



**АДМИНИСТРАЦИЯ
ИВНЯНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
БЕЛГОРОДСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ**
Посёлок Ивня

6 февраля 2026 г.

№ 59-па

**Об утверждении регламента
получения, рассмотрения,
обработки, анализа,
информирования и реализации
организационных и технических
мер, направляемых Федеральной
службой по техническому
и экспортному контролю**

Во исполнение подпункта «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 года № 250 (в редакции от 13 июня 2024 года № 500) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» Администрация Ивнянского муниципального округа **п о с т а н о в л я е т:**

1. Утвердить регламент получения, рассмотрения, обработки, анализа, информирования и реализации организационных и технических мер, направляемых Федеральной службой по техническому и экспортному контролю (приложение).

2. Контроль за исполнением постановления возложить на заместителя Главы округа – руководителя аппарата Администрации Ивнянского муниципального округа Позднякову Н.А.

**Глава
Ивнянского муниципального округа
Белгородской области**



И.А. Щепин

Приложение**УТВЕРЖДЁН**

постановлением Администрации
Ивнянского муниципального округа
от «06» 02 2026 № 59-на

РЕГЛАМЕНТ

**получения, рассмотрения, обработки, анализа, информирования
и реализации организационных и технических мер, направляемых
Федеральной службой по техническому и экспортному контролю**

1. Общие положения**1.1. Сфера применения**

Настоящий регламент (далее – Регламент) определяет порядок организации деятельности Администрации Ивнянского муниципального округа при получении, рассмотрении, анализе и реализации организационных и технических мер в области информационной безопасности, направляемых Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение подпункта «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 года № 250 (в редакции от 13 июня 2024 года № 500) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Указанный подпункт обязывает муниципальные органы Ивнянского муниципального округа, а также подведомственные им учреждения (далее – органы-исполнители и подведомственные учреждения) обеспечить незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой по техническому и экспортному контролю в пределах её компетенции и направляются с учётом меняющихся угроз в информационной сфере.

Данный регламент распространяет своё действие на органы-исполнители и подведомственные учреждения.

1.2. Субъекты, участвующие в процессе

В процессе получения и реализации мер, направляемых ФСТЭК России, участвуют следующие структурные подразделения и органы:

– информационно-технический отдел аппарата Администрации Ивнянского муниципального округа (далее – ИТ отдел) – выполняет функции головного подразделения по координации и контролю деятельности в области информационной безопасности;

– ОГБУ «Белгородский информационный фонд» обеспечивает функционирование и защищённость информационно-технологической инфраструктуры и информационных систем Администрации Ивнянского муниципального округа и подведомственных учреждений;

— органы-исполнители и подведомственные учреждения, являющиеся владельцами или операторами информационных систем и информационных ресурсов (региональные, государственные информационные системы, информационные системы персональных данных, иные информационные и автоматизированные системы, информационные ресурсы опубликованные в информационно-телекоммуникационной сети и т.д.), субъекты критической информационной инфраструктуры, иные организации, являющиеся пользователями информационной инфраструктуры Администрации Ивнянского муниципального округа.

1.3. Основные принципы

Деятельность по получению и реализации мер ФСТЭК России осуществляется на основе следующих принципов:

- незамедлительность — означает необходимость быстрого реагирования на поступившие меры с целью устранения выявленных угроз в информационной инфраструктуре;
- полнота — требует охвата всех необходимых направлений деятельности органов-исполнителей и подведомственных учреждений;
- взаимодействие и координация — предполагает согласованную работу всех органов-исполнителей и подведомственных учреждений, а также ОГБУ «Белгородский информационный фонд», как организации, обеспечивающей функционирование и защищённость информационной инфраструктуры Администрации Ивнянского муниципального округа и подведомственных учреждений;
- документирование и прозрачность — обеспечивает чёткое фиксирование всех процедур, связанных с получением, обработкой и реализацией организационно-технических мер ФСТЭК России;
- ответственность — устанавливает чёткую систему учёта деятельности должностных лиц;
- разделение ответственности между Администрацией Ивнянского муниципального округа и подведомственными учреждениями — основывается на их компетенции и полномочиях.

1.4. Целевые задачи

Целью настоящего Регламента является организация системного и оптимизированного процесса получения организационных и технических мер, направляемых ФСТЭК России, и обеспечение их незамедлительной реализации в Ивнянском муниципальном округе с целью повышения устойчивости информационных ресурсов к постоянно меняющимся и возникающим угрозам в информационной сфере. Достижение этой цели предполагает решение следующих задач:

- установление чётких сроков и ответственных должностных лиц на каждом этапе процесса обработки поступивших мер;
- обеспечение надлежащего анализа содержания и применимости полученных рекомендаций ФСТЭК России к условиям функционирования

информационной инфраструктуры органов-исполнителей и подведомственных организаций;

- оперативная передача информации заинтересованным сторонам;
- порядок контроля за ходом реализации мер и проверкой их практического применения;
- подготовка достоверных отчётных материалов о проделанной работе и представление их в установленном порядке во ФСТЭК России.

2. Порядок получения и первичной обработки мер

2.1. Каналы и способы получения мер

Организационные и технические меры, определяемые ФСТЭК России, направляются в Администрацию Ивнянского муниципального округа посредством электронной почты или через иные официальные каналы взаимодействия с региональными органами власти. Информационные материалы, содержащие сведения о мерах, поступают в виде писем ФСТЭК России, методических документов, рекомендаций, инструкций, приложений к официальным письмам или телеграммам.

2.2. Первичный анализ и оценка

Начальник информационно-технического отдела аппарата Администрации Ивнянского муниципального округа (далее – начальник ИТ отдела) незамедлительно (не позже одного рабочего дня со дня получения информации) проводит её детальное изучение и первичный анализ.

При проведении анализа учитываются характер и содержание направляемых мер, их отнесение к организационным или техническим мерам защиты информации, сферы угроз информационной безопасности, на устранение которых направлены данные меры. Анализ включает оценку структуры органов-исполнителей, на которые распространяются рекомендации ФСТЭК России, срочность выполнения и степень критичности указанных мер для информационной безопасности Ивнянского муниципального округа.

На основе проведённого анализа начальник ИТ отдела определяет, требуется ли немедленное направление мер в органы-исполнители для локальной реализации на уровне отдельных органов или речь идёт об общесистемных мерах, касающихся всей информационной инфраструктуры Администрации Ивнянского муниципального округа и подведомственных учреждений.

3. Рассмотрение и разработка плана действий

3.1. Процесс детального рассмотрения

После завершения первичного анализа начальник ИТ отдела организует процесс детального рассмотрения полученной информации совместно со специалистами в области информационной безопасности, при необходимости обсуждается содержание мер с представителями ОГБУ «Белгородский информационный фонд» для получения их экспертного мнения о технической

применимости и необходимости внесения изменений. На этом этапе уточняются вопросы, связанные с возможностью и целесообразностью реализации полученных мер в условиях функционирования информационной инфраструктуры органов-исполнителей, оценивается необходимость дополнительных ресурсов, сроков и технического обеспечения для выполнения рекомендаций ФСТЭК России.

3.2. Разработка плана действий

На основе проведённого анализа ИТ отдел при необходимости разрабатывает план работы по реализации мер информационной безопасности. План включает определение этапов работ, сроков их выполнения, ответственных должностных лиц и исполнителей, необходимых для достижения целей, ресурсов, технических решений и организационных мероприятий. В плане при необходимости предусматриваются меры по взаимодействию различных структурных подразделений Администрации Ивнянского муниципального округа, координация деятельности органов-исполнителей и подведомственных учреждений, обеспечение необходимого информационного обмена между участниками процесса.

3.3. Фиксация и эскалация технических ограничений

В случае выявления объективной невозможности выполнения меры ФСТЭК России в полном объёме или её выполнения в установленные сроки (в связи с отсутствием необходимых обновлений/исправлений, архитектурными ограничениями, риском нарушения работоспособности критических систем) в ходе детального рассмотрения или планирования реализации, ИТ отдел документирует выявленное ограничение с техническим обоснованием, рассматривает и документирует возможные компенсирующие меры, вносит данную информацию в план действий с пометкой о невозможности полного выполнения и указанием принятых компенсирующих мер, информирует о данных ограничениях и предложенных решениях вышестоящее руководство для последующего согласования с ФСТЭК России.

4. Информирование заинтересованных сторон

4.1. Направление мер органам-исполнителям и подведомственным учреждениям

При определении необходимости локальной реализации полученных от ФСТЭК России мер ИТ отдел передаёт соответствующую информацию в органы-исполнители, в сферу деятельности которых входит решение выявленных проблем информационной безопасности. Направление информации осуществляется посредством электронной почты и официальной рассылки, в которой указывается наименование и содержание полученных мер, срок их реализации, требуемые от органов-исполнителей. При этом органам-исполнителям необходимо организовать информирование всех подведомственных им учреждений с уточнением, какие конкретно работы должны быть проведены для реализации организационно-технических мер ФСТЭК России.

4.2. Направление общих мер структурным подразделениям

Организационные и технические меры, касающиеся функционирования общих информационно-технических систем и инфраструктуры органов-исполнителей, направляются начальником ИТ отдела в адрес руководителей органов-исполнителей и сопровождаются пояснением содержания, целей и необходимости выполнения, технической обоснованием применимости к имеющейся инфраструктуре. Начальник ИТ отдела уточняет, какие именно информационные системы и компоненты инфраструктуры требуют внесения изменений, какие данные и процедуры должны быть защищены, какова степень критичности выполняемых работ.

5. Реализация организационных и технических мер

5.1. Организация работ

Руководители органов-исполнителей, ответственные за информационную безопасность, на основе полученной от ИТ отдела информации организуют выполнение полученных от ФСТЭК России мер в рекомендуемые сроки и в части функционирования информационно-технической инфраструктуры и информационных систем. Организация работ предполагает определение состава специалистов, обладающих необходимыми знаниями и опытом для выполнения работ, и назначение ответственного за процесс реализации мер. Организация включает разработку или уточнение технических спецификаций и требований к выполняемым работам, разработку при необходимости плана выполнения работ с указанием сроков прохождения отдельных этапов, необходимости взаимодействия с ОГБУ «Белгородский информационный фонд» и иными организациями, привлекаемыми к выполнению работ.

5.2. Выполнение технических работ

Процесс выполнения мер включает проведение необходимых технических работ по модификации информационных систем, обновлению программного обеспечения, установке средств защиты информации, внесению изменений в конфигурацию систем обнаружения и предупреждения атак, усиление механизмов аутентификации и авторизации, внедрение дополнительных каналов защиты от компьютерных атак.

5.3. Контроль хода реализации

Начальник ИТ отдела осуществляет постоянный контроль за ходом реализации полученных мер. Контроль включает отслеживание соблюдения установленных сроков выполнения работ, проверку качества выполняемых работ и соответствие их содержания рекомендациям ФСТЭК России, выявление и устранение возникающих препятствий и проблем, своевременное информирование о статусе выполнения мер заместителя Главы округа – руководителя аппарата Администрации Ивнянского муниципального округа, на которого возложены полномочия по обеспечению информационной безопасности, в том числе

по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. При необходимости начальник ИТ отдела координирует работу различных подразделений для ускорения процесса реализации мер, а также осуществляет промежуточные проверки соответствия выполняемых работ установленным требованиям.

5.4. Реализация мер в органах-исполнителях и подведомственных учреждениях

Органы-исполнители, получившие от ИТ отдела информацию о необходимости реализации конкретных мер по защите информации в их ведомственных информационно-телекоммуникационных системах, а также подведомственные учреждения проводят работы в соответствии с полученными рекомендациями. Реализация мер в упомянутых выше организациях может включать как организационные меры, такие как издание приказов и распоряжений, разработка новых процедур и положений, проведение обучения и инструктажа персонала, так и технические работы, осуществляемые с привлечением специалистов или организаций, имеющих соответствующие лицензии на осуществление деятельности по технической защите информации. Каждый руководитель органа-исполнителя несёт ответственность за полноту и качество выполнения возложенных на него мер.

6. Контроль и проверка реализации мер

6.1. Методология проверки

ИТ отдел осуществляет проверку практического выполнения полученных от ФСТЭК России мер с целью убедиться в том, что реализованные меры действительно обеспечивают устранение выявленных угроз информационной безопасности. Проверка осуществляется на основе анализа представленных отчётов о проделанной работе, осмотра и тестирования реализованных технических решений, изучения документации по выполненным работам, проведения интервью с должностными лицами, ответственными за реализацию мер. При проведении проверки особое внимание уделяется функциональности внедрённых средств и механизмов защиты информации, правильности и полноте их настройки и конфигурации, соответствию реализованных решений требованиям и рекомендациям ФСТЭК России, выполнение утверждённого плана работы по реализации мер информационной безопасности.

6.2. Сроки и периодичность проверок

Первичная проверка выполнения мер ФСТЭК России осуществляется в течение 5 дней после получения сведений об окончании работ от исполнителей (если иные сроки не указаны в направляемых ФСТЭК России мерах). Для критических и срочных мер проверка может быть проведена немедленно после их выполнения. При необходимости проводятся дополнительные контрольные проверки спустя установленные периоды времени, позволяющие убедиться в стабильности функционирования реализованных решений и отсутствии регрессии

защитных свойств информационных систем. Периодичность проведения контрольных проверок определяется начальником ИТ отдела в зависимости от характера и критичности уязвимостей в информационной инфраструктуре организации.

7. Подготовка отчётной информации

7.1. Сбор информации о ходе реализации мер

Начальник ИТ отдела поручает сотрудникам ИТ отдела осуществить сбор информации о ходе реализации мероприятий, полученных от ФСТЭК России. Информация подлежит сбору от органов-исполнителей и должна включать сведения о результатах выполненных работ, сроках их выполнения, возникших трудностях и мерах, принятых для их устранения, использованных ресурсах и средствах защиты информации, а также о результатах проведённых тестирований и проверок.

7.2. Требования к отчётам об исполнении

Начальник ИТ отдела направляет в ФСТЭК России отчёт о реализации полученных мер, включающий сведения о виде и сроках выполнения работ, технических решениях и средствах защиты информации, которые были внедрены, описание трудностей и ограничений, выявленных в ходе реализации, принятых компенсирующих мерах и результатах работ. Отчёт направляется посредством электронной почты и официальной рассылки.

Органы-исполнители, на которые были возложены обязанности по реализации отдельных мер защиты информации, направляют в ИТ отдел информацию о проделанной работе в форме отчёта или справки, с информацией о реализованных организационных и технических мерах, об изданных приказах и распоряжениях, проведённых процедурах и внесённых положениях, а также о выполненных работах по модификации информационных систем. Отчёты направляются в ИТ отдел в установленные сроки посредством официальной рассылки и электронной почты Администрации Ивнянского муниципального округа.

7.3. Анализ отчётной информации

ИТ отдел проводит анализ полученных от органов-исполнителей отчётов о выполнении мер. При проведении анализа специалисты ИТ отдела изучают содержание отчётов, проверяют адекватность описанных в них действий и достаточность предпринятых мер для устранения выявленных угроз информационной безопасности, оценивают соответствие выполненных работ рекомендациям ФСТЭК России. При наличии в отчётах указаний на возникшие проблемы или невозможность выполнения отдельных мер проводится детальное выяснение причин и разрабатываются рекомендации по их устранению.

7.4. Подготовка итогового ответа

На основе собранной информации и проведённого анализа отчётов начальник или специалисты ИТ отдела готовят итоговый ответ во ФСТЭК России с информацией о том, какие именно меры были получены от ФСТЭК России, о предпринятых для их реализации мероприятиях, внедрённых организационных и технических решениях, достигнутых результатах.

7.5. Каналы и способы направления ответов

Подготовленный ответ во ФСТЭК России направляется посредством электронной почты с одновременным занесением документа в систему электронного документооборота Правительства Белгородской области. При направлении письма в электронной форме указываются все необходимые реквизиты, подпись отправителя выполняется электронной подписью в соответствии с действующим законодательством Российской Федерации. Копия направленного письма сохраняется в архиве ИТ отдела для целей ведения учёта и справочной информации.

7.6. Сроки представления отчётности

Отчёт о результатах реализации мер, полученных от ФСТЭК России, направляется в федеральное ведомство в сроки, устанавливаемые в сопроводительных письмах и рекомендациях ФСТЭК России.

При получении срочных или критических мер сроки представления отчётности могут быть сокращены. В случаях, когда реализация полученных мер требует продолжительного времени, допускается направление промежуточных отчётов о ходе выполнения работ с указанием ожидаемых сроков завершения.

8. Взаимодействие между органами и подразделениями

8.1. Координационные механизмы

Эффективное взаимодействие между ИТ отделом, структурными подразделениями, органами-исполнителями и подведомственными учреждениями обеспечивается посредством регулярного обмена информацией, проведения координационных совещаний и консультаций, использования системы электронного документооборота и электронной почты Администрации Ивнянского муниципального округа для передачи документов. Начальник ИТ отдела осуществляет роль координатора процесса получения и реализации мер, организует взаимодействие между участниками и обеспечивает своевременное прохождение информации через все необходимые инстанции.

8.2. Каналы обмена информацией

Основным каналом обмена информацией между ИТ отделом и структурными подразделениями является система электронного документооборота Правительства Белгородской области, позволяющая отслеживать движение документов и получать уведомления о важных событиях. Для оперативного разрешения возникающих вопросов используются электронная почта и телефонные переговоры должностных лиц.

При необходимости рассмотрения сложных технических вопросов проводятся очные совещания или совещания в режиме видео-конференц-связи с участием специалистов.

8.3. Ответственность за взаимодействие

Начальник ИТ отдела несёт ответственность за организацию взаимодействия между всеми участниками процесса получения и реализации мер и за обеспечение своевременного обмена необходимой информацией.

Начальник ИТ отдела несёт ответственность за своевременное получение и рассмотрение информации о необходимости реализации мер, за организацию работ и представление отчётов о выполнении. Руководители органов-исполнителей и подведомственных учреждений несут персональную ответственность за полноту и качество реализации возложенных на них мер защиты информации.

9. Учёт и документирование

9.1. Архивирование документов

Все документы, связанные с получением и реализацией мер ФСТЭК России, подлежат обязательному архивированию и хранению в ИТ отделе.

9.2. Доступ к информации

Доступ к документам, содержащим информацию о полученных и реализованных мерах ФСТЭК России, предоставляется должностным лицам, непосредственно причастным к реализации мер, руководителям органов-исполнителей и специалистам в области информационной безопасности в соответствии с их должностными обязанностями. Ограничение доступа обеспечивается в соответствии с требованиями законодательства Российской Федерации об информационной безопасности и защите конфиденциальной информации.

10. Сроки и ответственность

10.1. Установление сроков выполнения

Сроки выполнения полученных от ФСТЭК России мер устанавливаются в зависимости от их характера, критичности и сложности. Критические меры, требующие немедленного выполнения, должны быть реализованы в течение 1-3 рабочих дней с момента получения информации. Обычные меры, не носящие критичного характера, должны быть реализованы не позднее сроков, определённых ФСТЭК России.

10.2. Контроль исполнения

Контроль за исполнением настоящего Регламента возлагается на начальника отдела ИБ, который отслеживает соблюдение установленных сроков выполнения

мер, качество проведения работ, своевременность представления отчётности, применение дисциплинарных мер в отношении должностных лиц, допускающих нарушение установленного порядка.

10.3. Ответственность руководителей

Руководители и заместители руководителей органов-исполнителей несут персональную ответственность за обеспечение информационной безопасности соответствующих органов в соответствии с Указом Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и распоряжением Губернатора Белгородской области от 26 апреля 2021 года № 167-р «О защите информации».

11. Заключительные положения

11.1. Внесение изменений

Внесение изменений и дополнений в настоящий Регламент осуществляется при изменении требований законодательства Российской Федерации, изменении структуры органов власти Ивнянского муниципального округа, а также при совершенствовании процедур обработки мер ФСТЭК России на основе накопленного опыта. Проекты изменений разрабатываются ИТ отделом и утверждаются заместителем Главы округа – руководителем аппарата Администрации Ивнянского муниципального округа, на которого возложены полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в установленном порядке.

11.2. Применение типовых положений

При реализации настоящего Регламента допускается применение типовых положений, рекомендаций и методических документов, разработанных ФСТЭК России в соответствии с Положением о Федеральной службе по экспортному и техническому контролю, утверждённым Указом Президента Российской Федерации от 16 августа 2004 года № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю», в части организации оперативного информирования в пределах своей компетенции органов государственной власти субъектов Российской Федерации об угрозах безопасности информации и уязвимостях информационных систем и иных объектов критической информационной инфраструктуры, а также о мерах по технической защите от этих угроз и уязвимостей.

