О политике информационной безопасности органов

исполнительной власти Омской области

В целях реализации Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 9 сентября 2000 года № Пр-1895, плана мероприятий по обеспечению информационной безопасности в органах исполнительной власти Омской области и их подведомственных учреждениях, утвержденного Губернатором Омской области от 18 февраля 2014 года № ГБ-225/01, подпункта 20 пункта 9 Положения о Главном управлении информационных технологий и связи Омской области, утвержденного Указом Губернатора Омской области от 6 сентября 2013 года № 123, постановляю:

1. Утвердить прилагаемую политику информационной безопасности органов исполнительной власти Омской области (далее – политика информационной безопасности).
2. Органам исполнительной власти Омской области и их подведомственным учреждениям выполнять требования политики информационной безопасности.
3. Рекомендовать органам местного самоуправления Омской области руководствоваться требованиями политики информационной безопасности.
4. Главному управлению информационных технологий и связи Омской области обеспечить реализацию политики информационной безопасности органов исполнительной власти Омской области на территории Омской области.
5. Контроль исполнения настоящего постановления возложить на заместителя Председателя Правительства Омской области, руководителя Аппарата Губернатора и Правительства Омской области В.Б. Компанейщикова.

Губернатор Омской области,

Председатель Правительства

Омской области В.И. Назаров

Приложение

к постановлению Правительства Омской области

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_

ПОЛИТИКА

информационной безопасности органов исполнительной власти

Омской области

1. Общие положения

1. Понятия и термины, применяемые в настоящей политике, используются в значениях, установленных:

1. Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 9 сентября 2000 года № Пр-1895;
2. Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральным закономот 27 июля 2006 года № 152-ФЗ «О персональных данных»;
4. Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
5. Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
8. Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»;
10. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»;
11. ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

2. Законодательной основой политики являются [Конституция Российской Федерации](http://securitypolicy.ru/index.php/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%86%D0%B8%D1%8F_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8), [Гражданский](http://securitypolicy.ru/index.php/%D0%92%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8_%D0%B8%D0%B7_%D0%93%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8) и [Уголовный кодексы](http://securitypolicy.ru/index.php/%D0%92%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8_%D0%B8%D0%B7_%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8), законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

3. Политика предназначена для обеспечения общих основ информационной безопасности и выбора практических мероприятий по обеспечению и управлению информационной безопасностью в органах исполнительной власти Омской области (далее – органы власти) и их подведомственных учреждениях (далее – учреждения).

4. Органы власти и учреждения обязаны соблюдать требования настоящей политики и законодательства Российской Федерации в сфере информационной безопасности.

5. Работники органов власти и учреждений, ответственные за информационную безопасность, разрабатывают на местах организационно-распорядительную документацию, дополняющую данную политику.

1. Объекты защиты
2. Объектами защиты органов власти и учреждений являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3. Цели и задачи обеспечения информационной безопасности

1. Целью информационной безопасности является обеспечение непрерывности работы органов власти и учреждений при выполнении своих полномочий и функций.
2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств объектов защиты:
3. конфиденциальность;
4. целостность;
5. доступность.
6. Необходимый уровень конфиденциальности, целостности и доступности обеспечивается соответствующими множеству значимых факторов, воздействующих на безопасность информации, мерами и средствами обеспечения информационной безопасности.
7. Задачами для достижения цели информационной безопасности являются:
8. организация системы менеджмента информационной безопасности;
9. своевременное выявление, оценка и прогнозирование факторов, воздействующих на безопасность информации, причин и условий, способствующих нарушению нормального функционирования информационных систем органов власти и учреждений;
10. создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
11. создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
12. защита от несанкционированного доступа к объектам защиты;
13. защита от несанкционированной модификации используемых в информационных системах органов власти и учреждений программных средств, а также защита информационных систем от внедрения несанкционированных программ, включая компьютерные вирусы;
14. определение основных принципов информационной безопасности;
15. определение мер и средств обеспечения информационной безопасности.
16. Поставленные цели и решение задач достигаются:
17. строгим учетом всех объектов защиты;
18. категорированием и классификацией информационных систем и ресурсов для обеспечения защиты на надлежащем уровне;
19. регистрированием действий работников органов власти и учреждений, осуществляющих обслуживание объектов защиты;
20. распределением обязанностей по обеспечению информационной безопасности. Полномочия работников должны быть четко определены и закреплены должностными регламентами (инструкциями), в том числе в служебных контрактах (трудовых договорах) с работниками органов власти и учреждений;
21. выполнением всеми пользователями информационных систем органов власти и учреждений требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
22. персональной ответственностью за свои действия каждого работника, имеющего доступ к объектам защиты органов власти и учреждений, в рамках своих функциональных обязанностей;
23. повышением квалификации работников, ответственных за защиту информации в органах власти и учреждениях;
24. полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов органов власти и учреждений по вопросам обеспечения информационной безопасности;
25. систематической оценкой рисков. Решения о расходах на мероприятия по информационной безопасности в органах власти и учреждениях должны приниматься исходя из возможного ущерба в результате нарушения информационной безопасности;
26. непрерывным поддержанием необходимого уровня информационной безопасности органов власти и учреждений;
27. применением физических и технических (программно-аппаратных) средств защиты информационных ресурсов органов власти и учреждений;
28. эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению информационной безопасности.
29. Система менеджмента информационной безопасности
30. Система менеджмента информационной безопасности предназначена для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы защиты информации в органах власти и учреждениях при выполнении своих функций.
31. Основные принципы системы менеджмента информационной безопасности:
32. понимание необходимости системы информационной безопасности;
33. назначение ответственности за информационную безопасность;
34. создание административных обязанностей работников органов власти и учреждений, ответственных за обеспечение информационной безопасности;
35. оценка риска, определяющая соответствующие меры и средства контроля и управления информационной безопасностью;
36. обеспечение комплексного подхода к менеджменту информационной безопасности;
37. выявление и предупреждение инцидентов информационной безопасности;
38. непрерывная переоценка и соответствующая модификация системы информационной безопасности.
39. Для непосредственной организации и эффективного функционирования системы менеджмента информационной безопасности, исключающей возможные конфликты интересов, в органах власти целесообразно создать подразделение (назначить лицо), ответственное за обеспечение информационной безопасности, и возложить на него решение следующих основных задач:
40. реализация политики информационной безопасности, определение требований к системе защиты информации;
41. анализ текущего состояния обеспечения информационной безопасности;
42. организация мероприятий и координация работ по защите информации всех подразделений органов власти и учреждений;
43. контроль и оценка эффективности применяемых мер и средств защиты информации.
44. Основными функциями подразделений (лиц), ответственных за обеспечение информационной безопасности органов власти и учреждений, являются:
45. формирование требований к системам защиты в процессе создания и дальнейшего развития существующих объектов защиты;
46. подготовка решений по обеспечению конфиденциальности, целостности, доступности объектов защиты;
47. участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;
48. обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
49. разграничение доступа пользователей к объектам защиты;
50. наблюдение за функционированием системы защиты и ее элементов;
51. проверка надежности функционирования системы защиты;
52. разработка мер нейтрализации моделей возможных атак;
53. обучение работников правилам безопасной обработки информации;
54. контроль соответствия действий администраторов и пользователей установленным правилам обращения с информацией;
55. участие по указанию руководства в служебной проверке по фактам нарушения правил обращения с информацией и оборудованием вучреждениях в соответствии с законодательством Российской Федерации;
56. сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.
57. Факторы, воздействующие на безопасность информации
58. Выявление и учет факторов, воздействующих на защищаемую информацию, составляют основу для планирования и проведения эффективных мероприятий по информационной безопасности.
59. Выявление факторов, воздействующих на безопасность информации, должно осуществляться с учетом следующих требований:
60. достаточности уровней классификации факторов, позволяющих формировать их полное множество;
61. гибкость классификации, позволяющей расширять множества классифицируемых факторов, а также вносить необходимые изменения без нарушения структуры классификации.
62. Все множество факторов, воздействующих на защищаемую информацию, по природе их возникновения разделяются на два класса:
63. Объективные – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;
64. Субъективные – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные. Непреднамеренные угрозы вызваны ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п. Преднамеренные угрозы связанны с корыстными, идейными или иными устремлениями людей (злоумышленников).
65. По отношению к объектам защиты факторы разделяются на внутренние и внешние.
66. Основными факторами, воздействующими на безопасность информации, для органов власти и учреждений являются:
67. непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационных систем органов власти и учреждений (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем органов власти и учреждений;
68. преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом, халатность и т.п.) действия легально допущенных к информационным ресурсам органов власти и учреждений пользователей (в том числе работников, отвечающих за обслуживание и администрирование информационных систем), приводящие к непроизводительным затратам времени и ресурсов, разглашению, потере конфиденциальной информации или нарушению работоспособности информационных систем органов власти и учреждений;
69. деятельность преступных групп и формирований, политических и экономических структур, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационных систем органов власти и учреждений;
70. ошибки, допущенные при разработке компонентов информационных систем органов власти и учреждений и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);
71. явления техногенного характера, стихийные бедствия.
72. Реализация основных объективных факторов, воздействующих на безопасность информации, возможна путем:
73. выхода из строя оборудования и программных средств информационных систем органов власти и учреждений;
74. выхода из строя или невозможность использования линий связи;
75. пожаров, наводнений и других стихийных бедствий и явлений техногенного характера.
76. Реализация непреднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:
77. неумышленных действий, приводящих к частичному или полному нарушению функциональности компонентов информационных систем органов власти и учреждений или разрушению информационных или программно-технических ресурсов;
78. неосторожных действий, приводящих к разглашению информации ограниченного распространения или делающих ее общедоступной;
79. разглашения, передачи или утраты атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);
80. игнорирования организационных правил при работе с информационными ресурсами;
81. проектирования архитектуры систем, технологий обработки данных, разработки программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем органов власти и учреждений и информационной безопасности;
82. пересылки данных и документов по ошибочному адресу (устройства);
83. ввода ошибочных данных;
84. неумышленной порчи и утраты носителей информации;
85. неумышленного повреждения каналов связи;
86. неправомерного отключения оборудования или изменения режимов работы устройств или программ;
87. заражения компьютеров вирусами;
88. несанкционированного запуска технологических программ, способных вызвать потерю работоспособности информационных систем органов власти и учреждений или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
89. некомпетентного использования, настройки или неправомерного отключения средств защиты.
90. Реализация преднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:
91. умышленных действий, приводящих к частичному или полному нарушению функциональности информационных систем органов власти и учреждений или разрушению информационных или программно-технических ресурсов;
92. действий по дезорганизации функционирования информационных систем органов власти и учреждений;
93. хищения документов и носителей информации;
94. несанкционированного копирования документов и носителей информации;
95. умышленного искажения информации, ввода неверных данных;
96. отключения или вывода из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
97. перехвата данных, передаваемых по каналам связи, и их анализа;
98. хищения производственных отходов (распечаток документов, записей, носителей информации и т.п.);
99. незаконного получения атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
100. несанкционированного доступа к ресурсам информационных систем органов власти и учреждений с рабочих станций легальных пользователей;
101. хищения или вскрытия шифров криптозащиты информации;
102. внедрения аппаратных и программных закладок с целью скрытного осуществления доступа к информационным ресурсам или дезорганизации функционирования информационных систем органов власти и учреждений;
103. незаконного использования оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
104. применения подслушивающих устройств, дистанционной фото- и видео съемки для несанкционированного съема информации.
105. Основные принципы информационной безопасности
106. При построении системы информационной безопасности органов власти и учреждений необходимо руководствоваться следующими основными принципами:
     1. законность (осуществление защитных мероприятий и разработки системы информационной безопасности органов власти и учреждений в соответствии с действующим законодательством в области защиты информации);
     2. системность (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности);
     3. комплексность (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов);
     4. непрерывность (постоянная работа и организационная поддержка мер и средств защиты для эффективного обеспечения информационной безопасности);
     5. своевременность (постановка задач по комплексной защите информации и реализация мер обеспечения информационной безопасности на ранних стадиях разработки информационных систем в целом и их систем защиты информации в частности);
     6. преемственность и непрерывность совершенствования (совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите);
     7. разумная достаточность (выбор достаточного уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми);
     8. персональная ответственность (ответственность за обеспечение информационной безопасности для каждого работника органа власти и учреждения в пределах его полномочий);
     9. минимизация полномочий (предоставление пользователям минимальных прав в соответствии с должностными регламентами, должностными инструкциями работников органов власти и учреждений);
     10. исключение конфликта интересов (четкое разделение обязанностей работников органов власти и учреждений и исключение ситуаций, когда сфера ответственности допускает конфликт интересов);
     11. взаимодействие и сотрудничество (работники органов власти и учреждений должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений (ответственных лиц) за обеспечение информационной безопасности);
     12. гибкость системы защиты (способность реагировать на изменения внешней среды и условий осуществления органами власти и учреждениями своих функций);
     13. простота применения средств защиты (не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при работе пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций);
     14. обоснованность и техническая реализуемость (реализация на современном уровне развития науки и техники, обоснованность с точки зрения достижения заданного уровня безопасности информации, а также соответствие установленным нормам и требованиям по безопасности информации);
     15. специализация и профессионализм (реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными работниками);
     16. обязательность контроля (обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств).
107. Меры и средства обеспечения информационной безопасности
108. При осуществлении менеджмента информационной безопасности необходимо выделить следующие основные меры обеспечения информационной безопасности:
109. законодательные (законодательство Российской Федерации в сфере информационной безопасности). Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с работниками органов власти и учреждений;
110. морально-этические (нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе). Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в органах власти и учреждениях;
111. технологические (технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий);
112. организационные (меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность работников, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации);
113. физические (меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для предотвращения несанкционированного доступа к объектам защиты, а также технических средств визуального наблюдения, связи и охранной сигнализации);
114. технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющих функции защиты).
115. Для обеспечения информационной безопасности необходимо использовать средства:
116. физической защиты (введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки конфиденциальной информации, оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи);
117. антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);
118. резервирования (поддержание целостности и доступности объектов защиты);
119. разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);
120. криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств криптографической защиты информации, в том числе при передаче по каналам связи);
121. идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);
122. контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности функционирования системы защиты и целостности хранимой и обрабатываемой информации);
123. контроля и регистрации событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).
124. При выполнении договорных отношений между органами власти и учреждениями и сторонними организациями (предоставление доступа сторонним организациям к объектам защиты) обязательно выполнение всех необходимых мер и средств обеспечения информационной безопасности.
125. В служебной деятельности работники органов власти и учреждений обязаны использовать адреса электронной почты, зарегистрированные в почтовом домене Правительства Омской области omskportal.ru, запрещается использование сторонних серверов и сервисов электронной почты.
126. Ответственность за нарушение обеспечения информационной безопасности
127. Нарушение информационной безопасности может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_