



ПРАВИТЕЛЬСТВО МОСКВЫ
УПРАВА РАЙОНА ЯСЕНЕВО ГОРОДА МОСКВЫ
Юго-Западный административный округ

П Р И К А З

12.01.2022

№ 5

**Об утверждении Политики
информационной безопасности
управы района Ясенево города
Москвы**

В соответствии с положениями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», во исполнение распоряжения префектуры Юго-Западного административного округа города Москвы от 30.12.2021 № 334-РП, в целях принятия мер, направленных на обеспечение информационной безопасности в управе района Ясенево города Москвы (далее - управа),

ПРИКАЗЫВАЮ:

1. Утвердить политику информационной безопасности управы района Ясенево города Москвы (далее - Политика) в соответствии с приложением к настоящему приказу.
2. Заместителю главы управы по работе с населением **Сакибовой С.В.** обеспечить разработку и утверждение документов, определяющих Политику в сфере обеспечения информационной безопасности управы.
3. Советнику юридической службы **Мартыновой М.А.** обеспечить доведение Политики до сведения всех государственных гражданских служащих и работников управы.
4. Контроль за исполнением настоящего приказа и требований Политики оставляю за собой.

**Исполняющий обязанности
главы управы**

А.М. Борзунов

Мартынова М.А.
495-427-57-33

008699

Политика информационной безопасности управы района Ясенево города Москвы

1. Общие положения

Настоящая политика информационной безопасности (далее - Политика) является основополагающим документом, регулирующим деятельность управы района Ясенево города Москвы (далее - управа) по организации защиты информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно - телекоммуникационных сетях, и обеспечению установленного законодательством Российской Федерации уровня защиты в отношении информации ограниченного доступа, за исключением сведений, составляющих государственную тайну.

Настоящая Политика определяет цели и задачи управы в области обеспечения информационной безопасности, принципы обеспечения информационной безопасности.

2. Область действия

Политика распространяется на процессы обработки и обеспечения безопасности информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, за исключением сведений, составляющих государственную тайну.

Политика обязательна для исполнения государственными гражданскими служащими и работниками управы (далее – работники управы).

3. Цели и задачи обеспечения информационной безопасности

Под информационной безопасностью понимается состояние защищенности информации, при котором обеспечены: ее конфиденциальность, доступность и целостность.

Целью деятельности управы по обеспечению информационной безопасности является реализация соответствующего комплекса мер и средств контроля и управления, направленных на:

- прогнозирование, обнаружение, сдерживание, предотвращение, отражение информационных угроз, ликвидацию последствий их проявления и минимизацию возможного ущерба;
- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;



- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Задачами управы в области информационной безопасности, направленными на достижение указанной цели, являются:

- организация деятельности по обеспечению информационной безопасности;
- определение и применение мер обеспечения информационной безопасности с учетом всех направлений деятельности управы, а также существующих в управе категорий обрабатываемой информации, объектов обработки информации и информационных систем;
- обеспечение защиты от вмешательства в процесс функционирования компонентов информационных систем, ресурсов, информационно-технологической инфраструктуры, в том числе неизменности программной среды;
- своевременное обнаружение и предотвращение фактов несанкционированного доступа (далее - НСД) к информации и/или передачи ее лицам, не имеющим права на доступ к информации;
- предупреждение возможности неправомерных действий с информацией;
- незамедлительное восстановление информации, модифицированной или уничтоженной вследствие НСД;
- прогнозирование и своевременное выявление и устранение источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;
- доведение до работников управы и третьих лиц правил работы с информацией, подлежащей защите, а также требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации;
- осуществление постоянного эффективного контроля обеспечения информационной безопасности.

4. Принципы обеспечения информационной безопасности

Обеспечение информационной безопасности должно осуществляться в соответствии со следующими принципами:

а. Принцип законности.

При выборе и реализации мер обеспечения информационной безопасности должны строго соблюдаться требования законодательства Российской Федерации, актов государственных регулирующих органов, а также законодательства и иных правовых актов города Москвы, включая правовые акты управы в области обеспечения информационной безопасности.

б. Принцип комплексности.

Для обеспечения информационной безопасности должны реализовываться все доступные правовые, организационные и технические меры и мероприятия, направленные на предупреждение и пресечение угроз информационной безопасности.

с. Принцип своевременности.

Меры обеспечения информационной безопасности должны носить упреждающий характер, предполагающий постановку задач по информационной безопасности на основе анализа и прогнозирования угроз информационной безопасности, а также разработку эффективных мер предупреждения посягательств на защищаемую информацию. При возникновении инцидентов, которые повлекли или могут повлечь угрозу информационной безопасности, работники управы и третьи лица незамедлительно принимают меры по их устранению.

d. Принцип адекватности.

Применяемые меры обеспечения информационной безопасности должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз информационной безопасности и степени конфиденциальности информации.

е. Принцип стандартизации и унификации.

Применяемые и (или) планируемые к применению меры обеспечения информационной безопасности должны отвечать принципам стандартизации и унификации с целью обеспечения их экономической эффективности, удобства использования, сопровождения, модернизации, простоты масштабирования.

f. Принцип непрерывности функционирования.

Должна обеспечиваться отказоустойчивость, надежность, доступность и корректность функционирования мер обеспечения информационной безопасности. Информационные системы и ресурсы управы должны находиться в защищенном состоянии на протяжении всего своего жизненного цикла.

g. Принцип преемственности и непрерывности совершенствования.

Должно быть обеспечено постоянное совершенствование мер обеспечения информационной безопасности на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования систем (средств) защиты с учетом изменений в методах и средствах получения информации нарушителем, нормативных требований по ее (информации) защите, достигнутого передового отечественного и зарубежного опыта в этой области.

h. Принцип ответственности и обязательности контроля.

Принимаемые меры в целях обеспечения информационной безопасности определяют права и обязанности работников управы и обеспечивают их распределение между ними.

Первый заместитель главы управы осуществляет контроль и координацию деятельности структурных подразделений по обеспечению безопасности информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, за исключением сведений, составляющих государственную тайну.

i. Принцип осведомленности.

Все работники управы, а также третьи лица, использующие его информационные активы, должны быть осведомлены о требованиях законодательства Российской Федерации об информации, информационных технологиях и о защите информации и Политики, а также ответственности за их нарушение.

5. Требования по информационной безопасности

Управа осуществляет обеспечение информационной безопасности в соответствии с требованиями, установленными:

- федеральным законодательством Российской Федерации, законодательством города Москвы, а также правовыми актами Правительства Москвы;
- актами государственных регулирующих органов в сфере информационной безопасности;
- правовыми актами и внутренними документами управы в рамках установленной компетенции;
- национальными стандартами.

6. Связанные документы

Политика дополняется внутренними документами управы в области информационной безопасности, которые обеспечивают детализацию, дополнение и уточнение настоящей Политики.

Положения внутренних документов в области информационной безопасности должны соблюдаться работниками управы и третьими лицами в рамках их компетенций при обращении с информацией, подлежащей защите в управе.

7. Ответственность

Работники управы несут персональную ответственность за соблюдение требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации и Политики.

Третьи лица несут ответственность за соблюдение Политики в рамках заключенных с управой договоров, в том числе государственных контрактов.