ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ГОРОДА МОСКВЫ
«ЖИЛИЩНИК РАЙОНА КОНЬКОВО»
(ГБУ «Жилищник района Коньково»)

улица Миклухо-Маклая, дом 38, г. Москва, 117279
Телефон/факс (495) 429-75-59, E-mail: gbukonkovo@uzao.mos.ru
ОГРН 5147746445688 ИНН 7728898752 КПП 772801001

ПРИКАЗ

«21» ноября 2025 г. **№ 312 - ОД**

«Об утверждении Частной Политики управления уязвимостями информационных систем и ресурсов ГБУ «Жилищник района Коньково»

В целях обеспечения выполнения мер, направленных на установление требований к управлению уязвимостями информационных систем и ресурсов и иной ИТ-инфраструктуры, при использовании которых осуществляется реализация возложенных на ГБУ «Жилищник района Коньково» функций и полномочий:

1. Утвердить Частную Политику ГБУ «Жилищник района Коньково» города Москвы в отношении управления уязвимостями информационных систем и ресурсов (далее – Политика), согласно приложению к настоящему распоряжению.
2. **Начальнику отделу персонала Прокопчук Н.В.** обеспечить доведение Политики до сведения начальников отделов, в части касающейся.
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Директор **О.Ю. Бяхов**

Приложение
к приказу
от «21» ноября 2025 г.
№ 312-ОД

Частная Политика
управления уязвимостями ГБУ «Жилищник района Коньково» города Москвы

1. Общие положения

1.1. Настоящая Частная Политика управления уязвимостями информационных систем и ресурсов (далее – Политика) устанавливает общие правила и требования по управлению уязвимостями информационных систем
и ресурсов, оператором которых является ГБУ «Жилищник района Коньково» города Москвы (далее - ГБУ).

2. Термины и определения

ИСиР – информационные системы и ресурсы, оператором которых является ГБУ.

Ответственный за управление уязвимостями – лицо, определяемое ответственным за управление уязвимостями и информационную безопасность в Учреждение.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Участники информационного взаимодействия – органы исполнительной власти города Москвы, подведомственные им организации, иные организации, определенные правовым актом Правительства Москвы, содержащим положения об ИСиР, должностным лицам которых в ИСиР присвоены учетные записи.

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Регулирующий орган – государственная организация, которая контролирует исполнение требований законодательства Российской Федерации.

3. Общие требования к управлению уязвимостями

3.1. Детальное описание операций, включающее наименование операций, описание операций, исполнителей, продолжительность, входные и выходные данные описываются с учетом настоящей Политики и методическим документом «Руководство по организации процесса управления уязвимостями в органе (организации)» (утвержденным Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК) 17.05.2023) в документе, определяющем правила и процедуры,

реализуемые для обеспечения защиты информации в ИСиР в ходе ее эксплуатации (далее – документация по ЗИ), издаваемым оператором ИСиР или уполномоченной им организацией.

3.2. В случае размещения компонентов ИСиР в вычислительной инфраструктуре центров обработки данных, положения документации по ЗИ должны учитывать установленные правила, требования, ответственность, полномочия и порядок управления уязвимостями вычислительной инфраструктуры центров обработки данных.

3.3. В случае наличия среди компонентов ИСиР сертифицированных программных, программно-аппаратных средств защиты информации, документация по ЗИ должна учитывать эксплуатационную документацию на них, а также рекомендации разработчиков по управлению уязвимостями.

3.4. Работы по управлению уязвимостями могут проводиться оператором ИСиР самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.5. Управление уязвимостями в отношении автоматизированных рабочих мест, коммуникационного оборудования, иного программно-аппаратного обеспечения, используемого участниками информационного взаимодействия для взаимодействия с ИСиР обеспечивается участниками информационного взаимодействия, если иное не установлено правовым актом
Правительства Москвы и(или) документацией по ЗИ.

4. Мониторинг уязвимостей и оценка их применимости

4.1. На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке. Источниками данных об уязвимостях могут быть:

– системы управления информационной инфраструктурой;

– базы данных управления конфигурациями;

– документация на информационные системы;

– электронные базы знаний;

– база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/);

– базы данных, содержащие сведения об известных уязвимостях;

– официальные информационные ресурсы разработчиков программных
и программно-аппаратных средств и исследователей в области информационной безопасности;

– информационные сообщения регулирующих органов;

– результаты проведения контрольных мероприятий регулирующими органами;

– уведомления об уязвимостях от администраторов, обслуживающих компоненты ИСиР;

– иные источники.

4.2. На этапе мониторинга уязвимостей и оценки их применимости выполняются следующие операции:

– анализ информации об уязвимостях;

– оценка применимости уязвимостей;

– принятие решений на получение дополнительной информации;

– постановка задачи на сканирование объектов;

– сканирование объектов;

– оценка защищенности.

4.3. Периодичность проведения мониторинга уязвимостей ИСиР и оценка их применимости устанавливается в документации по ЗИ с учетом особенностей функционирования ИСиР, но не реже чем один раз в два года.

4.4. В случае опубликования в общедоступных источниках информации
об уязвимости компоненты, применяемой в ИСиР и(или) поступления информации об уязвимости от иных источников данных об уязвимостях, оценка применимости таких уязвимостей в отношении ИСиР должна проводиться
в течении пяти рабочих дней с момента поступления такой информации.

4.5. В случае выявления уязвимостей регулирующими органами во время проведения ими проверки, такие уязвимости считаются применимыми.

4.6. Мониторинг уязвимостей ИСиР и оценка их применимости могут проводиться в рамках процессов:

– контроля за обеспечением уровня защищенности информации, содержащейся в ИСиР;

– анализа уязвимостей проводимом при создании или модернизации (развитии) ИСиР.

4.7. Мониторинг уязвимостей ИСиР и оценка их применимости должны проводиться на основе сформированного плана и(или) методики, согласованных с Ответственным за управление уязвимостями, для всех компонентов ИСиР.

4.8. Используемые для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (далее – сканеры безопасности), на момент проведения мониторинга уязвимостей ИСиР должны иметь актуальную базу данных выявляемых уязвимостей, а также актуальный сертификат соответствия требованиям по безопасности информации.

4.9. На время работы сканеров безопасности ИСиР должна быть переведена в режим сервисного обслуживания.

4.10. В случае, если выполнение п. 4.9 невозможно либо работа сканеров безопасности может привести к нарушению функционирования компонентов ИСиР, сканирование осуществляется на специально развернутой тестовой копии компонентов ИСиР.

4.11. Результаты проведения мониторинга уязвимостей ИСиР и оценки их применимости направляются Ответственному за управление

уязвимостями
для организации работы по проведению оценки выявленных уязвимостей.

4.12. Ответственный за управление уязвимостями организует работу для выполнения требований данного раздела.

5. Оценка уязвимостей

5.1. На этапе оценки уязвимостей осуществляется определение уровня критичности уязвимостей применительно к ИСиР.

5.2. На этапе оценки уязвимостей выполняются операции:

– получение информации об объектах, подверженных уязвимостей;

– определение уровня опасности уязвимостей;

– определение влияния уязвимостей на ИСиР;

– оценка критичности уязвимостей.

5.3. Анализ результатов мониторинга уязвимостей ИСиР проводится в срок не более пяти рабочих дней, с целью классификации выявленных уязвимостей по степени их риска.

5.4. Операции по определению уровня опасности уязвимости, ее влияния на информационные системы и расчету критичности уязвимости выполняются в соответствии с «Методикой оценки уровня критичности уязвимостей программных и программно-аппаратных средств», утвержденной
ФСТЭК России 30.06.2025. При этом к критичным уязвимостям как минимум должны быть отнесены:

– применимые к ИСиР уязвимости, информация о которых поступила от регулирующих органов;

– уязвимости, выявленные регулирующими органами во время проведения ими контрольных мероприятий в отношении ИСиР;

– если в отчете, полученном по результатам работы сканеров безопасности, уязвимости присвоен максимальный уровень критичности.

5.5. Ответственный за управление уязвимостями организует работу для выполнения требований данного раздела.

6. Определение методов и приоритетов устранения уязвимостей

6.1. На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

– определения приоритетности устранения уязвимостей;

– выбор методов устранения уязвимостей: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

6.2. На этапе определения методов и приоритетов устранения уязвимостей выполняются следующие операции:

– определение приоритетности устранения уязвимостей;

– определение методов устранения уязвимостей;

– принятие решения о необходимости установки обновлений;

– постановка задачи на установку обновления (при необходимости);

– принятие решения о необходимости реализации компенсирующих мер защиты информации;

– постановка задачи на реализацию компенсирующих мер защиты информации (при необходимости).

6.3. При обнаружении критической уязвимости может быть принято решение о срочной установке обновления программного обеспечения компонентов ИСиР, подверженных уязвимости.

6.4. При обнаружении критической уязвимости может быть принято решение о срочной реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления.

6.5. Уязвимости, выявленные регулирующими органами во время проведения ими контрольных мероприятий в отношении ИСиР, подлежат устранению в срок, не превышающий срок проведения контрольных мероприятий, в случае наличия такой возможности.

6.6. Уязвимости, указанные в предписании, выданном по результатам проведения контрольных мероприятий регулирующих органов устраняются в срок, не превышающий срок, указанный в предписании.

6.7. По результатам определения методов и приоритетов устранения уязвимостей должен быть сформирован план устранения уязвимостей, в котором как минимум должно быть указано:

– наименование ИСиР в которой выявлена уязвимость;
– компонент ИСиР в котором выявлена уязвимость;
– описание уязвимости;
– категория критичности уязвимости;
– исполнитель, ответственные за устранение уязвимости;
– метод устранения уязвимости;
– срок устранения уязвимости.

6.8. Для организации процесса устранения уязвимостей между работниками разных подразделений, план устранения уязвимостей должен быть согласован с руководителями всех подразделений, принимающих участие в устранении уязвимости и(или) несущих ответственность за функционирование ИСиР и(или) ее компонентов.

6.9. Выбор метода устранения выявленных уязвимостей осуществляется исполнителем, ответственным за устранение уязвимостей.

6.10. План устранения уязвимостей ИСиР направляется Ответственному
за управление уязвимостями для организации работы по проведению контроля устранения уязвимостей. В случае, если у Ответственного за управление уязвимостями есть замечания или предложения по плану, он отправляет его на доработку ответственному за устранение уязвимостями.

6.11. Ответственный за управление уязвимостями организует работу для выполнения требований данного раздела.

7. Устранение уязвимостей

7.1. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга.

7.2. На этапе устранения уязвимостей выполняются следующие операции:

– согласование установки программного обеспечения;
– тестирование обновлений программного обеспечения;
– установка обновления в тестовом сегменте;
– принятие решения об установке обновления;
– установка обновления;
– формирование плана установки обновлений;
– разработка и реализация компенсирующих мер защиты информации.

7.3. В случае, если при проведении тестирования обновлений программного обеспечения, обнаружено негативное влияния от установки обновления на ИСиР дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации.

7.4. Проведение работ по установки обновлений должно производиться в соответствии с порядком управления конфигурацией ИСиР, описанном в документации по ЗИ.

7.5. Уязвимости, для устранения которых не была определена необходимость срочной установки обновлений, устраняются в ходе плановой установки обновлений.

7.6. Выбор мер устранения выявленных уязвимостей осуществляется Исполнителем, ответственным за устранение уязвимостей. К таким мерам, в том числе, могут относиться:

– установка обновлений безопасности, предоставляемых разработчиком ПО, в котором выявлены уязвимости;
– отключение неиспользуемого функционала, в котором выявлены уязвимости;
– организационные меры защиты информации;
– настройка средств защиты информации;
– внесение изменений в ИТ-инфраструктуру.

7.7. По результатам завершения процесса устранения выявленных уязвимостей производится повторный мониторинг уязвимостей для контроля наличия неустраненных уязвимостей. В случае выявления неустраненных уязвимостей принимаются меры по их устранению в соответствии с разделами 6, 7 Политики.

7.8. Ответственный за управление уязвимостями организует работу для выполнения требований данного раздела.

8. Контроль устранения уязвимостей

8.1. На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, принятие оперативных решений и решений по улучшению процесса управления уязвимостями.

8.2. На этапе контроля устранения уязвимостей должно проводится определение причин отклонений и неисполнений операций процесса управления уязвимостями. Возможными причинами являются:

– пропуск уязвимости в ходе мониторинга;

– ошибки оценки уязвимостей;

– нарушения сроков устранения уязвимостей;

– недостаточность принятых компенсирующих мер.

8.3. В случае наличия неустранённых уязвимостей повторно инициируется процесс устранения уязвимостей.

8.4. С целью контроля устранения выявленных уязвимостей должен вестись «Реестр устранения выявленных уязвимостей».

8.5. Не допускается проведение контроля устранения уязвимостей Исполнителем, ответственным за устранение уязвимостей.

8.6. По итогам проведения контроля устранения уязвимостей принимаются меры по улучшению процесса управления уязвимостями. К таким мерам в том числе относятся:

– внесение изменений в конфигурацию и алгоритмы средств сбора и обработки данных об уязвимостях;

– поиск и организация мониторинга новых источников сведений об уязвимостях;

– внесение изменений в процедуру оценки уязвимостей;

– повторное определение уровня критичности уязвимости применительно к ИСиР.

8.7. Ответственный за управление уязвимостями организует работу для выполнения требований данного раздела.

9. Ответственность

9.1. Исполнители, ответственные за устранение уязвимости, несут ответственность за устранение уязвимостей в срок, установленный планом устранения уязвимостей.