



**Министерство цифрового
развития и связи Омской области**

П Р И К А З

22 декабря 2022 года

№ 6-п

г. Омск

**Об утверждении политики информационной безопасности органов
исполнительной власти Омской области**

В соответствии пунктом 1 распоряжения Губернатора Омской области № 244-р от 1 октября 2015 года «О политике информационной безопасности органов исполнительной власти Омской области»:

Утвердить политику информационной безопасности органов исполнительной власти Омской области согласно приложению к настоящему приказу.

Министр

 А.А. Ключенко

Приложение
к приказу Министерства цифрового развития
и связи Омской области
от 22 декабря 2022 № 6-н

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 Указом Президентом Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

2) Федеральным законом № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»;

3) Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

4) постановлением Правительства Российской Федерации № 211 от 21 марта 2012 года «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 № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

6) постановлением Правительства Российской Федерации № 687 от 15 сентября 2008 года «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

7) приказом Федеральной службы по техническому и экспортному контролю № 21 от 18 февраля 2013 года «Об утверждении Составы 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 № 17 от 11 февраля 2013 года «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. 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).

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

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

2. Объекты защиты

5. Объектами защиты 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

6. Целью политики информационной безопасности является обеспечение непрерывности работы органов власти и учреждений при выполнении своих полномочий и функций.

7. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих основных свойств объектов защиты:

- 1) конфиденциальность;
- 2) целостность;
- 3) доступность.

8. Необходимый уровень конфиденциальности, целостности и доступности обеспечивается соответствующими множеством значимых

факторов, воздействующих на безопасность информации, мерами и средствами обеспечения информационной безопасности.

9. Задачами политики информационной безопасности являются:

- 1) организация системы менеджмента информационной безопасности;
- 2) своевременное выявление, оценка и прогнозирование факторов, воздействующих на безопасность информации, причин и условий, способствующих нарушению нормального функционирования информационных систем органов власти и учреждений;
- 3) создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- 4) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
- 5) защита от несанкционированного доступа к объектам защиты;
- 6) 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;
- 7) определение основных принципов информационной безопасности;
- 8) определение мер и средств обеспечения информационной безопасности.

10. Поставленные цели и решение задач достигаются:

- 1) строгим учетом всех объектов защиты;
- 2) категорированием и классификацией информационных систем и ресурсов для обеспечения защиты на надлежащем уровне;
- 3) регистрированием действий работников органов власти и учреждений, осуществляющих обслуживание объектов защиты;
- 4) 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;
- 5) выполнением всеми пользователями информационных систем органов власти и учреждений требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- 6) персональной ответственностью за свои действия каждого работника, имеющего доступ к объектам защиты органов власти и учреждений, в рамках своих функциональных обязанностей;
- 7) повышением квалификации работников, ответственных за защиту информации в органах власти и учреждениях;
- 8) полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов органов власти и учреждений по вопросам обеспечения информационной безопасности;
- 9) систематической оценкой рисков;

- 10) непрерывным поддержанием необходимого уровня информационной безопасности органов власти и учреждений;
- 11) применением физических и технических (программно-аппаратных) средств защиты информационных ресурсов органов власти и учреждений;
- 12) эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению информационной безопасности.

4. Система менеджмента информационной безопасности

11. 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.

12. Основные принципы системы менеджмента информационной безопасности:

- 1) понимание необходимости системы информационной безопасности;
- 2) назначение ответственности за информационную безопасность;
- 3) создание административных обязанностей работников органов власти и учреждений, ответственных за обеспечение информационной безопасности;
- 4) оценка риска, определяющая соответствующие меры и средства контроля и управления информационной безопасностью;
- 5) обеспечение комплексного подхода к менеджменту информационной безопасности;
- 6) выявление и предупреждение инцидентов информационной безопасности;
- 7) непрерывная переоценка и соответствующая модификация системы информационной безопасности.

13. Для непосредственной организации и эффективного функционирования системы менеджмента информационной безопасности, исключаяющей возможные конфликты интересов, в органах власти целесообразно создать подразделение или назначить лицо, ответственное за обеспечение информационной безопасности, и возложить на него решение следующих основных задач:

- 1) реализация политики информационной безопасности, определение требований к системе защиты информации;
- 2) анализ текущего состояния обеспечения информационной безопасности;
- 3) организация мероприятий и координация работ по защите информации всех подразделений органов власти и учреждений;
- 4) контроль и оценка эффективности применяемых мер и средств защиты информации.

14. Основными функциями подразделений (лиц), ответственных за

обеспечение информационной безопасности органов власти и учреждений, являются:

- 1) формирование требований к системам защиты в процессе создания и дальнейшего развития существующих объектов защиты;
- 2) подготовка решений по обеспечению конфиденциальности, целостности, доступности объектов защиты;
- 3) участие в проектировании систем защиты, их испытаниях и приемке в эксплуатацию;
- 4) обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
- 5) разграничение доступа пользователей к объектам защиты;
- 6) наблюдение за функционированием системы защиты и ее элементов;
- 7) проверка надежности функционирования системы защиты;
- 8) разработка мер нейтрализации моделей возможных атак;
- 9) обучение работников правилам безопасной обработки информации;
- 10) контроль соответствия действий администраторов и пользователей установленным правилам обращения с информацией;
- 11) участие по указанию руководства в служебной проверке по фактам нарушения правил обращения с информацией и оборудованием в учреждениях в соответствии с законодательством Российской Федерации;
- 12) сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности.

5. Факторы, воздействующие на безопасность информации

15. Выявление и учет факторов, воздействующих на защищаемую информацию, составляют основу для планирования и проведения эффективных мероприятий по информационной безопасности.

16. Выявление факторов, воздействующих на безопасность информации, должно осуществляться с учетом следующих требований:

- 1) достаточности уровней классификации факторов, позволяющих формировать их полное множество;
- 2) гибкость классификации, позволяющей расширять множества классифицируемых факторов, а также вносить необходимые изменения без нарушения структуры классификации.

17. Все множество факторов, воздействующих на защищаемую информацию, по природе их возникновения разделяется на два класса:

- 1) объективные - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независимых от человека;
- 2) 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 связаны с корыстными, идейными или иными устремлениями людей (злоумышленников).

18. По отношению к объектам защиты факторы разделяются на внутренние и внешние.

19. Основными факторами, воздействующими на безопасность информации, для органов власти и учреждений являются:

1) 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;

2) 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;

3) 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;

4) 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);

5) явления техногенного характера, стихийные бедствия.

20. Реализация основных объективных факторов, воздействующих на безопасность информации, возможна путем:

1) выхода из строя оборудования и программных средств информационных систем органов власти и учреждений;

2) выхода из строя или невозможность использования линий связи;

3) пожаров, наводнений и других стихийных бедствий и явлений техногенного характера.

21. Реализация непреднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

1) неумышленных действий, приводящих к частичному или полному нарушению функциональности компонентов информационных систем органов

власти и учреждений или разрушению информационных или программно-технических ресурсов;

2) неосторожных действий, приводящих к разглашению информации ограниченного распространения или делающих ее общедоступной;

3) разглашения, передачи или утраты атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т.п.);

4) игнорирования организационных правил при работе с информационными ресурсами;

5) проектирования архитектуры систем, технологий обработки данных, разработки программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем органов власти и учреждений и информационной безопасности;

6) пересылки данных и документов по ошибочному адресу (устройства);

7) ввода ошибочных данных;

8) неумышленной порчи и утраты носителей информации;

9) неумышленного повреждения каналов связи;

10) неправомерного отключения оборудования или изменения режимов работы устройств или программ;

11) заражения компьютеров вирусами;

12) 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.);

13) некомпетентного использования, настройки или неправомерного отключения средств защиты.

22. Реализация преднамеренных субъективных факторов, воздействующих на безопасность информации, возможна путем:

1) умышленных действий, приводящих к частичному или полному нарушению функциональности информационных систем органов власти и учреждений или разрушению информационных или программно-технических ресурсов;

2) действий по дезорганизации функционирования информационных систем органов власти и учреждений;

3) хищения документов и носителей информации;

4) несанкционированного копирования документов и носителей информации;

5) умышленного искажения информации, ввода неверных данных;

6) отключения или вывода из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);

7) перехвата данных, передаваемых по каналам связи, и их анализа;

8) хищения производственных отходов (распечаток документов,

записей, носителей информации и т.п.);

9) незаконного получения атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);

10) несанкционированного доступа к ресурсам информационных систем органов власти и учреждений с рабочих станций легальных пользователей;

11) хищения или вскрытия шифров криптозащиты информации;

12) внедрения аппаратных и программных закладок с целью скрытного осуществления доступа к информационным ресурсам или дезорганизации функционирования информационных систем органов власти и учреждений;

13) незаконного использования оборудования, программных средств или информационных ресурсов, нарушающего права третьих лиц;

14) применения подслушивающих устройств, дистанционной фото- и видеосъемки для несанкционированного съема информации.

6. Основные принципы информационной безопасности

23. 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 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 трудовых затрат 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).

7. Меры и средства обеспечения информационной безопасности

24. При осуществлении менеджмента информационной безопасности необходимо выделить следующие основные меры обеспечения информационной безопасности:

1) 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;

2) 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;

3) 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);

4) 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);

5) 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);

6) технические (меры защиты основаны на использовании различных электронных устройств и специального программного обеспечения, выполняющих функции защиты).

25. Для обеспечения информационной безопасности необходимо использовать средства:

1) 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);

2) антивирусной защиты (предотвращение потерь, ошибок и модификации информационных ресурсов);

3) резервирования (поддержание целостности и доступности объектов защиты);

4) разграничения доступа (управление доступом к информационным ресурсам, к сети общего пользования, к локальной вычислительной сети);

5) криптографической защиты (защита конфиденциальности, целостности и аутентичности информационных ресурсов путем применения средств криптографической защиты информации, в том числе при передаче по каналам связи);

6) идентификации и аутентификации (предотвращение работы с информационными ресурсами посторонних лиц путем обеспечения возможности распознавания каждого легального пользователя);

7) контроля целостности (своевременное обнаружение модификации или искажения информационных ресурсов, обеспечение правильности

функционирования системы защиты и целостности хранимой и обрабатываемой информации);

8) контроля и регистрации событий информационной безопасности (обеспечение обнаружения и регистрации всех событий, которые могут повлечь за собой нарушение информационной безопасности).

26. 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.

27. 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.

8. Ответственность за нарушение обеспечения информационной безопасности

28. Нарушение информационной безопасности может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.