**ГЛАВА КРЫЛОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**КИРОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**ПРИМОРСКОГО КРАЯ**

**РАСПОРЯЖЕНИЕ**

**17.07.2024 с. Крыловка 21 -од**

**О назначении ответственного за организацию обработки персональных данных и администратора безопасности в сегменте государственной информационной системы Приморского края** **"****Региональная информационная система обеспечения Градостроительной деятельности Приморского края"**

В целях исполнения Федерального закона от 27.07.2006 N 152-ФЗ   
"О персональных данных", Приказа ФСТЭК России от 11 февраля 2013 г. N 17  
"Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах",

1. Ответственным за организацию обработки персональных данных в администрации Крыловского сельского поселения назначить главу Крыловского сельского поселения Медведева Василия Сергеевича.
2. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.
3. Утвердить прилагаемую инструкцию ответственного за организацию обработки персональных данных.
4. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственному за организацию обработки персональных данных.
5. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.
6. Администратором безопасности в сегменте государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края " (далее –РИСОГД Приморского края) назначить главу Крыловского сельского поселения Медведева Василия Сергеевича.
7. Утвердить прилагаемую инструкцию администратора безопасности в сегменте РИСОГД Приморского края.
8. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности в сегменте РИСОГД Приморского края.
9. Администратору безопасности организовать проведение работ по защите информации в соответствии с руководящими документами ФСТЭК России и ФСБ России.
10. Допуск к обработке защищаемой информации осуществлять в соответствии с положениями о разграничении прав доступа в сегменте РИСОГД Приморского края (Приложение № 2 к Политике информационной безопасности в администрации Крыловского сельского поселения).
11. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении руководствоваться документом "Правила обработки персональных данных без использования средств автоматизации".
12. Лицам, допущенным к обработке персональных данных при автоматизированной их обработке и хранении руководствоваться следующими документами:

* Политика информационной безопасности в администрация Крыловского сельского поселения;
* инструкция пользователя сегмента государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края ".

1. Контроль за исполнением настоящего распоряжения оставляю за собой.

|  |  |  |
| --- | --- | --- |
| Глава Крыловского сельского поселения |  | В.С. Медведев |

УТВЕРЖДЕНА

распоряжением администрации

Крыловского сельского поселения

от "17" июля 2024г. № 21-од

**Инструкция администратора безопасности в сегменте  
государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края " администрации Крыловского сельского поселения**

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Администратор безопасности в сегменте государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края" (далее – Администратор) назначается распоряжением главы администрации Крыловского сельского поселения и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) и другой конфиденциальной информации в процессе ее обработки в сегменте государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края" (далее – РИСОГД Приморского края).
   2. Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере обработки и защиты ПДн и конфиденциальной информации.
   3. В своей деятельности Администратор руководствуется настоящей Инструкцией, Политика информационной безопасности в администрации Крыловского сельского поселения и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.
   4. Администратор безопасности подчиняется напрямую главе администрации Крыловского сельского поселения и имеет право требовать от пользователей сегмента РИСОГД Приморского края выполнения указаний и инструкций, связанных с защитой информации.
   5. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

* [Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) "Об информации, информационных технологиях и о защите информации"](https://www.consultant.ru/document/cons_doc_LAW_61798/);

* [Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) "О персональных данных"](https://www.consultant.ru/document/cons_doc_LAW_61801/);
* [Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"](https://www.consultant.ru/document/cons_doc_LAW_137356/);
* Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
* [Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"](https://www.consultant.ru/document/cons_doc_LAW_146520/);
* "Методический документ. Меры защиты информации в государственных информационных системах" (утв. ФСТЭК России 11.02.2014**)**;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
* ["Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)](https://www.consultant.ru/document/cons_doc_LAW_378330/);
* Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";
* Приказ ФАПСИ от 13.06.2001 N 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

1. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ В СЕГМЕНТЕ ГИС РИСОГД Приморского края
   1. Изучение особенностей технологических процессов обработки информации в администрации Крыловского сельского поселения с целью принятия решения о необходимости защиты информации в ГИС и классификации ГИС, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о ГИС сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.
   2. Определение актуальных угроз безопасности информации и разработка модели угроз, либо привлечение на договорной основе сторонних организаций для таких работ.
   3. Периодический пересмотр актуальных угроз безопасности информации в следующих случаях:

* ежегодный плановый пересмотр актуальных угроз безопасности информации;
* появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ГИС;
* существенное изменение условий функционирования ГИС, внедрение новых технологий;
* изменение нормативной документации, касающейся моделирования угроз безопасности информации;
* в результате инцидента безопасности.
  1. Разработка проектной документации на систему защиты информации в ГИС (Техническое задание, Технический проект), либо привлечение на договорной основе сторонних организаций для таких работ.
  2. Участие в реализации проекта по защите информации в ГИС.
  3. Выработка предложений главе администрации Крыловского сельского поселения по совершенствованию системы защиты информации в ГИС.
  4. Ведение учета применяемых в ГИС средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.
  5. Знание состава, структуры, назначения и выполняемых задач ГИС, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн и иной конфиденциальной информации.
  6. Обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде.
  7. Разработка плана мероприятий по обеспечению безопасности защищаемой информации в ГИС и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ГИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.
  8. Осуществление контроля неизменности состояния аттестованной ГИС (расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети). В случае планирования изменения условий функционирования ГИС, Администратор должен связаться с аттестующим органом и получить указания к дальнейшим действиям.
  9. Осуществление контроля физической сохранности и целостности технических средств ГИС, а также контроль сохранности и целостности опечатывающих пломб на технических средствах ГИС (в том числе и программно-аппаратных средствах защиты информации). Контроль неизменности состава технических средств в ГИС.
  10. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей.
  11. Организация учета иных машинных носителей информации.
  12. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ГИС (далее – Пользователи ГИС), по темам: правила работы в ГИС, защита информации в ГИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников администрации Крыловского сельского поселения в вопросах информационной безопасности.
  13. Организация первоначального доступа пользователям ГИС к ресурсам информационный системы в соответствии с утвержденным положением о разграничении прав доступа в ГИС. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ГИС в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ГИС, утвержденной в администрации Крыловского сельского поселения.
  14. Периодическое тестирование функций системы защиты от НСД согласно плану мероприятий по обеспечению безопасности информации, либо при изменении программной среды или полномочий Пользователей ГИС.
  15. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.
  16. Контроль выполнения Пользователями ГИС требований Инструкции пользователя ГИС, а также других установленных требований для обеспечения безопасности ПДн и иной конфиденциальной информации.
  17. В случае получения от Пользователей ГИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности ПДн и иной конфиденциальной информации в пределах своих полномочий.
  18. Обеспечение отсутствия на АРМ Пользователей ГИС средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, AdobeFlash, макросы MSOffice и т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.22. Выявление уязвимостей ГИС посредством периодического сканирования системы сертифицированным сканером безопасности. Принятие решений на основании итогов каждого сканирования.

2.23Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях).

* 1. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ГИС, или настройку/установку программного обеспечения ГИС.
  2. Обеспечение функционирования и поддержания работоспособности в ГИС:
* системы защиты информации от несанкционированного доступа;
* системы межсетевого экранирования;
* системы криптографической защиты информации;
* системы антивирусной защиты.
  1. Обеспечение непрерывности процессов в ГИС. В случае нарушения работоспособности технических средств и программного обеспечения ГИС, в том числе средств защиты ГИС, Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.
  2. Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ГИС.

1. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС

Администратор имеет право:

* 1. Знакомиться с нормативными актами администрации Крыловского сельского поселения, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.
  2. Вносить предложения главы администрации Крыловского сельского поселения по совершенствованию существующей системы защиты информации.
  3. Требовать от Пользователей ГИС соблюдения требований Инструкции пользователя ГИС и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн и иной конфиденциальной информации.
  4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн и иной конфиденциальной информации.
  5. Требовать прекращения работы в ГИС, как в целом, так и отдельных Пользователей ГИС, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ГИС.
  6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

1. РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ
   1. Одним из ключевых элементов системы защиты информации в ГИС является АРМ Администратора.
   2. АРМ Администратора устанавливается таким образом, чтобы исключался как преднамеренный, так и непреднамеренный несанкционированный доступ к техническим средствам АРМ Администратора.
   3. На АРМ Администратора устанавливаются средства централизованного управления: антивирусной защитой ГИС, средством защиты информации от несанкционированного доступа в ГИС. Также на АРМ Администратора устанавливается сканер уязвимостей.
   4. Администратор осуществляет централизованное управление политиками безопасности в ГИС, обновлениями средств защиты информации, обновлениями антивирусных баз и сигнатур, конфигурацией информационной системы. Также Администратор централизованно осуществляет периодическое сканирование уязвимостей ГИС.
   5. Администратор изучает журналы безопасности средств защиты информации на предмет выявления инцидентов безопасности.
   6. Рабочее место администратора является объектом защиты и защищается согласно требованиям к тому же классу, по которому классифицирована ГИС в целом.
2. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦАНИРОВАННОГО ДОСТУПА Dallaslock 8.0
   1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД) в ГИС и осуществляет управление и мониторинг этого средства.
   2. Администратор производит настройку подсистемы регистрации, идентификации и аутентификации в СЗИ от НСД Dallaslock 8.0 согласно утвержденному Положению о разграничении доступа. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.
   3. Технические средства (мобильные и стационарные) также проходят идентификацию и аутентификацию в ГИС. Идентификация и аутентификация устройств производится посредством информационного обмена по специализированным сетевым протоколам (ARP, SNMP, NetBIOS и др.). В качестве идентификаторов устройств могут выступать: логические имена, идентификационные номера, IP-адреса, MAC-адреса или комбинация этих параметров. Администратор определяет правила идентификации и аутентификации устройств в ГИС, конфигурирует протоколы и настраивает в средствах защиты информации соответствующие правила. Администратор принимает меры для предупреждения таких атак на ГИС как MAC-flooding, MAC-spoofing, ARP-spoofing, ARP-poisoning и других.
   4. Администратор осуществляет учет машинных носителей информации, как стационарных (жесткие диски АРМ и серверов, SSD-накопители и т. д.), так и съемных (флеш-накопители, съемные жесткие диски, карты памяти, память мобильных устройств и т. д.). Каждому носителю присваивается идентификационный номер. Для стационарных машинных носителей информации фиксируется местонахождение носителя (АРМ, кабинет), в случае замены или утилизации стационарного или съемного машинного носителя принимаются меры по гарантированному уничтожению информации на носителе или самого носителя с соответствующей пометкой в Журнале учета машинных носителей информации. Съемные машинные носители информации выдаются пользователем под роспись в Журнале учета машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале. Администратор средствами СЗИ от НСД Dallaslock 8.0 реализует запрет использования неучтенных машинных носителей в ГИС.
   5. Администратор осуществляет управление учетными записями с помощью встроенных механизмов ОС и с помощью механизмов СЗИ от НСД Dallaslock 8.0. В процессе управления учетными записями Администратор производит следующие действия:

* определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная учетная запись, учетная запись приложения, гостевая учетная запись, временная учетная запись и т. д.);
* объединение учетных записей в группы (при необходимости);
* проводит верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
* проводит анализ необходимости тех или иных полномочий в системе для учетных записей служб и приложений;
* производит заведение, активацию, блокирование и уничтожение учетных записей пользователей;
* проводит пересмотр и, при необходимости, корректировку учетных записей пользователей либо в процессе периодического мероприятия, либо в связи с изменением должностных обязанностей того или иного пользователя;
* уничтожает временные учетные записи пользователей, предоставленные для однократного (или ограниченного по времени) выполнения задач в ГИС, и учетные записи уволенных сотрудников;
* осуществляет настройку прав доступа пользователей к ресурсам ГИС средствами СЗИ от НСД Dallaslock 8.0 в соответствии с утвержденным Положением о разграничении доступа;
* средствами СЗИ от НСД Dallaslock 8.0 настраивает автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 90 дней.
  1. Администратор запрещает средствами СЗИ от НСД Dallaslock 8.0 любые действия пользователя в ГИС до прохождения процедур идентификации и аутентификации, в том числе ограничивает доступ к настройкам BIOS/UEFI. Администратору информационной безопасности до идентификации и аутентификации разрешаются следующие действия с целью диагностики проблем на элементах ГИС и восстановления работоспособности элементов ГИС:
* загрузка операционной системы в безопасном режиме;
* восстановление операционной системы с последней работоспособной конфигурацией;
* изменение параметров BIOS/UEFI;
* загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.
  1. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (учетных записей, первичных паролей). Администратор с помощью механизмов СЗИ от НСД Dallaslock 8.0 определяет парольную политику и требования к сложности паролей. Администратор выдает пользователю пароль для первоначального входа в ГИС. СЗИ от НСД требует от пользователя сменить пароль при первом же входе в систему. Плановая смена пароля производится пользователем самостоятельно. Смена пароля Администратором допускается в случаях компрометации пароля пользователя или при подозрении на его компрометацию, в этом случае система также должна запросить смену пароля пользователем при первом входе в ГИС после смены пароля Администратором. Администратор не должен и не обязан знать пароли пользователей ГИС. В ГИС средствами СЗИ от НСД Dallaslock 8.0 устанавливаются следующие требования к паролям:
* минимальная длина пароля составляет 6 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;
* при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;
* максимальное время действия пароля – 90 дней;
* минимальное время действия пароля – 10 дней;
* запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;
* при восьми неудачных попытках входа учетная запись блокируется не менее, чем на 10 минут.
  1. Администратор с помощью механизмов СЗИ от НСД Dallaslock 8.0 устанавливает временной промежуток в 15 минут в качестве допустимого времени бездействия пользователя. После истечения указанного времени происходит блокировка сеанса пользователя.
  2. Администратор средствами СЗИ от НСД Dallaslock 8.0запрещает пользователям самостоятельную установку любого программного обеспечения. В администрации Крыловского сельского поселения утверждается перечень разрешенного к установке в ГИС программного обеспечения. Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых с помощью ГИС. Перечень разрешенного к установке в ГИС программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.
  3. Механизмами СЗИ от НСД Dallaslock 8.0 Администратор устанавливает правила использования интерфейсов ввода/вывода технических средств ГИС. СЗИ от НСД настраивается таким образом, чтобы пользователь ГИС получал доступ к использованию только тех интерфейсов ввода/вывода, которые необходимы ему для выполнения служебных обязанностей.

1. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ
   1. При первичной настройке сетевого оборудования, Администратор изменяет все пароли по умолчанию, установленные производителем сетевого оборудования.
   2. С помощью средств межсетевого экранирования, штатных функций операционных систем и сетевых устройств и средства мониторинга и настройки Администратор осуществляет управление информационными потоками при передаче информации между устройствами и сегментами сети. Под управлением информационными потоками понимается: фильтрация информационных потоков, разрешение передачи информации в ГИС только по определенному Администратором маршруту и изменение (перенаправление) маршрута передачи информации.
   3. Администратор осуществляет настройку сетевого оборудования или контролирует этот процесс.
   4. Администратор анализирует технологические процессы обработки информации, а также особенности функциональных обязанностей сотрудников администрации Крыловского сельского поселения для оптимизации настроек средств межсетевого экранирования. Средство межсетевого экранирования настраивается по принципу разрешения только тех ресурсов, сетевых портов и протоколов, необходимых для нормального функционирования ГИС и администрации Крыловского сельского поселения в целом.
   5. Администратор организует взаимодействие с информационными системами сторонних организаций.
   6. Администратор обеспечивает защиту информации, передаваемой по недоверенным каналам связи за пределы контролируемой зоны, с помощью криптографических средств.
   7. Администратор осуществляет настройку и контроль функционирования специальных средств, осуществляющих фильтрацию и контроль входящих нежелательных электронных писем (спама). При этом, учитывая возможность ложного срабатывания такой системы, пользователь должен иметь возможность просмотра отфильтрованных сообщений. Администратор инструктирует пользователей о возможных типах мошенничества с использованием электронной почты (социальная инженерия, фишинг и прочее).
2. ОБСЛУЖИВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
   1. Общие правила работы с криптосредствами описаны в утвержденной Инструкции по обеспечению безопасности эксплуатации СКЗИ. В данном разделе описана часть, касающаяся функций и обязанностей Администратора.
   2. Исходя из требований к защите информации и актуальных угроз безопасности информации в ГИС, Администратор определяет необходимость использования средств криптографической защиты информации (далее – СКЗИ) в системе защиты информации ГИС.
   3. Администратор обеспечивает соответствие работы с СКЗИ технической и эксплуатационной документации к ним.
   4. Администратор осуществляет поэкземплярный учет СКЗИ, технической и эксплуатационной документации к ним в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ГИС.
   5. Администратор контролирует передачу СКЗИ, ключевой информации, технической и эксплуатационной документации пользователям ГИС. Факт передачи отражается в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ГИС.
   6. Администратор обеспечивает хранение дистрибутивов СКЗИ, эксплуатационную и техническую документацию к ним, ключевую информацию в шкафах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
   7. Администратор обеспечивает раздельное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.
   8. Администратор производит инструктаж пользователей перед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в ГИС.
   9. Администратор составляет и поддерживает в актуальном состоянии список лиц, допущенных к работе с СКЗИ.
   10. Администратор осуществляет проверку готовности СКЗИ к использованию в ходе проведения проверок согласно Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ГИС. Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в ГИС. Результат проверки отражается в Журнале периодического тестирования средств защиты информации в ГИС. Проверка каждого СКЗИ проводится не реже одного раза в месяц.
   11. Администратор инструктирует пользователей о порядке хранения ключевой информации и осуществляет контроль соблюдения пользователями правил хранения такой информации.
   12. Администратор принимает участие в составе группы реагирования на инциденты информационной безопасности в расследовании случаев попыток посторонних лиц получить сведения об используемых СКЗИ, случаев компрометации или при подозрении на компрометацию ключевой информации, случаев утраты дистрибутивов СКЗИ, ключевой информации, ключевых носителей, технической и эксплуатационной документации к СКЗИ, ключей от помещений и хранилищ СКЗИ. В случае компрометации ключевой информации, Администратор немедленно выводит ее из эксплуатации.
   13. Администратор в составе комиссии по уничтожению принимает участие в уничтожении ключевой информации и ключевых документов. Уничтожение ключевой информации производится путем физического уничтожения ключевого носителя или путем гарантированного затирания ключевой информации.
3. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ
   1. Администратор осуществляет настройку и контроль функционирования системы антивирусной защиты в ГИС. Управление системой осуществляет только Администратор. Антивирусная защита осуществляется на АРМ, серверах, мобильных технических средствах и иных точках доступа в ГИС.
   2. Администратор настраивает время, периодичность и другие параметры проведения полной антивирусной проверки узлов ГИС на наличие вредоносных компьютерных программ (вирусов) согласно "Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в сегменте РИСОГД Приморского края". Факт проверки отражается в "Журнале по учету мероприятий по контролю обеспечения защиты информации сегменте государственной информационной системы Приморского края "Региональная информационная система обеспечения Градостроительной деятельности Приморского края".
   3. Администратор самостоятельно или в составе группы реагирования на инциденты информационной безопасности (в случае значительного инцидента безопасности) реагирует на сообщения системы антивирусной защиты или пользователей об обнаружении вредоносных компьютерных программ (вирусов), или на подозрение наличия таковых, и принимает меры по нейтрализации обнаруженных угроз.
   4. Администратор настраивает периодичность обновления баз и сигнатур антивирусного средства. Администратор также настраивает механизм распространения обновленных антивирусных баз на все узлы ГИС. Обновление антивирусных баз и сигнатур проводится ежедневно.
4. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ
   1. Под системой регистрации и учета событий безопасности в ГИС понимается совокупность средств централизованного управления всех СЗИ в ГИС.
   2. Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе, являются объектами защиты. Администратор принимает меры по защите этой информации в соответствии с техническим заданием на систему защиты информации системы защиты информации. Доступ к записям системы регистрации и учета событий безопасности разрешен только Администратору.
   3. Администратор периодически изучает записи системы регистрации и учета событий безопасности и в случае обнаружения инцидентов безопасности информации созывает группу реагирования на инциденты информационной безопасности, которая в свою очередь действует согласно соответствующим инструкциям.
5. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ
   1. Для выявления уязвимостей в информационной системе используется сетевой сканер Canon i-SENSYS MF4018.
   2. Сканирование ГИС на наличие уязвимостей проводится с периодичностью, необходимой и достаточной для должной обработки отчета по результатам сканирования и принятия мер по устранению выявленных уязвимостей, но не реже одного раза в квартал.
   3. В случае проведения сканирований, для которых необходимо предоставить сканеру безопасности учетные данные в системе, создается отдельная учетная запись с минимально необходимыми правами. Вводить данные уже существующей учетной записи в сканер безопасности категорически запрещено.
   4. В случае получения информации о новых уязвимостях, связанных с информационной системой, из открытых источников необходимо провести обновление базы данных об уязвимостях и провести внеплановое сканирование.
   5. Администратор принимает меры по устранению или нейтрализации выявленных уязвимостей. В первую очередь обрабатываются уязвимости с наивысшим баллом по шкале CVSS. В случае необходимости, до устранения уязвимости могут быть локализованы (отключены от общей сети) сегменты или отдельные АРМы информационной системы.
   6. С целью оперативного устранения известных уязвимостей на серверах и АРМ информационной системы настраивается обновление в автоматическом режиме компонентов операционных систем, прикладного программного обеспечения и средств защиты информации.
   7. Администратор не реже чем один раз в месяц осуществляет контроль состава технических средств, программного обеспечения и средств защиты информации, а также корректности функционирования и настроек программного обеспечения и средств защиты информации.
6. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПРИ РЕМОНТЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБСЛУЖИВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УТИЛИЗАЦИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ
   1. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в ГИС (в том числе и средств защиты информации) сотрудниками сторонних организаций.
   2. Администратор присутствует в процессе ремонта технических средств ГИС сотрудниками сторонних организаций на территории администрации Крыловского сельского поселения. Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.
   3. Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.

УТВЕРЖДЕНА

распоряжением администрации Крыловского сельского поселения

от 17 июля 2024г. № 21-од

**Инструкция ответственного за организацию обработки персональных данных в администрации Крыловского сельского поселения**

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Ответственный за организацию обработки персональных данных в администрации Крыловского сельского поселения (далее – Ответственный) назначается распоряжением главы администрации Крыловского сельского поселения (далее – Администрация) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Администрации законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.
   2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн. Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.
   3. В своей деятельности Ответственный руководствуется Положением об обработке и защите персональных данных, настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.
2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
   1. Ответственный изучает все стороны деятельности Администрации и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

* организация доступа к ПДн и учет сотрудников Администрации, допущенных к обработке ПДн, как в программных комплексах, входящих в состав ИС, так и на бумажных носителях;
* контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
* контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
* организация работы по заключению договоров на работы по защите ПДн;
* контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления администрации Крыловского сельского поселения в реестре операторов ПДн;
* рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, назначаемым распоряжением главы администрации Крыловского сельского поселения;
* осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Администрации.

1. ОСНОВНЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
   1. Знать цели обработки ПДн в Администрации и перечень обрабатываемых ПДн.
   2. Соблюдать требования нормативных актов Администрации, устанавливающих порядок работы с ПДн.
   3. Обеспечивать доведение до сведения сотрудников Администрации законодательства Российской Федерации о ПДн, нормативных актов по вопросам обработки ПДн, требований к защите ПДн.
   4. Осуществлять внутренний контроль за соблюдением сотрудниками Администрации законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.
   5. Контролировать ведение документации, предусмотренной нормативными актами Администрации в части обеспечения безопасности ПДн.
   6. Обеспечивать доработку локальных нормативных документов по защите ПДн Администрации в случае такой необходимости или при поступлении такого требования от регулирующего органа.
   7. Участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.
   8. Обеспечивать организацию проведения занятий со специалистами Администрации по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Администрации).
   9. Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п.3 ч.4 ст.22.1 [Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) "О персональных данных"](https://www.consultant.ru/document/cons_doc_LAW_61801/).
2. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
   1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных на него задач.
   2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в подразделениях Администрации в соответствии с утвержденным распоряжением главы администрации Крыловского сельского поселения планом мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ИС.
   3. Требовать от сотрудников Администрации соблюдения требований нормативно-правовых и организационно-распорядительных документов по вопросам обработки ПДн.
   4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн.
   5. Требовать от сотрудников Администрации письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн.
   6. Вносить предложения главе администрации Крыловского сельского поселения об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.
   7. Давать сотрудникам Администрации обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными нормативными актами Администрации Крыловского сельского поселения.
   8. Привлекать в установленном порядке специалистов Администрации, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.