осуществляться ответственным за защиту информации.

5.2. В администрации должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в ИС:

- определен перечень лиц, имеющих физический доступ к машинным носителям информации;
- физический доступ к машинным носителям информации должен предоставляться только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

6. Контроль перемещения машинных носителей информации за пределы контролируемой зоны

6.1. В ИС администрация должна обеспечиваться контроль перемещения используемых машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

- определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;
- предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);
- учет перемещения машинных носителей информации;
- периодическая проверка наличия машинных носителей информации.

6.2. При передаче средств вычислительной техники (далее – СВТ) ИС администрация в сторонние организации для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ, либо осуществляется предварительное уничтожение (стирание) информации, содержащейся на несъемном машинном носителе информации.

7. Уничтожение (стирание) информации на машинных носителях, уничтожение машинных носителей информации, а также контроль уничтожения (стирания) информации

7.1. В администрации должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

7.2. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации (при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации) и обеспечиваться с использованием специального программного обеспечения, гарантирующего уничтожение информации.

7.3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

7.4. В ИС администрации должны использоваться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

7.5. В случае утраты машинных носителей информации немедленно ставится в известность руководитель соответствующего структурного подразделения и ответственный за защиту информации. На утраченные носители информации составляется Акт утраты машинных носителей информации (в соответствии с формой, представленной в Приложении № 2 к настоящим Правилам). Соответствующие отметки вносятся в Журнал учета.

7.6. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, должны быть уничтожены без возможности восстановления (путем физического разрушения или сильной деформации носителя) с составлением Акта уничтожения машинных носителей информации (в соответствии с формой, представленной в Приложении № 3 к настоящим Правилам) и регистрацией в Журнале учета.

7.7. При необходимости дальнейшего использования информации в деятельности администрация должно осуществляться архивирование информации, хранящейся на машинном носителе, подлежащем уничтожению.

7.8. Ответственный за защиту информации обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесения соответствующей информации в Журнал учета

8. Ответственность

8.1. Ответственность за выполнение правил эксплуатации машинных носителей информации несут пользователи ИС администрации.

8.2. Контроль выполнения установленных правил эксплуатации, регистрации и учёта машинных носителей информации осуществляет ответственный за защиту информации.

8.3. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

8.4. Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение № 1
к Правилам обращения с машинными носителями информации в информационных системах администрации Новосибирского района Новосибирской области
от 05.11.2024 № 3390-па

ФОРМА

ЖУРНАЛ
учета машинных носителей информации, используемых в информационных системах администрации Новосибирского района Новосибирской области

Журнал начат «____» _____ 20 ___ г.
Журнал завершен «____» _____ 20 ___ г.
Журнал составлен на листах

№ п/п	Тип машинного носителя информации	Регистрационный (учетный) номер машинного носителя информации	Ф.И.О., подпись получателя, дата, и место хранения машинного носителя информации	Ф.И.О., подпись сдавшего, дата	Ф.И.О., подпись принявшего, дата, и место хранения машинного носителя информации	Дата и номер акта об уничтожении/ акта утраты	Примечание
1	2	3	4	5	6	7	8
2							
3							
4							

Приложение № 2
к Правилам обращения с машинными носителями информации
в информационных системах
администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

ФОРМА

Акт
утраты машинных носителей информации

Комиссия в составе:

(должность, ФИО)

(должность, ФИО)

(должность, ФИО)

составила настоящий Акт об утрате нижеуказанных машинных носителей информации:

№ п/п	Тип машинного носителя информации	Учетный номер машинного носителя информации	Примечание

Всего машинных носителей

(цифрами и прописью)

Носители были утеряны при следующих обстоятельствах:

Отметка об утере внесена в Журнал учета машинных носителей информации, используемых в информационных системах администрации Новосибирского района Новосибирской области.

Члены комиссии:

(подпись) (ФИО)

(подпись) (ФИО)

«___» _____ 20___ г.

Приложение № 3
к Правилам обращения с машинными носителями информации
в информационных системах
администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

ФОРМА

Акт
уничтожения машинных носителей информации

Комиссия в составе:

(должность, ФИО)

(должность, ФИО)

(должность, ФИО)

составила настоящий Акт о том, что нижеуказанные машинные носители информации подлежат уничтожению как утратившие практическое значение и непригодные для дальнейшего использования:

№ п/п	Тип машинного носителя информации	Учетный номер машинного носителя информации	Примечание

Всего машинных носителей _____

(цифрами и прописью)

На машинных носителях уничтожена вся информация путем:

Вышеуказанные машинные носители уничтожены путем:

Отметка об уничтожении внесена в Журнал учета машинных носителей информации, используемых в информационных системах администрации Новосибирского района Новосибирской области

Члены комиссии:

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

Приложение № 6
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2014 № 3390-па

ПРАВИЛА
регистрации событий безопасности в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер по регистрации событий безопасности в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация оператор) и регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в ИС администрация.

1.2. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в ИС, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

2. Определение событий безопасности, подлежащих регистрации, и сроков их хранения

2.1. События безопасности, подлежащие регистрации в ИС администрация, определяются с учетом способов реализации угроз безопасности для ИС.

2.2. К событиям безопасности, подлежащим регистрации в ИС, относятся любые проявления состояния ИС и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.

2.3. События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС.

2.4. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется исходя из возможностей реализации угроз безопасности информации.

2.5. В ИС администрации подлежат регистрации следующие события безопасности:

- вход (выход), а также попытки входа субъектов доступа в ИС и загрузки (останова) операционной системы;

- подключение машинных носителей информации и вывод информации на носители информации;

- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

- попытки удаленного доступа.

2.6. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС администрации, и устанавливаются исходя из значимости события безопасности.

3. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3.1. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

3.2. Основной состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, представлены в Таблице 1.

Таблица 1 – Состав и содержание информации о событиях безопасности

№ п/п	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
1	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа
2	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на

№ п/п	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
		носитель информации
3	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)
4	Попытки доступа программных средств к защищаемым объектам доступа	Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип)
5	Попытки удаленного доступа	Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе

4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

4.1. Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения должны предусматривать:

- возможность выбора событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 3 настоящих Правил;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в пункте 3.2 настоящих Правил;
- хранение информации о событиях безопасности в течение установленного времени.

4.2. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

5. Реагирование на сбои при регистрации событий безопасности

5.1. Реагирование на сбои при регистрации событий безопасности в ИС администрации (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) осуществляется уполномоченными сотрудниками администрации.

5.2. Реагирование на сбои при регистрации событий безопасности предусматривает следующие меры:

- изменение параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС;
- запись поверх устаревших хранимых записей событий безопасности.

6. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

6.1. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться уполномоченными сотрудниками администрации для всех событий, подлежащих регистрации в соответствии с пунктом 3.2 настоящих Правил, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

6.2. В случае выявления признаков инцидентов безопасности в ИС администрации уполномоченными сотрудниками осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

7. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

7.1. В ИС администрации должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

7.2. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС администрации достигается посредством применения внутренних системных часов ИС или путем синхронизации системного времени.

8. Защита информации о событиях безопасности

8.1. Защита информации о событиях безопасности (записях регистрации (аудита)) в ИС администрации должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

8.2. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным сотрудникам администрации.

9. Ответственность

9.1. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

9.2.Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение № 7
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

ПРАВИЛА
антивирусной защиты информационных систем администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер по антивирусной защите информационных систем (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор) и регулируют вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС администрации.

1.2. Меры по антивирусной защите должны обеспечивать обнаружение в ИС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

1.3. Установка и настройка средств антивирусной защиты осуществляется уполномоченными сотрудниками администрации в соответствии с эксплуатационной документацией на применяемые средства антивирусной защиты.

2. Обеспечение антивирусной защиты

2.1.Порядок организации антивирусной защиты

2.1.1. Для обеспечения антивирусной защиты ИС администрации должны применяться средства антивирусной защиты, установленные на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС администрации и подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб - и другие сетевые сервисы).

2.1.2. Права на установку, конфигурирование и управление (администрирование) средствами антивирусной защиты предоставляются уполномоченным сотрудникам администрации.

2.1.3. Для реализации антивирусной защиты в ИС администрации осуществляется предоставление доступа средствам антивирусной защиты к объектам ИС, которые должны быть подвергнуты проверке.

2.1.3. Сотрудники администрации не должны допускать использования в ИС программного обеспечения и данных, не связанных с выполнением их

должностных обязанностей.

2.1.5. Уполномоченными сотрудниками администрации организуется проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов).

2.1.5. Проверка выделенных наиболее критичных компонентов ИС (системной памяти, объектов автозапуска, системных папок) на наличие вредоносных компьютерных программ (вирусов) осуществляется в автоматическом режиме по расписанию (один раз в сутки) и при необходимости вручную пользователями ИС.

2.1.6. Расширенный (полный) антивирусный контроль всех компонентов ИС проводится в автоматическом режиме с периодичностью один раз в месяц и при необходимости вручную уполномоченным сотрудником администрации.

2.1.7. В ИС должна осуществляться автоматическая проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, и других внешних источников) при загрузке, открытии или исполнении таких файлов.

2.1.8. В ИС должно осуществляться оповещение уполномоченных сотрудников администрация в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов).

2.1.9. Расширенный (полный) антивирусный контроль всех компонентов ИС проводится в автоматическом режиме с периодичностью один раз в месяц и при необходимости вручную.

2.1.9. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Контроль исходящей информации (в случае передачи информации на внешнем съемном носителе) необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель) (при наличии такой процедуры).

2.2. Порядок проведения антивирусного контроля.

2.2.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС администрация самостоятельно или вместе с уполномоченным сотрудником администрация проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.2. В случае обнаружения в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами), пользователь ИС обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за защиту информации, уполномоченных сотрудников администрация владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

2.3. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

2.3.1. Получение из доверенных источников и установка обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивают уполномоченные сотрудники администрации.

2.3.2. В ИС администрация обеспечивается контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) на соответствие предоставляемых производителем СЗИ контрольным суммам.

2.3.3. В ИС администрации Новосибирского района Новосибирской области обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов) уполномоченными сотрудниками ЦОД Правительства Новосибирской области.

3. Ответственность

3.1. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

3.2. Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение № 8
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

ПРАВИЛА
контроля (анализа) защищенности информации в информационных системах администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер по контролю (анализу) защищенности информации в информационных системах (далее – ИС) администрации Новосибирского района Новосибирской области (далее –администрация, оператор).

1.2. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в ИС, путем проведения мероприятий по анализу защищенности ИС и тестированию их систем защиты информации.

1.3. Мероприятия по контролю защищенности информации в ИС проводятся в пределах своих полномочий уполномоченными сотрудниками администрации, ответственным за защиту информации, содержащейся в информационных системах администрации.

2. Выявление, анализ и устранение уязвимостей информационных систем

2.1. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

2.2. В ИС администрации при выявлении (поиске), анализе и устранении уязвимостей должны проводиться:

-выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

-разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

-анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

-устранение выявленных уязвимостей, в том числе путем установки

обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

-информирование должностных лиц (пользователей, ответственных лиц) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

-Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

2.3. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

2.4. Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации ИС. На этапе эксплуатации ИС поиск и анализ уязвимостей проводится не реже одного раза в год. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемых в ИС администрации.

2.5. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС), направленные на устранение возможности использования выявленных уязвимостей.

2.6. В ИС администрации должны использоваться для выявления (поиска) уязвимостей средства анализа (контроля) защищенности (сканеры безопасности), имеющие стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИС на наличие уязвимостей, оценки последствий уязвимостей, имеющие возможность оперативного обновления базы данных выявляемых уязвимостей.

2.7. В ИС администрации должно осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей (для системы анализа защищенности).

2.8. Доступ к функциям выявления (поиска) уязвимостей предоставляется только уполномоченным сотрудникам администрации.

2.9. В целях предупреждения инцидентов безопасности уполномоченные сотрудники администрации должны проводить анализ журналов регистрации событий безопасности (журнал аудита) в целях определения, были ли выявленные

уязвимости ранее использованы в ИС администрации для нарушения безопасности информации

2.10. В случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1. В ИС администрации уполномоченными сотрудниками администрации в рамках своих полномочий обеспечивается получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИС администрации и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.3. Контроль установки обновлений программного обеспечения проводится с периодичностью – не реже одного раза в два года.

3.4. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации должны осуществляться:

- контроль работоспособности (не отключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

- восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.2. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится уполномоченными сотрудниками администрации не реже одного раза в 2 года.

5. Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1. При контроле состава технических средств, программного обеспечения и средств защиты информации (инвентаризации) должны осуществляться:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации, приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС администрации и принятие мер, направленных на устранение выявленных недостатков;

- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- исключение (восстановление) из состава ИС администрации несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.2. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится ответственным за защиту информации, уполномоченными сотрудниками администрации в рамках своих полномочий не реже одного раза в 2 года.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей, реализации правил разграничения доступом, полномочий пользователей в информационных системах

6.1. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС администрации должны осуществляться:

- контроль правил генерации и смены паролей пользователей;
- контроль заведения и удаления учетных записей пользователей;
- контроль реализации правил разграничения доступом;
- контроль реализации полномочий пользователей;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в администрации;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

6.2. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС администрации проводится уполномоченными сотрудниками администрации не реже одного раза в 2 года.

7. Ответственность

7.1. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

7.2. Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение № 9
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

ПРАВИЛА
обеспечения целостности и доступности информационных систем и информации в администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящие Правила разработаны в целях реализации мер по обеспечению целостности и доступности информационных систем (далее – ИС) и информации в администрации Новосибирского района Новосибирской области (далее – администрация, оператор).

1.2. Меры по обеспечению целостности ИС и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности ИС и содержащейся в ней информации, а также возможность восстановления ИС и содержащейся в ней информации.

1.3. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в ИС, в штатном режиме функционирования ИС.

1.4. Защита резервируемой информации в ИС администрации обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в администрации.

2. Обеспечение возможности восстановления программного обеспечения в информационной системе при возникновении нештатных ситуаций

2.1. Для обеспечения возможности восстановления программного обеспечения в ИС администрации должны быть приняты соответствующие планы по действиям персонала (ответственных, пользователей) при возникновении нештатных ситуаций.

2.2. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

- восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
- восстановление и проверку работоспособности системы защиты

информации, обеспечивающие необходимый уровень защищенности информации;

- возврат ИС администрации в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации.

2.3. В ИС администрации должны применяться компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

3. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

3.1. В ИС администрации должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

3.2. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования ИС путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

3.3. При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с настоящими Правилами, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования.

4. Периодическое резервное копирование информации на резервные машинные носители информации

4.1. В ИС администрации должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

- резервное копирование информации на резервные машинные носители информации с установленной периодичностью;
- разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
- регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

- принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

4.2. Резервное копирование и хранение данных должно осуществлять на периодической основе.

4.3. Хранение (размещение) резервных копий информации должно осуществляться на отдельных (размещенных вне ИС) средствах хранения резервных копий и в условиях, которые исключают воздействие внешних факторов на хранимую информацию.

4.4. Резервные копии должны храниться в течение установленного срока с целью обеспечения возможности восстановления данных.

4.5. Уполномоченными сотрудниками администрации в пределах своей компетенции определяются методы резервного копирования, порядок хранения и восстановления резервируемой информации и осуществляется периодическая проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

5. Восстановление информации с резервных машинных носителей информации

5.1. Восстановление информации из резервных копий осуществляется уполномоченными сотрудниками администрации.

5.2. Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС администрации и доступности информации:

- для защищаемой информации – не более 8 часов;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС администрации – не более 24 часов.

Приложение № 10
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

РЕГЛАМЕНТ
выявления инцидентов безопасности и реагирования на них в администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящий Регламент определяет правила и процедуры выявления и реагирования на инциденты информационной безопасности (далее – ИБ) в администрации Новосибирского района Новосибирской области (далее – администрация).

1.2. Под инцидентом информационной безопасности понимается непредвиденное или нежелательное событие (группа событий), которое привело (может привести) к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации (далее – инцидент).

1.3. Выявление инцидентов ИБ в администрации и реагирование на них обеспечивается ответственным за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), содержащейся в ИС администрации.

2. Этапы реагирования на инциденты безопасности

2.1. Жизненный цикл реагирования на инциденты состоит из следующих стадий:

- обнаружение и регистрация инцидента;
- устранение причин и последствий инцидента;
- расследование инцидента;
- реализация корректирующих мероприятий.

2.2. В ходе выявления инцидентов и реагирования на них осуществляются:

- 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 пользователями ИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

- 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 информационной системы 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.

3. Обнаружение инцидентов информационной безопасности

3.1. В качестве источников информации об инцидентах могут использоваться:

- журналы регистрации событий безопасности и оповещения системного и прикладного программного обеспечения ИС, средств защиты информации;

- информация, получаемая от сотрудников администрации;

- информация, полученная по результатам контроля (анализа) защищенности ИС и контроля эффективности СЗИ.

4. Информирование об инцидентах, анализ инцидентов

4.1. Уполномоченный сотрудник администрации ответственный за защиту информации, содержащейся в ИС администрации (далее – ответственный за выявление и реагирование на инциденты) получает информацию о случившихся инцидентах и принимает меры по их устранению.

4.2. Сотрудники администрации, а также иные лица, имеющие доступ к ИС администрации, в том числе осуществляющие техническое сопровождение ИС администрации, обязаны при получении информации обо всех нетипичных событиях ИБ незамедлительно сообщить о них ответственному за защиту информации, содержащейся в ИС администрации.

4.3. Некорректное функционирование ИС администрации может являться индикатором атаки или нарушения функционирования системы безопасности. К нетипичным событиям, о которых следует уведомлять ответственных за выявление и реагирование на инциденты, относятся:

- крахи системы, произвольные перезагрузки системы;

- самопроизвольное появление новых учетных записей;

- самопроизвольное появление новых файлов;

- изменения в размерах и датах файлов, не соответствующие фактическим датам обращения и внесения изменений;

- попытки записи в системные файлы;

- самопроизвольные модификация или удаление данных;

- отказ в обслуживании (отсутствие доступа к программным и техническим средствам);

- необъяснимо низкая производительность системы (слишком долгое время отклика системы);

- аномалии поведения системы (например, появление сообщений на экране, частые и необъяснимые звуковые сигналы);

- подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети);

- неконтролируемое внесение изменений в систему, ее настройки и параметры;

- неправильное срабатывание программного или аппаратного обеспечения;

- нарушения доступа (отказ в доступе в систему);

-другие нетипичные события.

4.4. Все сотрудники администрации, лица, выполняющие работы и оказывающие услуги на договорной основе, и имеющие доступ к ИС администрации, должны быть ознакомлены с процедурой информирования о выявленных инцидентах ИБ и иных нетипичных событиях.

4.5. Ответственные за выявление и реагирование на инциденты проводят сбор информации, связанной с событием, о котором поступило сообщение, для подтверждения и локализации инцидента ИБ.

5. Реагирование на инциденты информационной безопасности

5.1. В случае наличия признаков инцидента в полученной информации ответственные за выявление и реагирование на инциденты определяют предварительную степень важности инцидента, проводят первоочередные меры, направленные на локализацию инцидента ИБ, препятствующие его распространению (в том числе ограничение доступа к объектам, задействованным в инциденте ИБ) и минимизацию его последствий, принимает решение о необходимости проведения расследования.

5.2. Для реагирования на инциденты ответственный за выявление и реагирование на инциденты может привлекать по необходимости внешних экспертов. Необходимость привлечения тех или иных специалистов определяется в зависимости от вида инцидента.

5.3. Сотрудники администрации могут привлекаться к реагированию на инциденты ИБ по согласованию с Главой администрации.

5.4. После локализации инцидента необходимо приступить к ликвидации последствий и восстановлению системы (приведению системы к штатному режиму функционирования), проводится расследование и анализ произошедшего инцидента.

5.5. В ходе анализа инцидента по возможности выявляются следующие показатели:

- факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);

- опасность угрозы;

- область, перечень информационных ресурсов, затрагиваемых воздействием угрозы;

- потенциальные нарушители, цели и причины реализации угрозы;

- перечень мер по локализации и остановке распространения действия угрозы.

6. Анализ причин и оценка результата

6.1. Расследование инцидента ИБ проводится с целью раскрытия причинно-следственных связей и получения следующей информации:

- источники инцидента ИБ (нарушители);

- цели инцидента ИБ;

- способы осуществления инцидента ИБ.

6.2. По результатам проведенного расследования инцидента ответственные за выявление и реагирование на инциденты проводят:

- переоценку рисков, повлекших возникновение инцидента ИБ;

- анализ перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента ИБ;

- анализ инструкций и правил обеспечения информационной безопасности, включая настоящий документ;

- инструктаж (информирование об угрозах безопасности информации, правилах эксплуатации системы защиты информации ИС и отдельных средств защиты информации) сотрудников администрации для повышения их осведомленности в части информационной безопасности.

Приложение № 11
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 2390-па

ПОЛОЖЕНИЕ
по управлению конфигурацией информационных систем администрации Новосибирского района Новосибирской области

1. Общие положения

1.1. Настоящее Положение определяет порядок управления конфигурацией информационных систем (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор) и их системы защиты информации.

2. Порядок управления конфигурацией информационных систем и системы защиты информации

2.1. Действия по внесению изменений в конфигурацию ИС администрации и их системы защиты информации разрешены уполномоченным сотрудникам администрации, а также представителям сторонних организаций, оказывающих услуги гарантийного и (или) технического обслуживания программных и программно-аппаратных средств, включая средства защиты информации, ИС администрации в пределах полномочий согласно заключенным договорам, соглашениям, контрактам.

2.2. Управление конфигурацией ИС администрации осуществляется на основе согласованных решений уполномоченных лиц, указанных в п. 2.1 настоящего Положения, и включает:

- разработку параметров настройки, обеспечивающих защиту информации;
- анализ потенциального воздействия планируемых изменений на обеспечение защиты информации (возникновение дополнительных угроз безопасности информации и работоспособность ИС);
- санкционирование внесения изменений в ИС и их системы защиты информации;
- документирование действий по внесению изменений в ИС и их системы защиты информации и сохранение данных об изменениях конфигурации.

2.3. Объектами управления конфигурацией (компонентами ИС администрации и их системы защиты информации, подлежащих изменению в рамках управления конфигурацией) определены программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю.

2.4. Внесение изменений в ИС администрации и их системы защиты информации в отношении объектов управления конфигурацией может

осуществляться в рамках гарантийного и (или) технического обслуживания (в том числе дистанционно (удаленно)), программных и программно-аппаратных средств, включая средства защиты информации, ИС администрации.

2.5. Документирование (внесение информации (данных)) об изменениях в конфигурации ИС администрации и их систем защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в эксплуатационную документацию на систему защиты информации ИС осуществляет ответственный за защиту информации.

Приложение № 12
к постановлению администрации
Новосибирского района
Новосибирской области
от 05.11.2024 № 3390-па

ПОЛОЖЕНИЕ
по защите информации в администрации Новосибирского района Новосибирской области при выводе из эксплуатации информационных систем или после принятия решения об окончании обработки информации ограниченного доступа

1. Общие положения

1.1. Настоящее Положение разработано в целях обеспечения защиты информации при выводе из эксплуатации информационных систем (далее – ИС) администрации Новосибирского района Новосибирской области (далее – администрация, оператор).

1.2. Меры по обеспечению защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации обеспечиваются путем выполнения требований к порядку вывода ИС из эксплуатации и дальнейшему хранению содержащихся в ее базах данных информации.

3. Требования к порядку вывода ИС из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации

3.1. Основанием для вывода ИС из эксплуатации являются:

- завершение срока эксплуатации ИС, в случае если такой срок был установлен правовым актом о вводе ИС в эксплуатацию;
- нецелесообразность эксплуатации ИС, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации ИС;
- финансово-экономическая неэффективность эксплуатации ИС.

3.2. При наличии одного или нескольких оснований для вывода системы из эксплуатации, указанных в пункте 2.1 настоящего Положения, оператор утверждает правовой акт о выводе системы из эксплуатации.

3.3. Правовой акт о выводе ИС из эксплуатации включает:

- основание для вывода ИС из эксплуатации;
- перечень и сроки реализации мероприятий по выводу ИС из эксплуатации;
- порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам выводимой из эксплуатации ИС и обеспечения защиты информации, содержащейся в выводимой из эксплуатации ИС;

- порядок, сроки и способы информирования пользователей о выводе ИС из эксплуатации.

3.4. Перечень мероприятий по выводу ИС из эксплуатации включает:

- подготовку правовых актов, связанных с выводом ИС из эксплуатации;

- работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на программное обеспечение ИС, демонтажу и списанию технических средств ИС, обеспечению хранения и дальнейшего использования информационных ресурсов ИС;

- обеспечение защиты информации в соответствии с документацией на ИС и организационно-распорядительными документами по защите информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

3.5. Если нормативными правовыми актами Российской Федерации не установлено иное, то сроки хранения информации, содержащейся в базах данных системы, определяются оператором и не могут быть меньше сроков хранения информации, которые установлены для хранения документов в бумажном виде, содержащих такую информацию.

3.6. Срок вывода ИС из эксплуатации не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о выводе ИС из эксплуатации.

4. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации

4.1. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации, содержащейся в ИС, осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации ИС и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в ИС;

- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

4.2. Архивирование информации, содержащейся в ИС администрации должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора и осуществляется в соответствии с требованиями законодательства об архивном деле в Российской Федерации.

4.3. Архивирование информации, содержащейся в ИС администрации, обеспечивается уполномоченными сотрудниками администрации.

4.4. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для

ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

4.5. Процедуры уничтожения (стирания) информации, хранящейся на машинных носителях информации, а также физическое уничтожение машинных носителей информации производится ответственным за защиту информации, содержащейся ИС администрации.

Лист ознакомления

с постановлением администрации Новосибирского района Новосибирской области

от _____ № _____

«О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Новосибирского района Новосибирской области»

№ п/п	ФИО	Дата ознакомления	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			