Министерство
финансов Нижегородской области

П Р И К А З

13.03.2026 № 59

г. Нижний Новгород

Об утверждении регламента защиты информации от неправомерной передачи или распространения из государственной информационной системе управления общественными финансами министерства финансов Нижегородской области

В соответствии с постановлением Правительства Нижегородской области от 6 марта 2023 г. № 186 «Об утверждении Положения о государственной информационной системе управления общественными финансами министерства финансов Нижегородской области» в целях защиты информации от неправомерной передачи или распространения

п р и к а з ы в а ю:

1. Утвердить регламент защиты информации от неправомерной передачи или распространения из государственной информационной системе управления общественными финансами министерства финансов Нижегородской области (далее – Регламент).

2. Начальнику управления развития технологий системной безопасности и оптимизации бюджетных процессов Прыткову А.П. обеспечить размещение Регламента на официальном сайте министерства финансов Нижегородской области.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр О.Ю.Сулима

ЛИСТ СОГЛАСОВАНИЯ
проекта приказа министерства финансов Нижегородской области «Об утверждении регламента защиты информации от неправомерной передачи или распространения из государственной информационной системе управления общественными финансами министерства финансов Нижегородской области»

ПРОЕКТ ПРЕДСТАВЛЕН:

Начальник управления
РТСБиОБП
А.П.Прытков

_____ _____
подпись дата

ПРОЕКТ СОГЛАСОВАН:

Первый заместитель министра
Н.А.Никифорова

_____ _____
подпись дата

Управляющий делами
Д.А.Черных

_____ _____
подпись дата

Начальник отдела правового обеспечения
М.В.Хамков

_____ _____
подпись дата

ИСПОЛНИТЕЛЬ:

Заместитель начальника отдела
системной безопасности
А.А.Маркушин

_____ 04.03.2026
подпись дата

т. 421-94-80

УТВЕРЖДЕНО
приказом министерства финансов
Нижегородской области
от 13.03.2026 № 59

Регламент
защиты информации от неправомерной передачи или распространения из государственной информационной системе управления общественными финансами министерства финансов Нижегородской области

1. Общие положения

Настоящий регламент содержит положения, регламентирующие мероприятия, направленные на защиту информации от неправомерной передачи или распространения в результате действий пользователей, имеющих права доступа к защищаемой информации в государственной информационной системе управления общественными финансами министерства финансов Нижегородской области (далее – ГИС МФ НО), и выполняемые с использованием средств защиты информации от неправомерной передачи или распространения.

Настоящий регламент не содержит положений, касающихся мероприятий, направленных на обеспечение защиты информации от иных угроз безопасности информации, в том числе, связанных с утечками информации по техническим каналам.

2. Нормативные ссылки

В настоящем регламенте использованы нормативные ссылки на следующие государственные стандарты:

- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию.
- ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
- ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения.

- ГОСТ Р 59548-2022 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации.
- ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами. Общие положения.
- ГОСТ Р 59853-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

3. Термины и определения

В настоящем регламенте применены термины в соответствии с ГОСТ Р 50922-2006, ГОСТ Р 53114-2008, ГОСТ Р 59853-2021, а также следующие термины определениями:

1) Защита информации от неправомерной передачи или распространения из ГИС МФ НО (в результате действий пользователей, имеющих права доступа к защищаемой информации) - деятельность, направленная на предотвращение неконтролируемой передачи или распространения защищаемой информации с использованием программных и программно-аппаратных средств ГИС МФ НО лицами, имеющими к ней право доступа.

2) Канал неправомерной передачи или распространения информации из ГИС МФ НО - использование лицом, имеющим право доступа к защищаемой информации, программных или программно-аппаратных средств информационной (автоматизированной) системы, предназначенных для обработки (передачи или хранения) информации, с нарушением установленных у участника бюджетного процесса правил передачи или хранения защищаемой информации, в том числе с целью её неправомерной передачи или распространения.

3) Объект мониторинга (при защите информации от неправомерной передачи или распространения из ГИС МФ НО в результате действий пользователей, имеющих права доступа к защищаемой информации) - подсистема и компоненты ГИС МФ НО, которые используются в качестве источников данных, необходимых для выявления признаков возможной неправомерной передачи или распространения информации из ГИС МФ НО, в том числе телекоммуникационное оборудование, используемое в информационной (автоматизированной) системе, средства вычислительной

техники, с которыми работают пользователи ГИС МФ НО, серверы ГИС МФ НО, на которых функционируют сервисы коммуникаций, серверы ГИС МФ НО, на которых размещаются общие файловые ресурсы, средства защиты информации, используемые в ГИС МФ НО.

4) Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

5) Средство защиты информации от неправомерной передачи или распространения из ГИС МФ НО - средство защиты информации, предназначенное для предотвращения или выявления нарушений правил обработки (передачи или хранения) защищаемой информации, установленных у участника бюджетного процесса, пользователями, имеющими права доступа к защищаемой информации, которые привели или могут привести к неправомерной передаче или распространению защищаемой информации, и для обеспечения реагирования на такие нарушения.

6) Перечень мероприятий по защите информации от неправомерной передачи или распространения - совокупность мер по защите информации от неправомерной передачи или распространения, объединенных по определенному признаку в единую группу.

В настоящем регламенте определены четыре группы мероприятий по защите информации:

- первой группой мероприятий является группа объектов мониторинга, определяющая совокупность мероприятий по защите информации от неправомерной передачи или распространения, выполняемых в отношении объектов мониторинга, которые могут предоставить информацию, необходимую для защиты информации от неправомерной передачи или распространения;

- второй группой мероприятий по защите является меры взаимодействия с объектами мониторинга, которая определяет совокупность мероприятий по защите информации от неправомерной передачи или распространения, выполняемых с целью получения от объектов контроля информации, необходимой для защиты информации от неправомерной передачи или распространения;

- третьей группой мероприятий по защите является меры выявления признаков возможной неправомерной передачи или распространения, которая определяет совокупность мероприятий по защите информации от неправомерной передачи или распространения, выполняемых с целью анализа полученной информации и выявления в её составе признаков, указывающих на возможную неправомерную передачу или распространение информации, а также реагирования на выявленные признаки неправомерной передачи или распространения информации;

- четвертой группой мероприятий по защите является представление результатов и выявление признаков возможной неправомерной передачи или распространения, которая определяет совокупность мероприятий по защите информации от неправомерной передачи или распространения, выполняемых с целью представления информации о результатах защиты информации от неправомерной передачи или распространения лицам, ответственным за обеспечение защиты информации от неправомерной передачи или распространения.

7) Неправомерная передача или распространение информации из ГИС МФ НО - неконтролируемая передача или распространение защищаемой информации из ГИС МФ НО лицом, имеющим права доступа к защищаемой информации.

4. Мероприятия по защите информации от неправомерной передачи или распространения из ГИС МФ НО.

4.1. Мероприятия по защите информации от неправомерной передачи или распространения из ГИС МФ НО в результате действий пользователей, имеющих права доступа к защищаемой информации в ГИС МФ НО (далее – защита информации от неправомерной передачи или распространения), реализуются в процессе создания, развития (модернизации) или эксплуатации ГИС МФ НО в соответствии с требованиями нормативных правовых актов и методических документов по защите информации уполномоченных федеральных органов исполнительной власти Российской Федерации.

4.1.1. Мероприятия по защите информации от неправомерной передачи или распространения из ГИС МФ НО являются одной из составляющих деятельности по обеспечению информационной безопасности в министерстве

финансов Нижегородской области, и, в соответствии с требованиями законодательства Российской Федерации о техническом регулировании в области защиты информации и обеспечения информационной безопасности, осуществляются сотрудниками управления развития технологий системной безопасности и оптимизации бюджетных процессов министерства финансов Нижегородской области, осуществляющими функции по обеспечению информационной безопасности.

4.1.2. Целью мероприятий по защите информации от неправомерной передачи или распространения является блокирование (нейтрализация) угроз безопасности информации, связанных с действиями пользователей в ГИС МФ НО, приводящими к неправомерной передаче или распространению защищаемой информации из ГИС МФ НО. К таким действиям относятся действия пользователей ГИС МФ НО, в результате которых защищаемая информация становится или может стать доступной другим пользователям ГИС МФ НО или иным лицам, которые не должны иметь доступ к такой информации (неправомерная отправка защищаемой информации (в виде электронного сообщения или файла) лицам, которые не должны иметь к ней доступ; сохранение защищаемой информации в местах хранения (машинные носители информации или общие файловые ресурсы), из которых доступ к защищаемой информации могут получить лица, которые не должны иметь к ней доступ).

К неправомерной передаче или распространению информации могут приводить как преднамеренные, так и непреднамеренные действия пользователей ГИС МФ НО.

4.1.3. Мероприятия по защите информации от неправомерной передачи или распространения из информационной (автоматизированной) системы устанавливаются при подготовке к эксплуатации ГИС МФ НО (подготовительный этап) и в процессе эксплуатации ГИС МФ НО.

4.2. Мероприятия по защите информации от неправомерной передачи или распространения из ГИС МФ НО при подготовке к эксплуатации информационной (автоматизированной) системы.

4.2.1. Мероприятиями по защите информации от неправомерной передачи или распространения из ГИС МФ НО при подготовке к эксплуатации информационной (автоматизированной) системы являются:

- определение каналов неправомерной передачи или распространения информации из информационной (автоматизированной) системы;

- уведомление пользователей ГИС МФ НО о мониторинге средств вычислительной техники;

- определение запретов и правил для пользователей ГИС МФ НО;

- подготовка сотрудников или структурного подразделения, осуществляющего функции по обеспечению информационной безопасности, к работе по контролю каналов неправомерной передачи или распространения информации из ГИС МФ НО;

- взаимодействие подразделений, участвующих в работе по контролю каналов неправомерной передачи или распространения информации из ГИС МФ НО.

4.2.2. Основными каналами неправомерной передачи или распространения информации из ГИС МФ НО являются[1]:

- каналы на основе сервисов коммуникаций (сервисов, предоставляемых средствами электронной почты, средствами мгновенного обмена сообщениями и иных сервисов коммуникаций)[2];

- каналы на основе сервисов публикации на сетевых ресурсах[3];

- каналы на основе сервисов печати файлов (локальные и сетевые);

- каналы на основе съемных машинных носителей информации;

- каналы на основе общих файловых ресурсов[4].

4.2.3. Уведомление пользователей ГИС МФ НО о мониторинге средств вычислительной техник.

Соответствующее уведомление пользователям ГИС МФ НО о мониторинге средств вычислительной техники, с которыми они работают, и

---

[1] В качестве основы каналов неправомерной передачи или распространения рассматриваются и иные устройства, имеющие в своем составе встроенные носители информации (фото и видео камеры, смартфоны и другие устройства, которые могут подключаться как съемные машинные носители информации).

[2] В качестве основы каналов неправомерной передачи или распространения рассматриваются как штатные сервисы коммуникаций, функционирующие в составе ГИС МФ НО (сервис корпоративной электронной почты), так и сервисы коммуникаций в иных сетях, к которым имеет подключение ГИС МФ НО (общедоступные почтовые сервисы или сервисы обмена сообщениями в сети Интернет).

[3] В качестве основы каналов неправомерной передачи или распространения рассматриваются как штатные сервисы публикации на сетевых ресурсах, функционирующие в ГИС МФ НО (корпоративный веб-портал), так и сервисы публикации на сетевых ресурсах в иных сетях, к которым имеет подключение информационная (автоматизированная) система (например, облачное хранилище).

[4] В качестве основы каналов неправомерной передачи или распространения рассматриваются как штатные общие файловые ресурсы, функционирующие в информационной (автоматизированной) системе (корпоративный файловый сервер), так и общие файловые ресурсы в иных сетях, к которым имеет подключение информационная (автоматизированная) система (сервисы файловых хранилищ в сети Интернет). Неправомерная передача или распространение информации из этих ресурсов возможна из-за нарушения правил хранения защищаемой информации, например, хранение в общедоступной папке эксплуатационной документации на информационных (автоматизированных) систем, сведений об учетных данных пользователей и иной защищаемой информации.

мониторинге их действий с использованием средств защиты информации от утечки выдается при приеме на работу или в процессе ввода в эксплуатацию компонент ГИС МФ НО. Кроме того, одновременно с уведомлением пользователь ознакомляется под подпись с перечнем видов информации, подлежащих защите от неправомерной передачи или распространения информации, с правилами передачи и хранения защищаемой информации.

Для обеспечения выполнения мероприятий по защите информации от неправомерной передачи или распространения из ГИС МФ НО доводится до пользователей ГИС МФ НО, что создаваемая в ГИС МФ НО информация в соответствии с правилами определения видов информации является защищаемой информацией и что обладатель информации и средств её обработки имеет право обеспечивать контроль их сохранности и целевого использования, в том числе с применением средств защиты информации от утечки.

4.2.4. Для пользователей ГИС МФ НО введен запрет на:

- нарушение установленных в документах (политике защиты информации, внутренних регламентах и стандартах по защите информации), регламентирующих вопросы защиты информации в исполнительном органе Нижегородской области/участника бюджетного процесса, правил использования пользователями ГИС МФ НО, средств вычислительной техники и программного обеспечения (в том числе средств коммуникаций);

- несанкционированный вынос съемных машинных носителей информации и средств вычислительной техники, предоставленных работодателем (нанимателем);

- использование пользователями в неслужебных целях средств вычислительной техники, предоставленных работодателем (нанимателем), и программного обеспечения ГИС МФ НО.

Также определены правила (допустимо введение полного запрета)[5]:

- хранения личных данных на файловых ресурсах и устройствах, предоставляемых работодателем (нанимателем) для выполнения трудовых (служебных) обязанностей;

---

[5] Описание действий, которые запрещено проводить пользователям при эксплуатации ГИС МФ НО допускается включать во внутренний стандарт по защите информации, содержащий запреты действий пользователей при использовании и обеспечении эксплуатации информационных (автоматизированных) систем в министерстве финансов Нижегородской области.

- использования личных устройств и программных средств коммуникаций в служебных целях.

4.2.5. При подготовке сотрудников управления развития технологий системной безопасности и оптимизации бюджетных процессов, выполняющих функции по обеспечению информационной безопасности, к работе по контролю каналов неправомерной передачи или распространения информации из ГИС МФ НО выполняется:

- разработка и утверждение перечня видов информации, подлежащих защите от неправомерной передачи или распространения информации, и правил использования средств вычислительной техники и программного обеспечения при обработке защищаемой информации[6];

- инвентаризация обрабатываемой информации, по результатам которой устанавливается, какие виды обрабатываемой информации требуют обеспечения конфиденциальности[7]. Все виды информации, требующие обеспечения конфиденциальности, включаются в перечень информации, подлежащей защите от неправомерной передачи или распространения.

- определение правил использования пользователями ГИС МФ НО средств вычислительной техники и программного обеспечения (в том числе средств коммуникаций, сервисов публикации на сетевых ресурсах, сервисов печати файлов) при обработке информации, требующей обеспечения конфиденциальности;

- анализ в ГИС МФ НО назначенных пользователям прав доступа к объектам доступа на предмет избыточности с учётом изменения полномочий пользователей;

---

[6] 1) Перечень видов информации, подлежащих защите от неправомерной передачи или распространения информации, формируется исходя из целей и назначения ГИС МФ НО и сведений, содержащихся в информации, подлежащей защите от неправомерной передачи или распространения информации. К таким видам информации относятся персональные данные, финансовая информация, служебная информация, информация об объекте интеллектуальной собственности и иные виды информации, защищаемые в соответствии с требованиями законодательства Российской Федерации.
2) При использовании средств вычислительной техники и программного обеспечения при обработке защищаемой информации определяют:
- способы передачи соответствующих видов информации получателям (передача файлов по сети, передача с использованием сервисов коммуникаций, размещение на сетевом ресурсе, печать, копирование на съемный машинный носитель информации);
- списки лиц, которые могут передавать соответствующие виды информации, а также допустимых получателей такой информации как в рамках ГИС МФ НО, так и за её пределами;
- допустимые места хранения видов информации, подлежащих защите от неправомерной передачи или распространения информации, на общих сетевых ресурсах ГИС МФ НО (общие каталоги, системы документооборота, базы данных, почтовые архивы и иные ресурсы);
- разработку внутреннего регламента по защите информации от неправомерной передачи или распространения из ГИС МФ НО;
- участие в анализе событий безопасности, связанных с неправомерной передачей или распространением защищаемой информации ГИС МФ НО.

[7] Порядок обеспечения конфиденциальности обязательно вводится в отношении охраняемой законом тайны (коммерческой тайны, персональных данных, профессиональной тайны и иной).

- принятие мер, предусматривающих уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации на машинных носителях;

- принятие мер по выявлению признаков неправомерной передачи или распространения из ГИС МФ НО;

- принятие мер, предусматривающих реагирование на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО;

- принятие мер, предусматривающих анализ результатов деятельности по защите информации от неправомерной передачи или распространения из ГИС МФ НО.

4.2.6. Состав подразделений-участников взаимодействия определяется организационно-штатной структурой исполнительного органа Нижегородской области/участника бюджетного процесса. В постоянный состав подразделений-участников взаимодействия включаются специалисты, обеспечивающие:

- установку в информационной инфраструктуре исполнительным органом Нижегородской области/участника бюджетного процесса и настройку средства защиты информации от утечки (локальные администраторы систем);

- изменение параметров информационной инфраструктуры исполнительного органа Нижегородской области/участника бюджетного процесса в связи с выявленными инцидентами информационной безопасности – неправомерной передачи или распространения информации из информационной (автоматизированной) системы (локальные администраторы систем);

- разработку организационно-распорядительной документации, содержащей правила обращения с защищаемой информацией, и содержащей сведения о вводе в эксплуатацию средства защиты от утечки;

- анализ информационных ресурсов;

- настройку правил выявления нарушений хранения и передачи защищаемой информации в средствах защиты информации от утечки в соответствии с результатами анализа информационных ресурсов;

- обработку информации о признаках возможных нарушений правил обращения с защищаемой информацией, зафиксированных средством защиты информации от утечки: первичную оценку, принятие решения об их отнесении к инцидентам информационной безопасности, обработку выявленных инцидентов, принятие мер реагирования, проверку полноты и корректности выполненных мероприятий;

- разработку документов, содержащей правила обращения с защищаемой информацией и мер ответственности за их нарушение, документы о вводе в эксплуатацию средства защиты информации от утечки;

- реализацию мер ответственности работников, в отношении которых установлена их связь с неправомерной передачей или распространением информации из информационной (автоматизированной) системы;

- передачу в уполномоченные федеральные органы исполнительной власти Российской Федерации результатов служебных проверок, связанных с выявленными признаками возможной неправомерной передачи или распространения информации, в случае наличия состава правонарушения.

4.3. Мероприятия по защите информации от неправомерной передачи или распространения из ГИС МФ НО в процессе эксплуатации.

4.3.1. Деятельность по защите информации от неправомерной передачи или распространения из ГИС МФ НО включает следующие стадии:

- выявление признаков неправомерной передачи или распространения информации из ГИС МФ НО;

- реагирование на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО;

- анализ результатов деятельности по защите информации от неправомерной передачи или распространения из ГИС МФ НО.

4.3.2. Выявление признаков неправомерной передачи или распространения информации ГИС МФ НО.

Выполнение мероприятий, направленных на выявление признаков возможной неправомерной передачи или распространения защищаемой информации из ГИС МФ НО, осуществляется с использованием средств защиты информации от утечки.

Реализуемые мероприятия по выявлению признаков возможной неправомерной передачи или распространения защищаемой информации должны обеспечить контроль всех видов информации, которые определены у

участника бюджетного процесса как виды информации, подлежащее защите от неправомерной передачи или распространения, а также обеспечивать контроль каналов неправомерной передачи или распространения, которые имеются в ГИС МФ НО.

4.3.3. Реагирование на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО.

Реагирование на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО целесообразно осуществлять в рамках деятельности по управлению инцидентами информационной безопасности (компьютерными инцидентами).

Для этих целей допускается передача событий безопасности, регистрируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения из комплексной системы информационной безопасности и повышения устойчивости ГИС МФ НО в систему управления событиями безопасности в соответствии с ГОСТ Р 59547-2021. При организации деятельности по управлению инцидентами информационной безопасности могут предусматриваться правила для регистрации признаков инцидентов информационной безопасности на основе событий безопасности, регистрируемых при обнаружении признаков возможной неправомерной передачи или распространения информации.

Деятельность по управлению инцидентами информационной безопасности в части реагирования на неправомерную передачу или распространение информации должна быть организована в соответствии с документом, регламентирующем вопросы планирования реагирования на неправомерную передачу или распространение информации у участника бюджетного процесса. Если деятельность по управлению инцидентами информационной безопасности не организована, то реагирование на неправомерную передачу или распространение информации должно выполняться специалистами подразделения по информационной безопасности, осуществляющими эксплуатацию средства защиты информации от утечки. Такое реагирование должно предусматривать немедленное блокирование, в случае возможности, действий, приводящих к неправомерной передаче или распространению информации, установление причин неправомерной передачи или распространения информации из ГИС МФ НО, а также принятие организационных, технических и (или) правовых

мер, направленных на устранение причин неправомерной передачи или распространения информации.

4.3.4. Анализ результатов деятельности по защите информации от неправомерной передачи или распространения из ГИС МФ НО.

Анализ результатов деятельности по защите информации от неправомерной передачи или распространения из ГИС МФ НО предусматривает:

- анализ эффективности мероприятий по защите информации от неправомерной передачи или распространения из ГИС МФ НО[8];

- оценку эффективности мероприятий по реагированию на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО[9];

- разработку рекомендаций по устранению причин и условий для неправомерной передачи или распространения информации из ГИС МФ НО[10].

5. Проведение мероприятий по защите информации от неправомерной передачи или распространения из ГИС МФ НО

---

[8] Анализ эффективности мероприятий по защите информации от неправомерной передачи или распространения из информационной (автоматизированной) системы предусматривает периодический анализ реализуемых процедур с целью выявления недостатков, связанных с выявлением потенциальной неправомерной передачи или распространения информации из ГИС МФ НО. Выявление неполного покрытия контролем потенциальных каналов неправомерной передачи или распространения, выявление неполного покрытия контролем некоторых видов информации, подлежащей защите, выявление недостатков параметров, по которым идентифицируются факты (попытки) неправомерной передачи или распространения, выявление неполноты применяемых механизмов анализа для выявления неправомерной передачи или распространения, выявление значительного количества ложноположительных срабатываний по выявлению признаков неправомерной передачи или распространения информации. Необходимость периодического анализа реализуемых процедур связана с тем, что такие недостатки могут возникнуть в процессе жизненного цикла ГИС МФ НО. При модернизации могут возникнуть новые каналы неправомерной передачи или распространения или появиться новые виды обрабатываемой информации.

[9] Если реагирование на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО осуществляется в рамках деятельности по управлению инцидентами информационной безопасности, то анализ эффективности мероприятий по реагированию на выявленную неправомерную передачу или распространение информации осуществляется в рамках реализованных у участника бюджетного процесса процедур по анализу результатов деятельности по управлению инцидентами информационной безопасности.

Если деятельность по управлению инцидентами информационной безопасности не организована, то анализ эффективности мероприятий по реагированию на выявленную неправомерную передачу или распространение информации предусматривает определение методов и способов реагирования на выявленные факты (попытки) неправомерной передачи или распространения информации из ГИС МФ НО, которые показали свою эффективность в рамках уже завершенных процедур реагирования, анализ изменений количества нарушений, связанных с фактами (попытками) неправомерной передачи или распространения информации, аналогичных тем, по которым принимались меры по реагированию.

[10] Разработка рекомендаций по устранению причин и условий для неправомерной передачи или распространения информации из ГИС МФ НО осуществляется с целью предотвращения их повторного возникновения.

На основе результатов деятельности по защите информации от неправомерной передачи или распространения из информационной (автоматизированной) системы осуществляется (при необходимости) доработка (актуализация) документа, содержащего перечень видов информации, подлежащих защите от неправомерной передачи или распространения информации, и доработка (актуализация) внутреннего регламента по защите информации от неправомерной передачи или распространения из ГИС МФ НО.

5.1 Перечень мероприятий при организации защиты информации от неправомерной передачи или распространения из ГИС МФ НО.

Рекомендации по проведению мероприятий по защите информации от неправомерной передачи или распространения из ГИС МФ НО могут быть выполнены в рамках следующих уровней мониторинга [11]:

- уровень объектов мониторинга;

- уровень взаимодействия с объектами мониторинга;

- уровень выявления признаков возможной неправомерной передачи или распространения;

- уровень представления результатов выявления признаков возможной неправомерной передачи или распространения.

5.2. Уровень объектов мониторинга.

5.2.1. При формировании перечня объектов мониторинга для защиты информации от неправомерной передачи или распространения следует учитывать необходимость в обеспечении мониторинга всех имеющихся в ГИС МФ НО каналов неправомерной передачи или распространения информации из числа, определенных в соответствии с пунктом 4.2.2.

5.2.2. В качестве объектов мониторинга, с которых могут быть получены данные, необходимые для выявления признаков возможной неправомерной передачи или распространения информации из ГИС МФ НО, рассматриваются:

- телекоммуникационное оборудование, используемое в ГИС МФ НО;

- средства вычислительной техники, с которыми работают пользователи ГИС МФ НО;

- серверы ГИС МФ НО, на которых функционируют сервисы коммуникаций;

- серверы ГИС МФ НО, на которых размещаются общие файловые ресурсы;

- средства защиты информации, используемые в ГИС МФ НО.

---

[11] Для осуществления мероприятий по защите информации от неправомерной передачи или распространения из ГИС МФ НО в соответствии с положениями настоящего регламента достаточно реализовать не все мероприятия, представленные в пункте 5.1, а выбирать с учётом рекомендаций для объектов мониторинга, состав которых зависит от каналов неправомерной передачи или распространения, имеющихся в ГИС МФ НО, и определять состав механизмов, которые позволят контролировать эти каналы неправомерной передачи или распространения, в том числе с учётом возможного представления информации (текстовый, графический или иные виды).

К данным, используемым в целях выявления признаков возможной неправомерной передачи или распространения информации из ГИС МФ НО, относятся:

а) для передаваемой в рамках используемых сервисов коммуникации информации и для передаваемых файлов:

- содержание информации, передаваемой с использованием сервисов коммуникации, или содержимое передаваемых файлов, при их передаче как в рамках ГИС МФ НО, так и за её пределы (в том числе при осуществлении печати файла и копирования на съемные машинные носители информации);

- сведения об отправителе и получателях (при их наличии), в том числе идентификаторы учетных записей, адреса отправителя и получателей, сетевые адреса;

- способ передачи информации;

- дата и время передачи;

б) для файлов, хранящихся на общих сетевых ресурсах:

- имя файла;

- тип файла (расширение);

- размер файла;

- дата создания файла;

- дата и время размещения на общем сетевом ресурсе;

- содержимое файла, хранящегося на общем файловом ресурсе;

- сетевой адрес размещения файла на общем файловом ресурсе (включая каталог размещения);

- сведения о пользователе, разместившем файл.

5.2.3. Телекоммуникационное оборудование, используемое для передачи сетевого трафика, может использоваться для получения копии сетевого трафика, в составе которого имеются данные, необходимые для выявления признаков возможной неправомерной передачи или распространения информации.

При выборе телекоммуникационного оборудования, которое может использоваться в качестве объекта мониторинга, учитывается, что телекоммуникационное оборудование обладает возможностью ответвления копии сетевого трафика на сетевой интерфейс, с которого она может быть передана для проведения анализа с целью выявления признаков возможной

неправомерной передачи или распространения информации из информационной (автоматизированной) системы.

Из копии сетевого трафика могут быть получены данные, позволяющие осуществлять мониторинг следующих каналов неправомерной передачи или распространения информации:

- сервисов коммуникации;

- сервисов публикации на сетевых ресурсах.

5.2.3.1. К данным, которые могут быть получены от телекоммуникационного оборудования и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов коммуникации, относятся[12]:

- содержание информации, передаваемой с использованием сервисов коммуникации, обнаруженной в копии сетевого трафика (в том числе содержание любых прикрепляемых файлов);

- сведения о сервисе коммуникации, с использованием которого передается информация;

- адреса отправителей и получателей информации;

- дата и время коммуникации.

5.2.3.2. К данным, которые могут быть получены от телекоммуникационного оборудования и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов публикации на сетевых ресурсах, относятся[13]:

- содержимое файла, обнаруженного в копии сетевого трафика, связанного с использованием сервисов публикации на сетевых ресурсах;

---

[12] Если телекоммуникационное оборудование как объект контроля используется для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов коммуникации, в сетевом трафике не всегда возможно обнаружить сообщения, передаваемые между пользователями, ГИС МФ НО, так как такой обмен сообщениями происходит в рамках одного сервиса коммуникации. Поэтому телекоммуникационное оборудование используют для контроля сообщений, передаваемых с внутреннего сервера сервисов коммуникации ГИС МФ НО на внешние сервисы коммуникации. Сообщения, передаваемые с внутреннего почтового сервера участника бюджетного процесса на почтовые серверы сторонних организаций или на почтовые серверы общедоступных почтовых сервисов в сети Интернет. Для контроля сообщений, передаваемых между пользователями информационной (автоматизированной) системы в рамках одного внутреннего сервиса коммуникации, данные для выявления признаков возможной неправомерной передачи или распространения информации целесообразно получать не от телекоммуникационного оборудования, а от средств вычислительной техники, на которых установлены клиентские компоненты сервисов обмена почтовыми сообщениями, или от программного обеспечения (агента), осуществляющего мониторинг действий пользователей.

[13] К публикациям на сетевых ресурсах, которые необходимо контролировать, относится копирование файла в облачное хранилище в сети Интернет.

- сведения о сервисе, используемом для опубликования файла на сетевом ресурсе;

- сетевой адрес средства вычислительной техники, с которого осуществляется опубликование файла на сетевом ресурсе;

- дата и время коммуникации с телекоммуникационным оборудованием.

5.2.4. Средства вычислительной техники, на которых работают пользователи ГИС МФ НО, могут использоваться для получения от функционирующего на них программного обеспечения (агента), осуществляющего мониторинг действий пользователей, данных о действиях пользователей, которые могут приводить к неправомерной передаче или распространению защищаемой информации.

К действиям, которые могут привести к неправомерной передаче или распространению защищаемой информации, относятся:

- передача защищаемой информации с использованием клиентского программного обеспечения сервисов коммуникации;

- копирование файлов на съемные машинные носители информации;

- вывод информации из файлов на печать.

При мониторинге действий пользователей со средств вычислительной техники могут быть получены данные, позволяющие осуществлять мониторинг всех каналов неправомерной передачи или распространения информации, указанных в 4.2.2, но только на конкретном средстве вычислительной техники пользователя.

5.2.4.1. К данным, которые могут быть получены при мониторинге действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов коммуникации, относятся:

- идентификатор средства вычислительной техники, на котором используется сервис коммуникации;

- идентификатор учетной записи пользователя, работающего с сервисом коммуникации средства вычислительной техники[14];

---

[14] Идентификатором может являться логическое имя учетной записи пользователя, используемое им при осуществлении идентификации в информационной (автоматизированной) системе.

- идентификаторы учетных записей пользователей (электронные адреса), участвующих в коммуникации;

- содержание получаемой и передаваемой с использованием сервисов коммуникации информации (в том числе прикрепляемых файлов);

- дата и время коммуникации.

5.2.4.2. К данным, которые могут быть получены при мониторинге действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов публикации на сетевых ресурсах, относятся:

- идентификатор средства вычислительной техники, с которого осуществлялось опубликование файла на сетевом ресурсе;

- идентификатор учетной записи пользователя, осуществившего опубликование файла на сетевом ресурсе;

- сведения о сервисе, используемом для опубликования файла на сетевом ресурсе;

- имя файла;

- тип файла (расширение);

- размер файла;

- сведения о пользователе (автор), создавшем файл;

- дата создания файла;

- содержимое файла;

- дата и время опубликования файла на сетевом ресурсе.

5.2.4.3. К данным, которые могут быть получены при мониторинге действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервисов печати файлов, относятся:

- идентификатор средства вычислительной техники, с которого осуществлялась печать;

- идентификатор учетной записи пользователя, осуществившего печать;

- сведения об устройстве, которому выдано задание на печать;

- имя файла, выданного на печать;

- тип файла (расширение);

- содержимое файла;

- дата и время печати.

5.2.4.4. К данным, которые могут быть получены при мониторинге действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием съемных машинных носителей информации, относятся:

- идентификатор средства вычислительной техники, к которому был подключен съемный машинный носитель информации;

- идентификатор учетной записи пользователя, осуществившего копирование файла;

- сведения о съемном машинном носителе информации, на (с) который (которого) осуществлялось копирование файла;

- имя файла;

- тип файла (расширение);

- размер файла;

- сведения о пользователе (автор), создавшем файл;

- дата создания файла;

- содержимое файла, копируемого на съемный машинный носитель информации;

- дата и время копирования.

5.2.4.5. К данным, которые могут быть получены при мониторинге действий пользователей на средствах вычислительной техники и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием общих файловых ресурсов, относятся:

- идентификатор средства вычислительной техники, с которого осуществлялось копирование файла на общий файловый ресурс;

- идентификатор учетной записи пользователя, осуществившего копирование файла на общий файловый ресурс;

- имя файла;

- тип файла (расширение);

- размер файла;

- сведения о пользователе (автор), создавшем файл;

- дата создания файла;

- содержимое файла, скопированного на общий файловый ресурс;

- сетевой адрес размещения файла на общем файловом ресурсе (включая каталог размещения);

- атрибуты файла;

- дата и время копирования файла.

5.2.5. Серверы ГИС МФ НО, на которых функционируют сервисы коммуникации, могут предоставлять данные для выявления признаков возможной неправомерной передачи или распространения информации.

При контроле передачи информации на серверах сервисов коммуникации могут быть получены данные, позволяющие осуществлять мониторинг только канала неправомерной передачи или распространения информации, связанного с использованием определенного сервиса коммуникации.

К данным, которые могут быть получены при мониторинге передачи информации на серверах сервисов коммуникации и могут быть использованы для выявления признаков неправомерной передачи или распространения информации, связанных с использованием сервиса коммуникации, относятся:

- сведения о сервисе коммуникации, с использованием которого передается информация;

- содержание информации, отправляемой и получаемой с использованием сервиса коммуникаций (в том числе прикрепляемых файлов);

- идентификаторы участников коммуникации;

- дата и время коммуникации.

5.2.6. Серверы ГИС МФ НО, на которых размещаются общие файловые ресурсы, имеют возможность предоставлять данные, позволяющие выявлять признаки хранения на общих файловых ресурсах файлов, содержащих информацию, которая в соответствии с установленными правилами хранения защищаемой информации не должна храниться на этих ресурсах.

От серверов ГИС МФ НО, на которых размещаются общие файловые ресурсы, могут быть получены данные, позволяющие осуществлять мониторинг только канала неправомерной передачи или распространения информации, связанного с использованием общих файловых ресурсов.

К данным, которые могут быть получены от таких серверов и могут быть использованы для выявления признаков неправомерной передачи или

распространения информации, связанных с размещением файлов на общих файловых ресурсах, относятся:

- имя файла;
- тип файла (расширение);
- размер файла;
- сведения о пользователе (автор), создавший файл;
- дата создания файла;
- дата и время размещения на общем файловом ресурсе;
- контрольная сумма файла;
- содержимое файлов, хранящихся на общих файловых ресурсах;
- сетевые адреса для размещения файлов на общих файловых ресурсах;
- идентификаторы учетных записей пользователей, сохранявших файлы на общем файловом ресурсе.

5.2.7. Средства защиты информации, используемые на физических или логических границах ГИС МФ НО, могут применяться для раскрытия преобразованного (закрытого) сетевого трафика, который передается между узлами ГИС МФ НО и внешними информационными ресурсами в преобразованном (закрытом) виде с целью анализа передаваемой информации на предмет правомерности такой передачи[15].

5.2.8. Данные, необходимые для защиты информации от неправомерной передачи или распространения из ГИС МФ НО, могут быть получены от разных объектов мониторинга. Данные, которые могут быть получены с телекоммуникационного оборудования, могут быть получены и на средствах вычислительной техники при мониторинге действий пользователей, но в данном случае мониторинг обеспечивается на всех средствах вычислительной техники в ГИС МФ НО посредством программного обеспечения (агента).

5.3. Способы взаимодействия с объектами мониторинга.

5.3.1. Основными способами взаимодействия с объектами мониторинга являются:

---

[15] Случаем такого взаимодействия является использование межсетевого экрана для раскрытия зашифрованного сетевого трафика, проходящего через межсетевой экран, и отправка копии раскрытого сетевого трафика в средство защиты информации от утечки для анализа.
Каналы неправомерной передачи или распространения информации, контролируемые с использованием средств защиты информации, используемых на физических или логических границах информационной (автоматизированной) системы, и состав данных, которые могут быть получены от них, совпадают соответственно с каналами неправомерной передачи или распространения информации, контролируемыми с использованием теле-коммуникационного оборудования, и составом данных, которые могут быть получены от телекоммуникационного оборудования.

- получение копии сетевого трафика;

- использование программного обеспечения (агента), осуществляющего контроль действий пользователей;

5.3.2. Получение копии сетевого трафика используется, если в ГИС МФ НО в качестве объектов мониторинга используется телекоммуникационное оборудование, которое предоставляет копию сетевого трафика для анализа информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов. Также такой способ может применяться, если в ГИС МФ НО в качестве объектов мониторинга применяются средства защиты информации, используемые на физических или логических границах ГИС МФ НО, которые обеспечивают раскрытие преобразованного (закрытого) сетевого трафика и предоставляют копию раскрытого трафика для анализа информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов. Если в ГИС МФ НО отсутствует телекоммуникационное оборудование и средства защиты информации, имеющие возможность предоставлять копию сетевого трафика, то в ГИС МФ НО могут использоваться специализированные средства перехвата сетевого трафика, устанавливаемые в разрыв каналов связи.

5.3.3. Программное обеспечение (агент) используется на средствах вычислительной техники пользователей и обеспечивает получение от применяемого на средстве вычислительной техники программного обеспечения, в том числе средств защиты информации, данных о действиях пользователей, которые могут приводить к неправомерной передаче или распространению защищаемой информации:

- вывод файла на печать;

- копирование файла на съемный машинный носитель информации;

- копирование файла на сетевой ресурс;

- передача информации с использованием клиентского программного обеспечения компонентов сервисов коммуникации, установленных на его средстве вычислительной техники (в том числе с вложенными файлами);

- передача файлов с использованием клиентского программного обеспечения на различные файловые ресурсы (файловые хранилища, облачные хранилища);

- отправка информации или передача файла с использованием веб-интерфейса сервиса коммуникации;

- опубликование файлов или отдельных их частей, содержащих защищаемую информацию, на файловых ресурсах.

5.3.4. Перехват сетевого трафика, поступающего от сервисов коммуникации, используется в случае, когда в качестве объектов мониторинга могут использоваться серверы, на которых функционируют сервисы коммуникации. Данный способ предусматривает перехват информации (в том числе с вложенными файлами) с целью анализа правомерности обмена такой информацией пользователями сервиса коммуникации.

5.4. Уровень выявления признаков возможной неправомерной передачи или распространения.

5.4.1. Выявление признаков возможной неправомерной передачи или распространения предусматривает выполнение следующих действий:

- предварительная обработка информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов;

- анализ содержания информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов;

- проверка наличия признаков нарушения правил обработки информации;

- реагирование на выявленные признаки нарушения правил обработки информации.

5.4.2. Предварительная обработка информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов требуется для извлечения информации, которая в исходном виде не пригодна для проведения анализа. Такая предварительная обработка необходима, если требуется проводить анализ текстовой информации в следующих файлах:

- файлы, формат которых предусматривает хранение текстовой информации в преобразованном виде;

- архивные файлы, в состав которых включены файлы, содержащие текстовую информацию;

- графические файлы, в которых содержится текстовая информация.

При организации защиты информации от неправомерной передачи или распространения должна быть обеспечена возможность проведения предварительной обработки основных типов текстовых, архивных, графических файлов, используемых в ГИС МФ НО.

5.4.3. Анализ содержания информации, передаваемой с использованием сервисов коммуникации, и передаваемых файлов проводится с целью определения, осуществляется ли передача информации, в отношении которой требуется осуществлять мониторинга правомерности её копирования из информационной (автоматизированной) системы (в случае вывода файла на печать или его копирования на съемный машинный носитель информации), правомерности передачи такой информации другим пользователям информационной (автоматизированной) системы или за её пределы, а также правомерности её хранения на средствах вычислительной техники пользователей, серверах ГИС МФ НО и на общем файловом ресурсе.

Основными методами анализа являются:

- морфологический контентный анализ;
- распознавание документов по графическому образцу;
- распознавание цифровых отпечатков в документе;
- атрибутный анализ файлов.

Методы анализа реализуются средствами защиты информации от утечки. Средства защиты информации от утечки являются многокомпонентными. Состав используемых компонентов определяется в зависимости от вида защищаемой информации и используемой ГИС МФ НО. Требования средствами защиты информации от утечки определяются нормативными правовыми актами ФСТЭК России.

5.4.4. Выявление нарушений.

Проверка наличия признаков нарушения правил обработки информации выполняется, если в результате анализа информации, передаваемой с использованием сервиса коммуникаций, или анализа содержимого файла выявлен вид информации, подлежащий защите информации от неправомерной передачи или распространения.

Проверка наличия признаков нарушения правил обработки защищаемой информации в первую очередь предусматривает мониторинг правомерности со стороны определенных пользователей осуществлять копирование определенных видов информации из информационной (автоматизированной) системы (в случае вывода файла на печать или его копирование на съемный машинный носитель информации), передачу такой информации другим пользователям информационной (автоматизированной) системы или за её пределы.

В случае проведения анализа содержимого файлов на серверах ГИС МФ НО, предназначенных для размещения общих файловых ресурсов, осуществляется проверка правомерности хранения информации определенного вида на соответствующем общем файловом ресурсе.

5.4.5. Реагирование на выявленные признаки нарушения правил обработки защищаемой информации.

Способ реагирования на выявленные признаки нарушение правила обработки защищаемой информации зависит от выявленного нарушения.

При выявлении признаков неправомерного копирования определенных видов информации из ГИС МФ НО (в случае вывода на печать или копирования информации на съемный машинный носитель информации), неправомерной передачи такой информации другим пользователям ГИС МФ НО или за её пределы могут реализовываться следующие способы реагирования:

- отправка уведомления о нарушении уполномоченному лицу (администратору безопасности, руководителю пользователя ГИС МФ НО, осуществившего передачу файла или информации, или иным лицам);

- отправка уведомления о нарушении пользователю ГИС МФ НО, осуществившему передачу файла или информации;

- регистрация события безопасности о нарушении в журнале событий безопасности;

- блокирование неправомерного копирования информации из ГИС МФ НО или неправомерной передачи такой информации (при наличии возможности).

При выявлении нарушения правил хранения защищаемой информации на общих сетевых ресурсах должна обеспечиваться возможность реализации следующих способов реагирования:

- отправка уведомления о нарушении уполномоченному лицу (администратору безопасности, руководителю пользователя ГИС МФ НО, осуществившего размещение защищаемой информации, или иным лицам);

- отправка уведомления о нарушении пользователю ГИС МФ НО, осуществившему размещение защищаемой информации;

- регистрация события безопасности о нарушении в журнале событий безопасности;

- активные действия в отношении защищаемой информации (в том числе, перемещение файла в каталог, заданный пользователем, уполномоченным выполнять действия по мониторингу неправомерной передачи или распространения информации, запрет доступа к файлам и иные действия).

5.5. Уровень представления результатов выявления признаков возможной неправомерной передачи или распространения.

5.5.1. На уровне представления результатов выявления признаков возможной неправомерной передачи или распространения осуществляется просмотр сведений о всех зарегистрированных событиях безопасности, полученных по результатам выявления признаков неправомерной передачи или распространения информации. Событие безопасности содержит следующие сведения:

- уникальный идентификатор события безопасности;

- дата и время регистрации события безопасности;

- уровень важности события безопасности (определяется в соответствии с ГОСТ Р 59548-2022);

- субъект, действия которого привели к регистрации события безопасности;

- действие, которое привело к регистрации события безопасности;

- условия, которые стали причиной регистрации события безопасности (обнаруженные ключевые слова или иные условия);

- объект мониторинга, на котором зарегистрировано событие безопасности;

- содержимое фрагмента объекта мониторинга, которое привело к регистрации события безопасности;

- способ передачи информации[16];

- субъект, являющийся получателем[17].

5.5.2. На уровне представления результатов выявления признаков возможной неправомерной передачи или распространения формируются как минимум следующие отчеты:

---

[16] Способ передачи информации может отсутствовать в составе представляемой информации в случае регистрации события безопасности, связанного с обнаружением неправомерной печати файла, неправомерного копирования файла на съемный машинный носитель информации и неправомерного хранения файла на общем файловом ресурсе.

[17] Сведения о субъекте, являющемся получателем, не указывается в случае регистрации события безопасности, связанного с обнаружением неправомерной печати файла, неправомерного копирования файла на съемный машинный носитель информации и неправомерного хранения файла на общем файловом ресурсе.

- о зарегистрированных событиях безопасности;

- о пользователях.

5.5.2.1. Отчет о зарегистрированных событиях безопасности представляет собой консолидированную информацию в наглядном виде за определенный период времени, которая демонстрирует:

- общее количество событий безопасности;

- распределение событий безопасности по различным показателям (уровню важности, группам пользователей, видам информации)[18].

5.5.2.2. Отчет о пользователях представляет собой консолидированную информацию о нарушениях пользователя (пользователей), его (их) идентификационные данные, взаимодействиях с другими пользователями и иных действиях за определенный период времени, в том числе:

- идентификационные данные пользователя (например, ФИО, должность, адрес электронной почты и иная информация);

- сведения о событиях безопасности, которые зарегистрированы в результате действий пользователя, включая дату и время возникновения событий безопасности;

- сведения о взаимодействиях пользователя;

- сведения об информации, переданной и (или) полученной пользователем;

- сведения о подключении съемных машинных носителей информации и выводе на них информации пользователем;

- сведения о выводе информации на печать пользователем;

- иные сведения.

6. Порядок применения средств защиты информации от утечки из информационной (автоматизированной) системы

6.1. При планировании применения в ГИС МФ НО средств защиты информации от утечки учитывается, необходимость обеспечения возможности взаимодействия с объектами мониторинга, выбранными в соответствии с пунктом 5.1, с учётом возможных каналов неправомерной передачи или распространения информации.

[18] Формами представления отчета являются: таблица, список, граф связей и иные.

Входящее в состав средств защиты информации от утечки программное обеспечение (агент), осуществляющее контроль действий пользователей, предоставляет возможность выполнения своих функций в среде операционных систем, применяемых на средствах вычислительной техники, с которыми работают пользователи ГИС МФ НО. Средство защиты информации от утечки предоставляет возможность перехвата информации от тех сервисов коммуникации, которые применяются в ГИС МФ НО.

6.2. Применяемое в ГИС МФ НО средство защиты информации от утечки должно содержать функции безопасности, которые позволяют реализовать защиту информации от неправомерной передачи или распространения в соответствии с положениями раздела 5.

6.3. Для выявления признаков возможной неправомерной передачи или распространения информации, в соответствии с пунктом 5.3.1, в средстве защиты информации от утечки должны быть определены объекты, содержащие защищаемую информацию, и политики безопасности информации.

Описание объектов, содержащих защищаемую информацию, производится для обеспечения возможности идентификации информации, отнесенной к видам информации, подлежащим защите информации от неправомерной передачи или распространения. Описание объекта, как минимум, должно включать следующие характеристики:

- наименование объекта;
- признаки, с использованием которых идентифицируется объект;
- вид информации, которую содержит объект[19].

В политике безопасности информации определяется совокупность правил, которые характеризуются условиями, используемыми для выявления нарушения, и действиями, предпринимаемыми в случае обнаружения нарушения.

В качестве условий могут определяться допустимые места хранения определенных объектов такой информации на общих сетевых ресурсах ГИС МФ НО, списки лиц, имеющих право передавать или получать соответствующий вид информации, и иные условия. В качестве действий,

[19] В качестве объекта, содержащего защищаемую информацию, может быть определен файл пояснительной записки технического проекта, который содержит информацию о технических характеристиках объекта интеллектуальной собственности. В качестве признаков, с использованием которых может быть идентифицирован объект, может выступать составленный список лексем, которые содержатся в документе.

которые предпринимаются в качестве реагирования на выявленные признаки нарушения, могут быть определены следующие: перемещение файла с защищаемой информацией в определенный каталог, блокирование передачи информации с использованием сервиса коммуникации или иные действия.

6.4. Средство защиты информации от утечки[20] при обеспечении возможности передачи информации о зарегистрированных событиях безопасности в систему управления событиями безопасности должно выступать в качестве источника данных мониторинга в соответствии с ГОСТ Р 59547-2021.

6.5. При эксплуатации средств защиты информации от утечки обеспечивается принятие мер, направленных на предотвращение: потери данных о зарегистрированных событиях, связанных с обнаружением признаков неправомерной передачи или распространения информации; выхода из строя средства защиты информации от утечки или его элементов, или иных сбоев, повлекших к нарушению защиты информации от неправомерной передачи или распространения. В качестве таких мер необходимо рассматривать:

- предупреждение (сигнализация, индикация) уполномоченного пользователя средства защиты информации от утечки при заполнении установленной части (процент или фактическое значение) объема памяти для хранения данных;
- разделение архива данных на оперативный и долгосрочный;
- архивирование (резервное копирование) данных (части данных) на съемные машинные носители информации, в системы хранения данных, на специализированные устройства или на отдельные серверы;
- дублирование (кластеризация) компонентов средства защиты информации.

6.6. Средство защиты информации от утечки может содержать в своем составе функцию инспекции файловых ресурсов[21].

Инспекция файловых ресурсов применяется в ГИС МФ НО для выявления нарушений установленных правил хранения защищаемой информации, которые могут привести к её неправомерной передаче или распространению. Данный способ предусматривает сканирование ГИС МФ НО с целью

---

[20] При необходимости может быть предусмотрена передача информации о зарегистрированных событиях безопасности средством защиты информации от утечки в систему управления инцидентами в качестве возможного признака инцидента в соответствии с ГОСТ Р 59710-2022.

[21] Инспекция файловых ресурсов относится к уровню взаимодействия с серверами файловых ресурсов как объектов мониторинга.

выявления имеющихся в ней общих сетевых ресурсов и анализа содержимого файлов, размещенных на этих ресурсах, для выявления нарушений установленных правил хранения защищаемой информации[22].

6.7. Средство защиты информации от утечки может содержать в своем составе функцию поведенческого анализа пользователей ГИС МФ НО. Функция поведенческого анализа пользователей ГИС МФ НО может быть реализована в виде отдельного средства[23].

Результаты поведенческого анализа целесообразно учитывать при формировании политик безопасности информации, в соответствии с которыми средство защиты информации от утечки осуществляет обнаружение событий безопасности, связанных с неправомерной передачей или распространением информации.

7. Рекомендации по защите данных, собираемых и формируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения из информационной (автоматизированной) системы

7.1. В информационной (автоматизированной) системе должна осуществляться защита данных, собираемых и формируемых в рамках мероприятий по защите от неправомерной передачи или распространения информации.

К данным, собираемым в рамках мероприятий по защите информации от неправомерной передачи или распространения, для которых требуется защита информации, относятся:

- файлы, содержащие оригиналы документов, используемые для создания графических образцов и цифровых отпечатков;

- информация из информационной (автоматизированной) системы, получаемая для проведения анализа на предмет неправомерной передачи или распространения.

---

[22] Нарушением правил хранения является факт обнаружения на сетевом файловом ресурсе файла, содержимое которого в соответствии с установленными правилами хранения защищаемой информации не предназначено для хранения на данном сетевом файловом ресурсе.

[23] Функция поведенческого анализа основывается на данных, собираемых средством защиты информации от утечки, и относится к уровню представления результатов выявления признаков возможной неправомерной передачи или распространения.

К данным, формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения, для которых требуется защита информации, относятся:

- политики безопасности, настроенные для применения метода морфологического контентного анализа;

- графические образцы документов, формируемые для применения метода распознавания документов по графическому образцу;

- события безопасности, связанные с обнаружением признаков неправомерной передачи или распространения информации;

- отчеты, формируемые в процессе функционирования средства защиты информации от утечки.

7.2. Для защиты данных, собираемых и формируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения, реализуют следующие меры защиты информации:

- идентификация и аутентификация пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- управление идентификаторами пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- управление средствами аутентификации (аутентификационной информацией) пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- управление учетными записями пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- защита аутентификационной информации пользователей, осуществляющих доступ к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения, в процессе её ввода, для аутентификации от возможного использования лицами, не имеющими на это полномочий;

- управление доступом пользователей к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- ограничение неуспешных попыток получения доступа пользователей при доступе к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- регистрация событий безопасности, связанных с доступом к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- определение типов съемных машинных носителей информации, на которые разрешен вывод данных, собираемых и формируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения;

- определение категорий пользователей, которым предоставлены полномочия выводить данные, собираемые и формируемые в рамках мероприятий по защите информации от неправомерной передачи или распространения, на съемные машинные носители информации;

- мониторинг вывода данных, собираемых и формируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения, на съемные машинные носители информации.

Должна обеспечиваться регистрация следующих типов событий безопасности, связанных с доступом к данным, собираемым и формируемым в рамках мероприятий по защите информации от неправомерной передачи или распространения, которые установлены в ГОСТ Р 59548-2022:

- прохождение идентификации и аутентификации субъекта доступа;

- управление учетными записями пользователей;

- управление средствами аутентификации;

- управление атрибутами доступа;

- получение доступа к защищаемой информации;

- подключение съемных машинных носителей информации;

- вывод данных, собираемых и формируемых в рамках мероприятий по защите информации от неправомерной передачи или распространения, на съемные машинные носители информации;

- управление (администрирование) функциями безопасности;

- управление журналами событий безопасности.

Дополнительно могут регистрироваться все действия, которые средство защиты информации от утечки выполняет в отношении полученной

для анализа защищаемой информации информационной (автоматизированной) системы.

7.3. Полученная для анализа защищаемая информация информационной (автоматизированной) системы может сохраняться в каталогах или базах данных, доступ к которым ограничен только допущенными к такой информации лицами, определенными владельцем информации или оператором информационной (автоматизированной) системы.

7.4. Защита данных, собираемых и формируемых в процессе функционирования средства защиты информации от утечки, осуществляется исходя из классов защищенности (категорий значимости, уровней защищенности информации) ГИС МФ НО, в которых применяется средство защиты информации от утечки.

7.5. Результаты выявленных событий безопасности, связанных с неправомерной передачей или распространением защищаемой информации, могут использоваться для:

- проведения служебной проверки в отношении пользователей ГИС МФ НО, в процессе работы которых обнаружены признаки возможной неправомерной передачи или распространения информации[24];

- передачи результатов служебных проверок в уполномоченные федеральные органы исполнительной власти Российской Федерации, в установленных законом порядке случаях[25].

К утечке, несанкционированному доступу, неправомерной передаче или распространению защищаемой информации из ГИС МФ НО могут приводить следующие группы угроз безопасности информации:

- угрозы безопасности информации, связанные с неправомерной передачей или распространением защищаемой информации пользователями, имеющими права доступа к ней в информационных (автоматизированных) системах;

- угрозы безопасности информации, связанные с осуществлением внутренними и внешними нарушителями, попыток получения

---

[24] Проведение служебных проверок может быть регламентировано документами, утвержденными у участников бюджетного процесса.

[25] Порядок привлечения к ответственности, в случае наличия состава правонарушения, установлен законодательством Российской Федерации. Информация, собранная с использованием средства защиты информации от утечки, может быть принята в качестве доказательств правонарушения при условии соответствии требованиям законодательства Российской Федерации к оформлению сбора соответствующих материалов.

несанкционированного доступа к информации, к которой они не имеют прав доступа в ГИС МФ НО;

- угрозы безопасности информации, связанные с использованием нарушителем технических каналов утечки защищаемой информации.