**Примерный перечень**

организационно-распорядительных документов, подлежащих предоставлению в ходе осуществления контроля состояния технической защиты информации в исполнительных органах государственной власти Камчатского края, органах местного самоуправления муниципальных образований в Камчатском крае и подведомственных им учреждениях Камчатского края, являющихся операторами государственных (муниципальных) информационных систем Камчатского края

на 2020 год

1. Приказ «О создании комиссии по определению и классификации государственной информационной системы (далее – ГИС)».
2. Акт классификации ГИС.
3. Акт определения требуемого уровня защищённости персональных данных, обрабатываемых в ГИС.
4. Приказ «О проведении мероприятий по защите информации, обрабатываемой в ГИС».
5. Приказ «О назначении лиц, ответственных за организацию и обеспечение защиты информации, обрабатываемой в ГИС».
6. Перечень информации в ГИС, подлежащей защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных действий в отношении такой информации.
7. Перечень должностей сотрудников, допущенных к обработке защищаемой информации в ГИС.
8. Список лиц, допущенных к техническому и программному обслуживанию ГИС.
9. Список лиц, допущенных к работе в ГИС.
10. Регламент выявления инцидентов и реагирования на них.
11. Регламент эксплуатации виртуальной инфраструктуры.
12. Регламент контроля (мониторинга) за обеспечением уровня защищенности информации, обрабатываемой в ГИС.
13. Регламент управления конфигурацией ГИС и системы защиты информации ГИС.
14. Регламент защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.
15. Регламент использования средств криптографической защиты информации.
16. Регламент применения технических мер защиты информации в ГИС.
17. Правила и процедуры идентификации и аутентификации субъектов доступа к объектам доступа.
18. Правила и процедуры управления доступом субъектов доступа к объектам доступа.
19. Правила и процедуры защиты машинных носителей информации.
20. Правила и процедурыанализа защищенности ГИС.
21. Правила и процедуры регистрации событий безопасности в ГИС.
22. Правила и процедуры обеспечения целостности информации.
23. Правила и процедуры антивирусной защиты.
24. Правила и процедуры контроля и управления физическим доступомк техническим средствам ГИС.
25. Правила и процедуры защиты ГИС, ее средств, систем связи и передачи данных.
26. Правила и процедуры проведения анализа угроз информационной без­опасности и уязвимостей программного обеспечения (в т.ч. с учетом угроз и уязвимостей, содержащихся в банке данных угроз безопасности информации (bdu.fstec.ru)).
27. Правила и процедуры резервного копирования и восстановления.
28. Правила и процедуры неавтоматизированной обработки персональных данных.
29. Правила и процедуры управления программной средой информационных систем обработки персональных данных.
30. Правила и процедуры обнаружения (предотвращения) вторжений.
31. Правила и процедуры управления (администрирования) системой защиты информации вторжений (компьютерных атак).
32. Правила и процедуры внешнего взаимодействия.
33. Правила и процедуры работы с обезличенными персональными данными.
34. Правила и процедуры защиты периметра информационных систем.
35. Инструкция администратора информационной безопасности ГИС.
36. Инструкция системному администратору ГИС.
37. Инструкция администраторам ГИС в части обеспечения безопасности информации.
38. Инструкция пользователям информационных систем ГИС в части обеспечения безопасности информации.
39. Инструкция по организации антивирусной защиты в ГИС.
40. Инструкция по организации парольной защиты в ГИС.
41. Инструкция лица, ответственного за организацию обработки персональных данных в ГИС.
42. Инструкция по порядку учета и хранения машинных и съемных накопителей информации, использующихся в ГИС.
43. Политика обработки персональных данных в ГИС.
44. Положение об обработке персональных данных в ГИС.
45. Требования к организационным и техническим мерам по защите информации в ГИС.
46. Правила и процедуры организации работы внешних пользователей ГИС.
47. Описание технологического процесса обработки информации в ГИС;
48. Разрешительная система доступа к информационным ресурсам ГИС
49. Журнал учета выдачи персональных идентификаторов.
50. Журнал учета изменений в конфигурации ГИС и системы защиты ГИС.
51. Журнал регистрации инцидентов информационной безопасности.
52. Журнал учета и выдачи машинных носителей информации (МНИ).
53. Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним.
54. Журнал учета выдачи ключей от защищаемых помещений ГИС.
55. Журнал проведения инструктажей по информационной безопасности.
56. Журнал учета обращений субъектов персональных данных.
57. Журнал учета логинов администраторов ГИС.
58. Журнал учета проведения анализа угроз информационной без­опасности и уязвимостей программного обеспечения.
59. Журнал учета получения и установки программного обеспечения и антивирусных баз.
60. Журнал учета проведения контроля за обеспечением уровня защищенности ин­формации в ГИС.
61. Технический паспорт ГИС.
62. Перечень основных технических средств ГИС.
63. Логическая структура ГИС.
64. Физическая топология ГИС.
65. Перечень программного обеспечения ГИС.
66. Перечень сертифицированных средств защиты информации ГИС.
67. Сведения об установленных в ГИС требованиях к мерам по обеспечению безопасности информации
68. Схемы размещения технических средств ГИС.
69. Схема организации криптографической защиты информации ГИС.
70. Модель нарушителя и модель угроз безопасности информации, обрабатываемой в ГИС.
71. Программа и методика аттестационных испытаний ГИС на соответствие требованиям по обеспечению безопасности информации (разрабатывает лицензиат Федеральной службы по техническому и экспортному контролю).
72. Протокол аттестационных испытаний на соответствие требованиям безопасности информации ГИС(выдает лицензиат Федеральной службы по техническому и экспортному контролю).
73. Заключение по результатам аттестационных испытаний ГИС (выдает лицензиат Федеральной службы по техническому и экспортному контролю).
74. Аттестат соответствия ГИС требованиям по обеспечению безопасности информации (выдает лицензиат Федеральной службы по техническому и экспортному контролю).
75. График работ по аттестации ГИС.
76. План организационно-технических мероприятий по защите информации в ГИС на текущий год.
77. Результаты ежеквартального мониторинга ГИС по оценке состояния информационной безопасности, прогнозированию и обнаружению информационных угроз, определению приоритетных направлений их предотвращения и ликвидации последствий их проявления.