Приложение 1 к приказу комитета имущественных отношений

города Мурманска

от 29.12.2023г. № 2235

План мероприятий по обеспечению безопасности защищаемой информации

в комитете имущественных отношений города Мурманска на 2024 год

| **№ п/п** | **Наи­ме­но­вание ме­роп­рия­тия** | **Срок вы­пол­не­ния** | **При­ме­ча­ние** |
| --- | --- | --- | --- |
| 1. | Документальное регламентирование работы с информацией | Пос­тоян­но | Разработка и (или) актуализация организационно-распорядительных документов по защите информации |
| 2. | Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство | Пос­тоян­но | В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения тре­бо­ва­ний законодательства в области за­щи­ты информации». Равно­значным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном но­си­теле признается согласие в форме электронного до­ку­мен­та, подписанного в соответствии с федеральным за­ко­ном электронной подписью |
| 3. | Пересмотр договора с третьими лицами на поручение обработки ПДн  | При необхо­ди­мос­ти | В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соб­лю­дении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных» |
| 4. | Ограничение доступа сотрудников к защищаемой информации | При необхо­ди­мос­ти | В случае создания ИС, а также приведения имеющихся ИС в соответствие с требованиями по безопасности ин­фор­ма­ции необходимо разграничить доступ сотрудников комитета имущественных отношений города Мурманска к защищаемой информации |
| 5. | Взаимодействие с субъектами ПДн | Пос­тоян­но | Работа с обращениями субъектов ПДн, ведение журналов учета передачи ПДн, обращений субъектов ПДн, уве­дом­ление субъектов ПДн об уничтожении, изменении, прек­ра­ще­нии обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц |
| 6. | Ведение журналов учета машинных но­си­телей защищаемой информации, средств защиты информации | Пос­тоян­но | - |
| 7. | Повышение квалификации сотрудников в области защиты информации | При необхо­ди­мос­ти | Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, по­вы­ше­ние осведомленности сотрудников – постоянно (данное обучение проводит ответственный за защиту информации, не со­дер­жа­щей сведения, составляющие государственную тайну, в информационных системах комитета имущественных отношений города Мурманска) |
| 8. | Инвентаризация информационных ресурсов  | Раз в год - при проведении ежегодной инвентаризации  | Проводится с целью выявления в инфор­ма­цион­ных ресурсах присутствия защищаемой информации |
| 9. | Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки | При необхо­ди­мос­ти | Для ПДн комитетом имущественных отношений города Мурманска устанавливаются сроки об­ра­бот­ки, которые документально подтверждаются в ло­каль­ных актах комитета имущественных отношений города Мурманска. При пересмотре сроков необходимые изменения вносятся в соответствующие документы |
| 10. | Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации | При необхо­ди­мос­ти | Уничтожение электронных (бумажных) носи­телей информации при достижении целей обработ­ки защищаемой информации производится с оформ­ле­нием Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению защищаемой информации, не со­дер­жащей сведения, составляющие го­су­дарственную тайну» |
| 11. | Определение класса защищенности ИС | При необхо­ди­мос­ти | Определение класса за­щи­щен­нос­ти ИС осуществляется при соз­да­нии ИС, при изменении состава ИС, масштаба ИС, степеней ущерба для характеристик ИС (конфиденциальности, целостности, доступности) |
| 12. | Определение уровня защищенности ПДн при их обработке в ИС | При необхо­ди­мос­ти | Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн |
| 13. | Выявление угроз безопасности и разработка моделей угроз и нарушителя | При необхо­ди­мос­ти | Разрабатывается при создании СЗИ |
| 14. | Аттестация ИС на соответствие требованиям по обеспечению безопасности информации | При необхо­ди­мос­ти | - |
| 15. | Эксплуатация ИС и контроль безопасности защищаемой информации | Постоянно | - |
| 16. | Анализ угроз безопасности в информационной системе | Пос­тоян­но | В рамках данного мероприятия проводится:* выявление, анализ и устранение уязвимостей или принятие мер по предотвращению воз­мож­ности эксплуатации выявленных уязвимостей;
* анализ изменения угроз безопасности информации в информационных системах;
* оценка возможных последствий реализации угроз безопасности информации.

По результатам раз­ра­ба­ты­ва­ет­ся/кор­рек­ти­ру­ет­ся модель нарушителей и угроз безопасности информации.При проведении работ необходимо руководствоваться действующими нормативно-методическими документами в области защиты информации |
| 17. | Обновление программного обеспечения (в том числе средств защиты информации) | При необхо­ди­мос­ти | Получение обновлений производится из до­ве­рен­ных источников |
| 18. | Информирование сотрудников, работающих в информационных системах о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационных систем | Пос­тоян­но | - |
| 19. | Доведение до сотрудников, работающих в информационных системах требований по защите информации, а также положений организационно-распорядительных документов по защите информации | Пос­тоян­но | - |
| 20. | Обучение сотрудников, работающих в информационных системах правилам эксплуатации отдельных средств защиты информации | Пос­тоян­но | Мероприятие проводится при:* вводе средств защиты информации в эксплуатацию;
* изменении правил эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией;
* изменении пользователей средств защиты информации;
* по запросу пользователей,

но не реже одного раза в два года |
| 21. | Проведение практических занятий и тренировок с сотрудниками, работающими в информационных системах по блокированию угроз безопасности информации и реагированию на инциденты | Пос­тоян­но | Мероприятие проводится не реже одного раза в два года |
| 22. | Контроль за обеспечением уровня защищенности информации, содержащейся в информационных системах | Пос­тоян­но | Проводится комитетом имущественных отношений города Мурманска самостоятельно или с привлечением организации, имеющей лицензию на деятельность по технической защите информации, для:* информационных систем с установленным 2 или 3 классом защищенности не реже одного раза в два года;
* для информационных систем с установленным 1 классом защищенности не реже одного раза в год.

Процедура контроля и результаты должны быть задокументированы |