Приложение
к приказу
от «28» марта 2025 г.
№ 81/1-ОД

**Политика
Государственного бюджетного учреждения города Москвы «Жилищник
района Коньково» (ГБУ «Жилищник района Коньково»)
в отношении резервного копирования и восстановления объектов
резервного копирования**

1. Общие положения

Настоящая политика резервного копирования и восстановления объектов резервного копирования (далее – Политика) устанавливает общие правила и требования резервного копирования информации, данных, компонентов информационных систем и ресурсов (далее – ИСиР), города Москвы, оператором которых является Государственного бюджетного учреждения города Москвы «Жилищник района Коньково» (далее - ГБУ «Жилищник района Коньково»), и других объектов резервного копирования, определенных настоящим документом, включая ИТ-инфраструктуру и программно-аппаратные (программно-технические) комплексы, участвующие в обработке информации.

2. Термины и определения

Администратор – лицо, назначаемое распорядительным документом оператора ИСиР и/или ИТ-инфраструктуры, ответственным за управление (администрирование) системой защиты информации в ИСиР и/или ИТ-инфраструктуры.

Долгосрочное хранение – процедура хранения выборочных резервных копий на отчуждаемых носителях информации сроком один год и более.

ИТ-инфраструктура – совокупность программных и аппаратных средств, в том числе автоматизированных рабочих мест, с использованием которых осуществляется реализация возложенных на ГБУ «Жилищник района Коньково» функций и полномочий, а также доступ к ИСиР города Москвы.

Компонент ИСиР и/или ИТ - инфраструктуры – часть ИСиР и/или ИТ-инфраструктуры, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Объект резервного копирования – информация, файловые системы, отдельные файлы, сетевые диски, виртуальные машины и иные данные, настройки, компоненты ИСиР, и другие объекты, которые необходимы для восстановления функционирования ИСиР и/или ИТ-инфраструктуры.

Окно резервного копирования – период времени, необходимый для выполнения резервного копирования в штатном режиме, определяемый временем начала и временем завершения процедур резервного копирования.

Резервное копирование – процедура, предусматривающая создание заданного количества актуальных копий объекта резервного копирования для использования их в случае утраты или повреждения рабочей копии объекта резервного копирования или его части.

Сервисная организация – контрагент Оператора ИСиР и/или ИТ-инфраструктуры по контракту (договору), в том числе лица, привлекаемые таким контрагентом в качестве субподрядчика (соисполнителя) по контракту (договору).

Средство резервного копирования, управляемое централизованно – программное обеспечение, предназначенное для решения основных задач по управлению, настройке и обслуживанию средств резервного копирования объектов резервного копирования, управляемое с помощью централизованной консоли.

3. Общие требования

3.1. Частные правила, требования, порядок проведения резервного копирования и восстановления объектов резервного копирования для конкретной ИСиР и/или ИТ-инфраструктуры, а также лица, ответственные за процедуры резервного копирования, их полномочия определяются с учетом настоящей Политики в организационно-распорядительных документах, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИСиР в ходе их эксплуатации (далее – документация по РК).

3.2. Резервное копирование и восстановление объектов резервного копирования может проводиться самостоятельно лицом, выполняющим функции оператора ИСиР и/или ИТ-инфраструктуры по их эксплуатации, и (или) с привлечением сервисной организации.

3.3. Администратор обеспечивает организацию работ по проведению резервного копирования и восстановления объектов резервного копирования и контролирует их выполнение.

4. Требования к резервному копированию и восстановлению информации, функционирования объектов резервного копирования

4.1. Для осуществления резервного копирования в приоритетном порядке необходимо использовать средства резервного копирования, управляемые централизованно. В случае отсутствия технической возможности следует использовать средства резервного копирования, встроенные в операционные системы.

4.2. Резервное копирование (далее - РК) должно осуществляться:

- на резервные машинные носители информации в соответствии с параметрами, установленными в документации по РК с учетом настоящей Политики;

- объектов резервного копирования, необходимых для восстановления штатного функционирования ИСиР и/или ИТ-инфраструктуры, перечень которых определяется в документации по РК;

- в автоматическом режиме по расписанию, и(или) автоматизированном режиме (с применением средств автоматизации и с участием человека), и(или) без использования средств автоматизации (при необходимости или невозможности автоматизации).

4.3. В документации по РК должно быть определено место хранения резервных копий информации, содержащейся в ИСиР и/или ИТ-инфраструктуре. При этом необходимо:

- создавать и хранить не менее трех резервных копий информации (одну основную и две резервные);

- использовать для хранения резервных копий не менее двух разных типов носителей (например, система хранения данных на жестких дисках, система хранения на магнитных лентах и др.);

- хранить одну из резервных копий в физически отдельном (обособленном) от иных резервных копий месте (помещении).

4.4. Резервное копирование информации, содержащейся в ИСиР и/или ИТ-инфраструктуре в зависимости от объема данных, частоты их изменения и ресурсов для хранения резервных копий должно осуществляться с использованием одного из следующих методов и/или их возможных комбинаций:

- инкрементное резервное копирование информации (используется в случае обработки больших объемов данных) - ежедневно (не реже одного раза в 24 часа);

- дифференциальное резервное копирование информации (резервное копирование информации относительно последней полной резервной копии) - еженедельно (не реже одного раза в неделю);

- полное резервное копирование информации - ежемесячно (не реже одного раза в месяц).

4.5. Должна осуществляться автоматическая регистрация событий, связанных с резервным копированием объектов резервного копирования.

4.6. Восстановление объектов резервного копирования производится при необходимости.

4.7. Регулярно (после завершения каждого резервного копирования информации) необходимо проверять целостность резервных копий информации.

4.8. Проведение тестовых восстановлений объектов резервного копирования должно осуществляться с периодичностью, определенной в документации по РК, но не реже одного раза в год для каждого компонента ИСиР и/или ИТ-инфраструктуры.

4.9. Тестовое восстановление может проводиться в рамках процессов контроля за обеспечением уровня защищенности информации в ИСиР и/или ИТ-инфраструктуре.

4.10. Тестовое восстановление проводится с учетом особенностей функционирования ИСиР и/или ИТ-инфраструктуры в целях оценки возможности восстановления объектов резервного копирования с резервных копий, а также их полноты и актуальности.

4.11. Должна осуществляться автоматическая регистрация событий, связанных с восстановлением объектов резервного копирования.

4.12. Должны быть приняты меры для защиты объектов резервного копирования, обеспечивающие их конфиденциальность, целостность и доступность в соответствии с требованиями законодательства Российской Федерации, предъявляемыми к мерам защиты информации, обрабатываемой в ИСиР, в соответствии с определенным классом защищенности ИСиР и уровнем защищенности персональных данных. При наличии технической возможности меры защиты информации должны включать в себя шифрование резервных копий.

Состав мер защиты объектов резервного копирования неклассифицированных ИСиР должен соответствовать мерам защиты информации, предусмотренным приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК) России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для защиты информации в информационных системах 3-го класса защищенности или выше.

5. Выбор параметров резервного копирования и восстановления информации

5.1. Параметры резервного копирования и восстановления объектов резервного копирования должны определяться в документации по РК, в том числе, с учетом категории данных, обрабатываемых в ИСиР и/или ИТ-инфраструктуре, и технических возможностей средств резервного копирования. Как минимум должны быть определены следующие параметры:

- состав объектов, подлежащих резервному копированию;
- перечень данных, обрабатываемых в ИСиР и/или ИТ-инфраструктуре, подлежащих резервному копированию;
- периодичность проведения тестового восстановления;
- периодичность резервного копирования;
- время хранения резервных копий;
- окно резервного копирования;
- срок долгосрочного хранения (только для объектов, требующих долгосрочного хранения).

5.2. При выборе состава объектов резервного копирования требуется руководствоваться необходимостью исключения дублирования данных, содержащихся в резервной копии.

5.3. Периодичность резервного копирования должна определяться в соответствии с установленными в документации по РК параметрами, обеспечивающими допустимость потери данных глубиной не более 24 часов.

5.4. Время хранения резервных копий должно определяться в соответствии с установленными в документации по РК параметрами в зависимости от особенностей ИСиР и/или ИТ-инфраструктуры, но не менее 2 недель для объектов в продуктивной среде.

5.5. Окно резервного копирования должно выбираться в соответствии с установленными в документации по РК параметрами, и определяется в зависимости от особенностей ИСиР и/или ИТ-инфраструктуры. В целях формирования консистентных резервных копий информации резервное копирование необходимо осуществлять преимущественно в промежутки времени, когда пользователи не используют ИСиР и/или ИТ-инфраструктуру.

5.6. Продолжительность долгосрочного хранения должна выбираться в соответствии с установленными в документации по РК параметрами, и определяется в зависимости от особенностей ИСиР и/или ИТ-инфраструктуры.

5.7. Долгосрочное хранение должно осуществляться на отчуждаемых носителях информации, которые должны храниться на площадке, территориально удаленной от основного места размещения компонентов ИСиР и/или ИТ-инфраструктуры.