



ПОСТАНОВЛЕНИЕ
АДМИНИСТРАЦИИ ОРДИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ПЕРМСКОГО КРАЯ

11.10.2024

№ 1352

**Об утверждении Политики
информационной безопасности
в администрации Ординского
муниципального округа
Пермского края**

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», администрация Ординского муниципального округа

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Политику информационной безопасности в администрации Ординского муниципального округа Пермского края.
2. Постановление вступает в силу с момента его подписания.
3. Контроль за исполнением постановления возложить на руководителя аппарата администрации муниципального округа Кузнецову Н.В.

Глава муниципального округа

А.С. Мелёхин

Политика
информационной безопасности в администрации
Ординского муниципального округа Пермского края

I. Общие положения

1. Политика информационной безопасности (далее – Политика) определяет принятие правовых, организационных и технических мер, которыми руководствуется администрация Ординского муниципального округа Пермского края (далее – администрация), в своей деятельности направленных на:

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.

Основными составными элементами Политики являются:

защита информации при организации работ с персональными данными;

защита информации, не составляющей государственную тайну, в автоматизированных и информационных системах;

защита информации с ограниченным доступом, не составляющей государственную тайну, с использованием средств криптографической защиты информации;

защита информации, размещаемой на «Официальном сайте Ординского муниципального округа» в информационно-телекоммуникационной сети «Интернет».

2. Общее руководство обеспечением информационной безопасности администрации осуществляет глава муниципального округа – глава администрации Ординского муниципального округа Пермского края. В администрации обеспечением информационной безопасности осуществляет отдел организационно-правовой работы администрации Ординского муниципального округа Пермского края (далее – Отдел). Контроль за соблюдением требований по информационной безопасности несет должностное лицо, назначенное ответственным за защиту информации.

II. Область применения

3. Настоящая Политика распространяется на все отделы администрации и обязательна к исполнению всеми ее сотрудниками.

4. Сотрудники обязаны соблюдать порядок обращения с конфиденциальными документами, ключевыми носителями и другой защищаемой информацией, соблюдать требования настоящей Политики и иных документов, регламентирующих деятельность в области информационной безопасности.

5. Действие Политики не распространяется на отношения, возникающие при обработке информации ограниченного доступа, содержащей сведения, составляющие государственную тайну. Защита информации, содержащей сведения, составляющие государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

III. Термины и определения

6. В настоящей Политике используются следующие термины:

автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

аудит информационной безопасности администрации – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой администрацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит);

информационная технология – совокупность правил, приемов и методов применения средств вычислительной техники для выполнения функций хранения, обработки, передачи и использования производственной, финансовой, аналитической или иной информации, связанной с функционированием администрации;

информационный технологический процесс – часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования администрации;

информационная безопасность администрации – состояние защищенности информационных активов администрации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры администрации;

информационные активы администрации – активы администрации, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей;

инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов администрации;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств в соответствии с законодательством;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

мониторинг информационной безопасности администрации – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности администрации, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и прочее;

несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств,

предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем;

политика информационной безопасности администрации – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых администрацией для обеспечения информационной безопасности;

риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы;

роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом администрации. К субъектам относятся сотрудники администрации, посетители, а также иницилируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему;

режим конфиденциальности информации – организационно-технические мероприятия по обеспечению конфиденциальности информации (защите информации), включающие в себя:

определение перечня информации, составляющей конфиденциальную информацию;

ограничение доступа к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

учет лиц, получивших доступ к конфиденциальной информации, и(или) лиц, которым такая информация была предоставлена или передана;

регулирование отношений по использованию конфиденциальной информации работниками на основании трудовых договоров, контрагентами на основании гражданско-правовых договоров и соглашений, работниками со срочными трудовыми договорам и проходящих в администрации практику (стажировку);

угроза – опасность, предполагающая возможность потери (блокирования) информации;

управление информационной безопасностью администрации - совокупность целенаправленных действий, осуществляемых в рамках настоящей Политики в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер - защита информации);

уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности администрации при реализации угроз в информационной сфере;

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

IV. Основные принципы обеспечения информационной безопасности

7. Основными принципами обеспечения информационной безопасности являются:

постоянный и всесторонний анализ автоматизированных систем и информационных технологий с целью выявления уязвимостей информационных активов администрации;

своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность, корректировка моделей угроз и нарушителя;

разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом. При этом меры, принимаемые для обеспечения информационной безопасности, не должны усложнять деятельность администрации, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности;

контроль эффективности принимаемых защитных мер;

персонафикация и адекватное разделение ролей и ответственности между сотрудниками администрации, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

V. Цели и задачи информационной безопасности

8. Основной целью является защита информации, содержащейся в информационных системах от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий сотрудников администрации или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности информации.

9. Для достижения цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности должна обеспечивать эффективное решение следующих задач, таких как:

оценка состояния информационной безопасности, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

укрепление вертикали управления и централизация сил обеспечения информационной безопасности в органе власти и местного самоуправления;

совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;

организация и координация руководством органа власти и местного самоуправления работ по обеспечению информационной безопасности;

возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника органа власти и местного самоуправления в пределах его полномочий;

обеспечение непрерывного функционирования информационных систем и системы обеспечения информационной безопасности;

обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты информационной безопасности;

ведение мониторинга состояния защищенности информации при ее обработке в информационных системах;

защита от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных (трудовых) обязанностей), то есть защиту информации от несанкционированного доступа;

защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

обеспечение работоспособности криптографических средств защиты информации;

постоянный контроль выполнения требований законодательства Российской Федерации в области обеспечения информационной безопасности;

создание системы непрерывного обучения, тренировки и проверки осведомленности сотрудников администрации по вопросам обеспечения информационной безопасности;

обеспечение защиты информации от несанкционированного доступа, предотвращение утраты, искажения или уничтожения информации на этапах сбора, обработки, хранения и предоставления конечному потребителю информации.

10. Поставленные основные цели и задачи обеспечения информационной безопасности достигаются:

учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных систем);

полнотой и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

подготовкой сотрудников администрации, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности;

четким знанием и строгим соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

персональной ответственностью за свои действия каждого сотрудника администрации, имеющего доступ к информационным ресурсам, в рамках выполнения своих трудовых обязанностей;

эффективным контролем за соблюдением пользователями информационных ресурсов обязательных требований по обеспечению информационной безопасности.

VI. Объекты обеспечения информационной безопасности

11. К объектам обеспечения информационной безопасности относятся:

информационные ресурсы, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (служебная тайна, персональные данные и другая информация ограниченного распространения), а также общедоступная (открытая) информация;

системы формирования, распространения и использования информационных ресурсов, включающие в себя информационные системы различного класса и назначения, правила и процедуры сбора, обработки, хранения и передачи информации;

информационная инфраструктура, включающая центры обработки и анализа информации, средства, системы связи и передачи данных.

12. При этом, в информационной системе объектами информационной безопасности 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.

13. Информационная безопасность всех вышеуказанных объектов создаст условия надежного функционирования администрации.

VII. Основные направления деятельности администрации по обеспечению информационной безопасности

14. Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

15. К основным направлениям обеспечения информационной безопасности относятся:

правовое обеспечение информационной безопасности – деятельность направлена на создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности;

организация деятельности по обеспечению информационной безопасности – деятельность направлена на создание документированных процессов обеспечения информационной безопасности между всеми подразделениями органа власти и местного самоуправления;

обеспечение информационной безопасности при управлении информационными ресурсами – деятельность направлена на идентификацию, классификацию информационных систем и ресурсов, а также их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов;

обеспечение информационной безопасности, связанное с сотрудниками администрации – деятельность направлена на минимизацию рисков, вызванных действиями сотрудников администрации в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников администрации по вопросам обеспечения информационной безопасности;

физическая безопасность информационных ресурсов – деятельность направлена на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные системы и ресурсы;

обеспечение информационной безопасности на этапах жизненного цикла информации в информационной инфраструктуре – деятельность направлена на минимизацию рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационных системах;

управление доступом к информационным ресурсам – деятельность направлена на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;

управление инцидентами информационной безопасности – деятельность направлена на проведение мероприятий по своевременному выявлению и реагированию на инциденты информационной безопасности;

соответствие обязательным требованиям – деятельность направлена на соответствие требованиям законодательства Российской Федерации, локальных нормативных актов по обеспечению информационной безопасности.

VIII. Принципы формирования системы обеспечения информационной безопасности

16. Построение системы обеспечения информационной безопасности и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

К основным принципам формирования системы обеспечения информационной безопасности относятся:

законность – предполагает разработку системы обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области обеспечения информационной безопасности;

системность – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на них со стороны нарушителей, пути проникновения в информационные системы и несанкционированного доступа к информации;

централизация управления – предполагает, что деятельность по обеспечению информационной безопасности должна быть встроена в управленческие процессы администрации, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения информационной безопасности должны быть организованы и управляемы;

персональная ответственность – предполагает возложение персональной ответственности на каждого сотрудника администрации в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения информационной безопасности;

минимизация полномочий – предполагает предоставление прав доступа сотрудникам администрации к информационным ресурсам в том случае и объеме, необходимом для качественного выполнения своих служебных (трудовых) обязанностей;

своевременность – предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз безопасности информации, потенциально способных нанести ущерб;

комплексный подход – предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимосвязанных программно-технических, организационных, правовых мер обеспечения информационной безопасности на единой концептуальной основе;

непрерывность – предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты;

совершенствование – предполагает постоянное совершенствование мер и средств защиты информации на основе модернизации организационных и технических решений, кадрового состава, анализа функционирования информационной системы и системы ее защиты с учетом изменений в методах и средствах перехвата информации, обязательных требований по защите информации;

взаимодействие и сотрудничество – предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники администрации должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных за обеспечение информационной безопасности. Все сотрудники администрации должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе;

гибкость системы защиты – система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления администрацией своих полномочий. В число таких изменений входят изменения организационной и штатной структуры; изменение существующих или внедрение принципиально новых информационных систем, технических средств;

обоснованность и техническая реализуемость – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

обязательность контроля – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности. Выявленные недостатки системы обеспечения информационной безопасности должны немедленно доводиться до сведения руководителя администрации, а также оперативно устраняться.

IX. Требования по обеспечению информационной безопасности

17. Обеспечение безопасности информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы.

18. В качестве методов защиты информации применяются:

18.1. регламентация доступа в служебные помещения администрации.

Регламентация доступа в служебные помещения осуществляется в целях обеспечения физической сохранности носителей информации, оборудования и исключения возможности несанкционированного доступа в служебные помещения, в том числе в которых ведется обработка конфиденциальной информации;

18.2. разграничение доступа к техническим средствам и информационным ресурсам администрации.

Разграничение доступа к техническим средствам и информационным ресурсам направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

Для работы с информационными ресурсами сотруднику администрации предоставляется автоматизированное рабочее место (далее – АРМ). Программное обеспечение устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением. При передаче АРМ другому сотруднику администрации производится удаление профиля пользователя АРМ.

Для обеспечения безопасности информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

К работе с информационными ресурсами допускаются сотрудники администрации, ознакомленные с настоящей Политикой. Для осуществления доступа к информационным ресурсам сотруднику администрации создается учетная запись – присваивается уникальный идентификатор (имя, логин) и пароль доступа. При увольнении учетная запись служащего блокируется;

18.3. применение антивирусной защиты.

Антивирусная защита применяется с целью защиты информационных ресурсов и программного обеспечения (далее – ПО) от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее – вирус) посредством использования специализированного ПО (далее – антивирусное ПО).

Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается;

18.4. применение криптографической защиты информации.

Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи;

18.5. регламентация использования электронной почты.

Система электронной почты используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних

коммуникаций. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов вирусами.

Угрозы, связанные с электронной почтой:

возможность создания писем с фальшивыми адресами;

возможность нарушения конфиденциальности электронных писем;

возможность изменения в процессе передачи содержимого электронных писем;

осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражению вирусами;

получение спама.

Отправка, получение официальных запросов и ответов в целях исполнения своих функций осуществляется с использованием официальных адресов электронной почты.

Официальный адрес электронной почты администрации размещается на «Официальном сайте Ординского муниципального округа» в информационно-телекоммуникационной сети «Интернет», на бланках администрации. Специалист, ответственный за работу с официальной электронной почтой администрации, осуществляет работу с почтой согласно должностной инструкции.

Отправка, получение электронных сообщений в целях исполнения должностных обязанностей сотрудников администрации осуществляется с использованием индивидуального электронного адреса каждого сотрудника. При увольнении сотрудника администрации электронный почтовый ящик отключается с последующим автоматическим удалением.

При работе с электронной почтой сотрудники администрации обязаны:

перед отправкой тщательно проверять сообщения на отсутствие информации ограниченного доступа;

периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;

проверять сообщения электронной почты на наличие вирусов;

использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

При работе с электронной почтой сотруднику администрации запрещено:

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации;

отправлять персональные данные без предварительного обезличивания или шифрования;

отправлять сообщения с иного электронного почтового ящика или от имени другого сотрудника администрации без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое

злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных сотрудников администрации, кроме случаев, санкционированных руководителями, или в целях администрирования систем;

использовать веб-сервисы Google, Gmail, Hotmail, Yahoo, Яндекс или подобные почтовые системы третьих сторон («вебмайл») для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

Содержимое электронного почтового ящика сотрудника администрации может быть проверено Отделом без предварительного уведомления сотрудника администрации в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется сотруднику администрации и его руководителю функционального подразделения;

18.6. регламентация работы в сети «Интернет».

Сеть «Интернет» используется сотрудниками администрации для получения информации в рамках исполнения должностных обязанностей.

Регламентация работы в сети «Интернет» осуществляется с целью снижения риска заражения информационных ресурсов вирусами.

Доступ к сети «Интернет» предоставляется сотруднику администрации с АРМ, закрепленного за сотрудником администрации для исполнения должностных обязанностей, с использованием учетной записи служащего.

Угрозы, связанные с работой в сети «Интернет»:

легкость перехвата данных и фальсификации IP-адресов в сети «Интернет»;
заражение вирусами.

Сотрудникам администрации запрещается:

осуществлять действия, запрещенные законодательством Российской Федерации;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации;

распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети «Интернет»;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

передавать информацию, обрабатываемую в администрации, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, WhatsApp, Skype и другие), социальных сетей (Twitter, Facebook, LiveJournal и другие), облачных сервисов (iCloud, Google Drive, Dropbox и другие).

Сотрудники администрации обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить в Отдел.

Доступ к сети Интернет может быть заблокирован сотрудниками Отдела без предварительного уведомления сотрудника администрации при возникновении угрозы безопасности информации;

18.7. регламентация создания и эксплуатации информационных систем.

Для проведения работ по обеспечению безопасности информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Срок начала эксплуатации системы не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о вводе системы в эксплуатацию.

Сотрудники администрации осуществляют эксплуатацию системы в соответствии с рабочей документацией.

Х. Ответственные за обеспечение информационной безопасности

19. Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в администрации назначается сотрудник Отдела ответственным за обеспечение информационной безопасности.

20. На этого сотрудника возлагается решение следующих основных задач:

анализ текущего состояния обеспечения информационной безопасности;

организация мероприятий и координация работ по обеспечению информационной безопасности;

контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

21. Основные функции сотрудника Отдела обеспечения информационной безопасности заключаются в следующем:

формирование требований к системе обеспечения информационной безопасности в процессе создания и дальнейшего развития существующих компонентов информационной системы;

участие в проектировании системы обеспечения информационной безопасности, ее испытаниях и вводе в эксплуатацию;

обеспечение функционирования системы защиты информации и ее элементов, включая управление криптографическими системами;

обучение пользователей и обслуживающего персонала правилам обработки информации;

оказание методической помощи сотрудникам администрации в вопросах обеспечения информационной безопасности;

контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с конфиденциальной информацией;

организация по указанию руководства служебного расследования по фактам нарушения правил обращения с конфиденциальной информацией и оборудованием;

принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

участие в работе по выявлению и устранению компьютерных инцидентов информационной безопасности.

XI. Основные организационные, технические и правовые меры обеспечения безопасности информации

22. Для организации и внедрения системы защиты информации в информационной инфраструктуре администрации важное значение имеет анализ технических, структурных, эксплуатационных и иных особенностей информационных систем, используемых технологий и архитектурных решений.

23. Правовые (законодательные) меры обеспечения безопасности информационных систем.

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Следует учитывать, что лица, виновные в нарушении обязательных требований по обеспечению информационной безопасности несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

24. Организационные меры обеспечения безопасности информационных систем.

К организационным мерам обеспечения безопасности информационных систем – относятся меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

В целях минимизации риска неправомерного завладения информацией или совершения действий от имени другого пользователя в администрации принята политика чистого стола и чистого экрана. Ответственными за исполнением этой политики являются все сотрудники администрации, а контроль выполнением должны осуществлять руководители функциональных подразделений.

При работе с документами, распечатанными на бумажном носителе, необходимо придерживаться следующих правил:

держат в столе только те документы, которые необходимы для работы в настоящий момент;

не оставлять документы на столе, если сотрудник администрации выходит из-за рабочего места. Документы необходимо убирать в ящик стола или в соответствующие папки;

при работе с документами, содержащими информацию ограниченного доступа необходимо убирать их в сейф, если сотрудник администрации отходит от рабочего места.

25. При работе с документами в электронном виде необходимо придерживаться следующих правил:

всегда блокировать (Win+L) рабочий стол при выходе из-за рабочего места даже на непродолжительное время;

устанавливать монитор таким образом, чтобы его изображение не было видно от входной двери;

установить автоматическую блокировку экрана через 10 минут простоя (установив хранитель экрана (ScreenSaver) и поставить галочку «Запрашивать пароль» или «Начинать с экрана входа в систему»);

минимизировать заполнение рабочего стола ярлыками программ и папок, не размещать документы на рабочем столе;

использовать фоны рабочего стола, содержащие общие требования (рекомендации) по информационной безопасности.

26. Технические меры обеспечения безопасности информационных систем. Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

Технические меры обеспечения безопасности информационных систем реализуются, в том числе посредством применения средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Данный перечень размещен на официальном сайте Федеральной службы по техническому и экспортному контролю России (www.fstec.ru).

Применение организационных и технических мер защиты информации, реализуемых в информационных системах в рамках их систем защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение вторжений;

контроль (анализ) защищенности информации;

обеспечение целостности информационной системы и информации;

обеспечение доступности информации;

защиту среды виртуализации;

защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных, в том числе, посредством применения активных и пассивных средств защиты

информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на обеспечение конфиденциальности, целостности и доступности информации.

В условиях растущего санкционного давления со стороны политических оппонентов и недружественных стран, осуществляющих контроль компаний производителей информационно-телекоммуникационного оборудования и программного обеспечения, в том числе с использованием возможностей спецслужб иностранных государств, администрации необходимо ориентироваться на выбор отечественного программного и информационно-телекоммуникационного оборудования, соответствующего требованиям информационной безопасности, что также соответствует текущему курсу импортозамещения Правительства Российской Федерации.

27. Криптографические методы и средства защиты.

Криптографические методы и средства защиты (далее – СКЗИ) используются для обеспечения информационной безопасности.

Организация системы информационной безопасности на основе инфраструктуры с использованием СКЗИ позволит решить задачи:

организации обеспечения защищенного документооборота с использованием имеющихся систем, как внутри, так и при взаимоотношениях с другими организациями. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;

реализации централизованно контролируемой системы информационной безопасности, при этом гибкой и динамически управляемой;

универсализации методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа по информационно-телекоммуникационным сетям общего пользования и других систем с использованием уже имеющихся в этих приложениях механизмов обеспечения информационной безопасности;

использования имеющихся реализаций российских криптографических алгоритмов в операциях с сертификатами и при защите электронного документооборота.

Использование СКЗИ для обеспечения безопасности информации необходимо в случаях, если:

информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью данных средств (передача информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче информации, содержащей сведения конфиденциального характера, по информационно-телекоммуникационным сетям общего пользования);

хранение информации на носителях, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью не криптографических методов и способов).

При применении СКЗИ требуется учитывать:

криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

для обеспечения безопасности информации при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России.

28. Физические меры защиты.

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключаяющими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

ХII. Порядок реагирования на компьютерные инциденты

29. Реагирование на компьютерные инциденты включает в себя выполнение следующих мероприятий:

29.1. фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;

29.2. координацию деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента;

29.3. фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;

29.4. определение причин инцидента и возможных его последствий для информационного ресурса:

первичный анализ инцидента;

комплексный анализ инцидента;

локализацию инцидента;

сбор сведений для последующего установления причин инцидента;

планирование мер по ликвидации последствий инцидента;

ликвидацию последствий инцидента;

контроль ликвидации последствий.

Решения должны приниматься отдельно для каждого информационного ресурса, затронутого компьютерным инцидентом.

ХIII. Обучение сотрудников администрации и повышение осведомленности в вопросах обеспечения информационной безопасности

30. Все пользователи информационной системы должны быть ознакомлены с организационно-распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, осуществляется под подпись. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки конфиденциальной информации.

31. Целью обучения сотрудников является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений законодательства Российской Федерации в области обеспечения информационной безопасности и правил по защите информации.

32. Задачи повышения осведомленности сотрудников администрации в вопросах информационной безопасности:

информирование сотрудников администрации о существующих угрозах и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации, обновление их теоретических и практических знаний в области обеспечения информационной безопасности;

доведение до сотрудников администрации основных положений, ограничений и требований существующих нормативно-распорядительных документов, принятых в администрации;

выработка у сотрудников администрации умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);

выработка у сотрудников администрации привычек, способствующих поддержанию высокого уровня информационной безопасности;

выработка у сотрудников администрации умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности;

доведение до сотрудников администрации их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации;

оценка эффективности, развитие и совершенствование проводимых мероприятий по информационной безопасности в целом.

Формы и методы повышения осведомленности сотрудников администрации в области информационной безопасности:

инструктаж при приеме на работу;

повышение квалификации (курсы, семинары, тренинги);

дистанционное обучение;

инструктажи и зачеты по положениям законодательства Российской Федерации в области обеспечения информационной безопасности и настоящей Политики.

XIV. Контроль состояния информационной безопасности

33. Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по

техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

34. Основная задача контроля заключается в получении объективных оценок текущего состояния обеспечения информационной безопасности, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности, оказание методической помощи по обеспечению защиты информации, организация работы по обеспечению информационной безопасности.

35. Контроль проводится Отделом обеспечения информационной безопасности или комиссией, назначаемой для этой цели.

36. Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.