ПРАВИТЕЛЬСТВО МОСКВЫ

ПРЕФЕКТУРА ЮГО-ЗАПАДНОГО АДМИНИСТРАТИВНОГО ОКРУГА ГОРОДА МОСКВЫ

РАСПОРЯЖЕНИЕ

28 октября 2025 № 312-РП

Об утверждении Частной Политики префектуры Юго-Западного административного округа города Москвы в отношении контроля за обеспечением уровня защищенности информации в информационных системах и ресурсах

В целях обеспечения выполнения мер, направленных на установление требований к обеспечению уровня защищенности информации в информационных системах и ресурсах, при использовании которых осуществляется реализация возложенных на префектуру Юго-Западного административного округа города Москвы и подведомственные ей организации государственных функций и полномочий:

1. Утвердить Частную Политику префектуры Юго-Западного административного округа города Москвы в отношении контроля за обеспечением уровня защищенности информации в информационных системах и ресурсах (далее – Политика), согласно приложению к настоящему распоряжению.

2. **Начальнику Управления государственной службы и кадров префектуры** обеспечить доведение Политики до сведения руководителей структурных подразделений префектуры, в части касающейся.

3. **Главам управ районов, директору ГКУ «ДЗ ЖКХиБ ЮЗАО» и руководителям государственных бюджетных учреждений, подведомственных префектуре**:

3.1. В срок **до 29.10.2025** разработать и утвердить Политику в отношении контроля за обеспечением уровня защищенности информации в информационных системах и ресурсах.

4. Контроль за выполнением настоящего распоряжения возложить на руководителя аппарата префектуры **Романову О.Н.**

Префект **О.А.Волков**

Разослать через СЭД ПМ: Волкову О.А., Ломовой Е.Н., Алисултанову А.Р., Промыслову В.Ю., Светличной Е.В., Хубаевой З.Н., Романовой О.Н., УГСиК префектуры, УД префектуры, управам районов, ГКУ «ДЗ ЖКХиБ ЮЗАО», ГБУ, подведомственным префектуре.

Разослать на бумажном носителе: прокуратуре ЮЗАО, в дело.

Соболев В.В.
60739

Приложение
к распоряжению префектуры
от «28» сентября 2025 г.
№ 312-РП

ЧАСТНАЯ ПОЛИТИКА
контроля за обеспечением уровня защищенности информации в информационных системах и ресурсах префектуры Юго-Западного административного округа города Москвы

1. Общие положения

Настоящая Частная Политика контроля за обеспечением уровня защищенности информации в информационных системах и ресурсах (далее – Политика) устанавливает общие правила и требования контроля за обеспечением уровня защищенности информации, обрабатываемой в информационных системах и ресурсах города Москвы, включая программно-аппаратные (программно-технические) комплексы, участвующие в обработке информации, оператором которых является префектура Юго-Западного административного округа города Москвы (далее – ИСиР).

2. Термины и определения

Документация по ЗИ – документы, определяющие правила и процедуры, реализуемые для обеспечения защиты информации в ИСиР в ходе их эксплуатации.

Оператор ИСиР – префектура Юго-Западного административного округа города Москвы (далее - Префектура) или подведомственная ей организация, которой в установленном порядке переданы функции оператора ИСиР.

Ответственный за ЗИ – лицо, определяемое ответственным за защиту информации в ИСиР в порядке, установленном приказом префектуры от 30 декабря 2021 № 177-ПП.

Регулирующий орган – государственный орган (уполномоченная таким органом организация), наделенный полномочиями по контролю исполнения требований законодательства Российской Федерации.

Сервисная организация – контрагент Оператора ИСиР по контракту, в том числе лица, привлекаемые контрагентом в качестве субподрядчика (соисполнителя) по контракту (договору).

3. Общие требования

3.1. Периодичность осуществления контроля за обеспечением уровня защищенности информации (далее – Контроль) устанавливается в документации по ЗИ, с учетом особенностей ИСиР, но не реже одного раза в два года, с учетом Контроля, осуществляемого в рамках аттестации ИСиР

на соответствие требованиям по защите информации (повторной аттестации, дополнительных аттестационных испытаний).

3.2. Контроль проводится Оператором ИСиР самостоятельно и (или) с привлечением сервисной организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.3. Правила, требования, ответственность, полномочия и порядок проведения контроля за обеспечением уровня защищенности информации конкретной ИСиР утверждаются в документации по ЗИ такой ИСиР с учетом Политики.

3.4. Ответственный за ЗИ организует работы по проведению Контроля, в ходе которых в том числе осуществляются:

- планирование Контроля;
- анализ защищенности информации с учетом особенностей функционирования ИСиР;
- анализ и оценка функционирования ИСиР и ее системы (подсистемы) защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы (подсистемы) защиты информации;
- документирование процедур и результатов Контроля.

4. Порядок планирования Контроля

4.1. Контроль может проводиться на плановой и внеплановой основе.

4.2. Плановый Контроль включает в себя проведение мероприятий в соответствии с планом проведения контроля защиты информации в ИСиР (далее – План), утвержденным Ответственным за ЗИ.

4.3. Основанием для внепланового Контроля являются:

- наличие замечаний к ИСиР со стороны регулирующих органов во время проведения контрольных (надзорных) мероприятий;
- расследование инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности информации и выявивших недостатки в системе (подсистеме) защиты информации ИСиР;
- изменение требований законодательства Российской Федерации.

4.4. Проведенный внеплановый Контроль по решению Ответственного за ЗИ может быть зачтен при исполнении Плана как плановый Контроль.

4.5. По запросу протоколы контроля защиты информации направляются в Управление информационной безопасности Департамента информационных технологий города Москвы (далее - Департамент).

5. Порядок проведения анализа защищенности информации

5.1. Анализ защищенности информации в ИСиР проводится с учетом особенностей функционирования ИСиР в целях оценки возможных последствий реализации угроз безопасности информации в ИСиР, возможности преодоления нарушителем системы (подсистемы) защиты информации ИСиР и предотвращения реализации угроз безопасности информации.

5.2. Анализ защищенности ИСиР должен включать:

- проверку состава технических средств, программного обеспечения и средств защиты информации;

- проверку отсутствия уязвимостей ИСиР, правильность установки и настройки средств защиты информации, корректность работы программного обеспечения и средств защиты информации;

- в случае выявления известных на момент проведения Контроля уязвимостей ИСиР, определение дополнительных угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИСиР;

- проверку правил генерации и смены паролей пользователей, персонала, создания и удаления учетных записей пользователей, персонала, реализации правил разграничения доступа, полномочий пользователей, персонала в ИСиР.

5.3. В результате анализа защищенности информации ИСиР:

- подлежат устранению выявленные уязвимости ИСиР либо подлежат применению компенсирующие меры, нейтрализующие возможность использования выявленных уязвимостей;

- при выявлении уязвимостей ИСиР, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации.

В случае невозможности за время проведения Контроля устранить выявленные уязвимости ИСиР Ответственным за ЗИ утверждается план устранения выявленных уязвимостей ИСиР. По запросу план устранения выявленных уязвимостей ИСиР направляется в Департамент.

5.4. Процессы анализа защищенности информации должны проводиться с учетом политики управления уязвимостями информационных систем и ресурсов префектуры (распоряжение префектуры от 28.10.2025 № 311-РП).

5.5. По решению Ответственного за ЗИ анализ защищенности ИСиР может проводиться с привлечением Департамента на основе заявки, направленной через систему электронного документооборота, используемую Правительством Москвы.

5.6. Устранение выявленных уязвимостей может осуществляться Оператором ИСиР самостоятельно и (или) с привлечением сервисной организации.

6. Порядок проведения анализа и оценки функционирования ИСиР и ее системы (подсистемы) защиты информации

6.1. В рамках анализа и оценки функционирования ИСиР и ее системы (подсистемы) защиты информации подлежат проведению в том числе следующие мероприятия:

- проверка определения (пересмотр) информации, подлежащей защите;

- оценка изменений в ИСиР, оказывающих влияние на безопасность информации, обрабатываемой в ней;

- анализ ИСиР на соответствие требованиям нормативных правовых актов, методических документов и национальных стандартов в области защиты информации;

- анализ дополнительных угроз безопасности информации, появляющихся в связи с изменениями в ИСиР;

- анализ классификации ИСиР в соответствии с требованиями о защите информации;

- проверка мер защиты информации, реализованных в ИСиР для нейтрализации угроз безопасности информации;

- проверка соответствия реализованных мер защиты информации требованиям о защите информации в ИСиР;

- проверка функционирования системы (подсистемы) защиты информации ИСиР в ходе ее эксплуатации;

- выявление иных недостатков в функционировании ИСиР.

7. Порядок документирования процедур и результатов Контроля

7.1. Результаты проведенного Контроля должны отражаться в протоколе контроля защиты информации ИСиР и в техническом паспорте.

7.2. В протоколе контроля защиты информации подлежат отражению результаты всех мероприятий, предусмотренных разделами 5 и 6 Политики.

7.3. По запросу протоколы контроля защиты информации направляются в Департамент.

7.4. Порядок учета и хранение документов по результатам проведенного Контроля устанавливается в документации по ЗИ ИСиР.

7.5. По результатам Контроля Ответственным за ЗИ должно приниматься решение о наличии либо отсутствии оснований для доработки (модернизации) системы (подсистемы) защиты информации ИСиР с последующими испытаниями системы (подсистемы) защиты информации ИСиР и/или о дополнительной проверке эффективности системы (подсистемы) защиты информации ИСиР в виде дополнительных аттестационных испытаний или повторной аттестации ИСиР на соответствие требованиям по защите информации.

8. Ответственность

8.1. Ответственность за организацию выполнения требований Политики несет Ответственный за ЗИ.