

ТЫВА РЕСПУБЛИКАНЫҢ ЧϴϴН-ХЕМЧИК КОЖУУН

МУНИЦИПАЛДЫГ РАЙОННУҢ ЧАГЫРГАЗЫ

**АЙТЫЫШКЫН**

АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО РАЙОНА

ДЗУН-ХЕМЧИКСКИЙ КОЖУУН РЕСПУБЛИКИ ТЫВА

**РАСПОРЯЖЕНИЕ**

«\_\_» \_\_\_\_\_\_\_ 2021г. г. Чадан № \_\_\_

**О внесении изменений в распоряжение**

**администрации Дзун-Хемчикского кожууна Республики Тыва**

**от 21 января 2021 г. №22-р**

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012   
№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

**РАСПОРЯЖАЮСЬ:**

1. Изменить пункт 1.1 в распоряжение администрации Дзун-Хемчикского кожууна Республики Тыва от 21 января 2021 г. №22-р «О защите информации» следующего содержания:

«1.1. Назначить ответственным за организацию обработки персональных данных:

-Монгуш Тайгану Мергеновну – И. о. руководителя аппарата- управляющего делами.»

2. Изменить пункт 3.4 в распоряжение администрации Дзун-Хемчикского кожууна Республики Тыва от 21 января 2021 г. №22-р «О защите информации» следующего содержания:

«3.4. Журналы по защите информации согласно приложению 9, приложение 40, приложение 44, приложение 45, приложение 46, приложение 47 к настоящему распоряжению.»

3. Дополнить пункт 3 в распоряжение администрации Дзун-Хемчикского кожууна Республики Тыва от 21 января 2021 г. №22-р «О защите информации» следующего содержания:

«

3.8.Перечень объектов защиты информационных системах администрации Дзун-Хемчикского кожууна (приложение 30);

3.9. Описание технологического процесса обработки информации в государственной информационной системе «Локальная вычислительная сеть администрации Дзун-Хемчикского кожууна Республики Тыва (приложение 31);

3.10. Положение об обеспечении мер защиты информации в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад администрации Дзун-Хемчикского кожууна (приложение 32);

3.11. Положение о разграничении прав доступа к информации, обрабатываемой в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад администрации Дзун-Хемчикского кожууна (приложение 34);

3.12. ПОЛОЖЕНИЕ об использовании сети Интернет в автоматизированном рабочем месте государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад администрации Дзун-Хемчикского кожууна (приложение 37);

3.13. Границы контролируемой зоны (приложение 41);

3.14. Список должностей, лиц, допущенных (имеющих доступ) в помещения Администрации Дзун-Хемчикского кожууна, в которых ведется обработка конфиденциальной информации (приложение 42);

3.15. Матрица доступа к сведениям конфиденциального характера, обрабатываемым в администрации Дзун-Хемчикского кожууна (приложение 48);

»

4. Дополнить пункт 5 в распоряжение администрации Дзун-Хемчикского кожууна Республики Тыва от 21 января 2021 г. №22-р «О защите информации» следующего содержания:

«

Утвердить инструкции и правила по защите информации:

- Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация, ФСС (личный кабинет), Технокад (приложение 33);

- Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения в государственной информационной системах администрации Дзун-Хемчикского кожууна (приложение 35);

- ИНСТРУКЦИЯ по модификации и техническому обслуживанию программного обеспечения и аппаратных средств государственной информационных системах

администрации Дзун-Хемчикского кожууна (приложение 36);

- ПОРЯДОК действий при обнаружении отказов функционирования технических средств государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад (приложение 38);

- Регламент порядка проведения проверок состояния защиты государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад администрации Дзун-Хемчикского кожууна (приложение 39);

- Правила доступа в помещения администрации Дзун-Хемчикского кожууна в рабочее и нерабочее время, а также в нештатных ситуациях (приложение 43);

- ИНСТРУКЦИЯ администратора безопасности информации (приложение 49);

»

**Председатель Администрации**

**Дзун-Хемчикского кожууна** **Тюлюш А.Ч.**

**Приложение 30**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**ПЕРЕЧЕНЬ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМАХ АДМИНИСТРАЦИИ ДЗУН-ХЕМЧИКСКОГО КОЖУУНА**

1. Информация, содержащаяся в информационной системе;
2. 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);
3. Общесистемное ПО;
4. Прикладное ПО;
5. Специальное ПО;
6. Информационные технологии;
7. Средства защиты информации.

**Приложение 31**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ АДМИНИСТРАЦИИ ДЗУН-ХЕМЧИКСКОГО КОЖУУНА РЕСПУБЛИКИ ТЫВА»**

2021 г.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

***Информационная система (ИС)*** -система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

***Автоматизированное рабочее место (АРМ)***- программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

***Администратор ИС*** - лицо, ответственное за функционирование информационной системы в установленном штатном режиме работы.

***Администратор безопасности информации*** - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

***Конфиденциальная информация*** -информация, доступ к которой ограничен федеральными законами или, в случаях допускаемым Законодательством Российской Федерации, ее обладателем (информация ограниченного доступа).

***Машинные носители информации*** ­- магнитные, оптические и сменные носители информации, предназначенные для записи и считывания информации, используемые в средствах вычислительной техники (съемные и несъемные).

***Обработка информации* -** совокупность операций сбора, накопления, [ввода](javascript:void(17031)), [вывода](javascript:void(17032)), приема, [передачи](javascript:void(22510)), записи, [хранения](javascript:void(21055)), регистрации, уничтожения, [преобразования](javascript:void(26258)), отображения [информации](javascript:void(20458)).

***Резервное копирование*** - процесс создания копии данных на носителе (flash-накопителе, жёстком диске и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

***Технологический процесс обработки информации*** - последовательность действий пользователей при работе с информацией.

***Средство защиты информации (СЗИ)*** - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

# 2. НАЗНАЧЕНИЕ ГИС «ЛВС АДМИНИСТРАЦИИ ДЗУН-ХЕМЧИКСКОГО КОЖУУНА РТ»

* 1. ГИС «ЛВС Администрации Дзун-Хемчикского кожууна РТ» предназначена для реализации полномочий администрации Дзун-Хемчикского кожууна Республики Тыва (далее –администрации Д-Х кожууна РТ), для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации Д-Х кожууна РТ, подведомственных учреждений к индивидуальным, общим или групповым информационным и техническим ресурсам сети, обеспечения коммуникаций пользователей друг с другом, обработки и хранения открытой информации и (или) информации ограниченного доступа, при наличии ЗЛВС. ГИС «ЛВС Администрации Дзун-Хемчикского кожууна РТ» может включать в себя ресурсы и предоставлять их другим лицам на основе договоров об информационном взаимодействии в соответствии с действующим законодательством.
  2. Информация конфиденциального характера, обрабатываемая в ГИС «ЛВС Администрации Дзун-Хемчикского кожууна РТ» в Организации используется при решении следующих основных задач:
* обеспечение реализации полномочий председателя администрации Дзун-Хемчикского кожууна Республики Тыва и для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации Д-Х кожууна РТ, подведомственных учреждений к индивидуальным, общим или групповым информационным и техническим ресурсам сети, обеспечения коммуникаций пользователей друг с другом, обработки и хранения открытой информации и (или) информации ограниченного доступа ;
* обеспечение реализации председателя администрации Дзун-Хемчикского кожууна Республики Тыва и для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации Д-Х кожууна РТ, подведомственных учреждений иных возложенных на него федеральным и республиканским законодательством полномочий.

1. **РАСПОЛОЖЕНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ**
   1. ГИС «ЛВС Администрации Дзун-Хемчикского кожууна РТ» расположена по адресу:

* Юридический адрес: 668111, Республика Тыва, г. Чадан, ул. Ленина, д.42;
* Фактический адрес: 668111, Республика Тыва, г. Чадан, ул. Ленина, д.42;
  1. Помещения, в которых ведется обработка информации конфиденциального характера, оборудованы техническими средствами защиты (охранная, пожарная сигнализация, система видеонаблюдения), физическая охрана помещений, организован пропускной режим на помещениях администрации Д-Х кожууна РТ, в которых осуществляется обработка конфиденциальной информации.
  2. Доступ сотрудников и других лиц в помещения администрации Д-Х кожууна РТ осуществляется в соответствии с утвержденным списком лиц, имеющих доступ в данное помещение.

# ОПИСАНИЕ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ ОБЪЕКТА

* 1. Структура администрации Д-Х кожууна РТ является иерархической. Организационная структура администрации Д-Х кожууна РТ представлена на рисунке 1.

СТРУКТУРА

Аппарата администрации муниципального района Дзун-Хемчикский кожуун Республики Тыва

Председатель администрации – 1 м.сл.

Руководитель аппарата – управ. делами 1 м.сл,.

Первый заместитель председателя по безопасности, профилактике правонарушений и взаимодействии с правоохранительными органами -1 м.сл.

Начальник отдела (главный бухгалтер) – 1 м.сл.

Специалисты - 6 Не отн.

Консультант – 1 м.сл (по док.обеспечению)

Главный специалист -1 м.сл. (орг.обесп и ОМСУ)

Консультант по внутр. финанс контролю -1 м сл

Спец. по обращ.граждан и соц.сетью– 1 Не отн

Отдел правового и кадрового обеспечения -3 ед.:

Начальник отдела -1 м.сл,

гл. специалист - 1 м.сл(архив)

гл. специалист – 1 Не отн(кадр),

Заместитель председателя по экономике– 1 м.сл.

Заместитель председателя по социальной политике и взаимодействии с общественными организациями-1 м.сл

Заместитель председателя по жизнеобеспечению и развитию инфраструктуры -1 м.сл

(Бухгалтер-1 Не отн, водитель -1 МОП)

Начальник отдела -3 м.сл.

Консультант - 4 м.сл.

Заместитель председателя-начальник финансового управления -1 м.сл.

Начальник отдела экономики -1 м..сл.

Консультант по тендерным торгам и прогр.обесп. - 1 м.сл

Спец. по проектному управлению-1 (Не отн)

Гл. специалист по развитию предпринимат. и туризма -1 Не отн

Начальник отдела ГО и ЧС – 1 м сл,

Старший ЕДДС -1 Не отн

Диспетчер-3 Не отн

Начальник управления культуры –

1 м.сл.

Начальник управления образования – 1 м.сл.

Ответственный секретарь административной комиссии -1м сл.

Ответственный секретарь

КДН и ЗП – 1 Не отн

ия кул

Начальник управления УТ и СР -1 м.сл.

Инженер-1 Не отн

Начальник отдела УМИ и ЗО - 1м.сл.

Специалист по земельному контролю -1 м.сл.

Консульт.по архит и стр-1м.сл

Консультант по молодежной политике и спорту – 1 м.сл.

Консультант- 1м.сл.

Ведущий специалист- 1 м.сл. +1 (Не отн)

Консультант -1 м.сл Главный специалист -1(не отн.)

+

+1

Отдел административно-хозяйственного обеспечения -10 ед.:

Начальник отдела АХО – 1 ед. Не отн.

МОП-6 ед. +МОП техн-3 ед.

Начальник отдела-2 м.сл.

Главный специалист по делам семьи, материнства и детства-1 м.сл.

Водитель - 1 МОП

Консультант - 3 м.сл

Начальник управления сельского хозяйства -1 м.сл

Мун. службы – 41ед.

Не относящиеся к мун. службе –20 ед.

Младший обслуживающий персонал – 11 ед.

Итого: 72 ед.

Рисунок 1. – Организационная структура администрации Д-Х кожууна РТ

1. **ПЕРЕЧЕНЬ ПОДСИСТЕМ ГИС «ЛВС АДМИНИСТРАЦИИ ДЗУН-ХЕМЧИКСКОГО КОЖУУНА РТ»**

Перечень подсистем государственной информационной системы «Локальная вычислительная сеть администрации Д-Х кожууна РТ» представлен в таблице 1.

Таблица 1. – Перечень подсистем ГИС «ЛВС администрации Д-Х кожууна РТ»

| **№**  **п/п** | **Наименование подсистемы**  **государственной информационной системы** | **Категория обрабатываемой информации** |
| --- | --- | --- |
| **1** | **2** | **3** |
|  | Информационная система «Кадры» | Персональные данные |
|  | Информационная система «Бухгалтерия» | Персональные данные |
|  | Информационная система «Обращения граждан» | Персональные данные |
|  | Система электронного документооборота "Практика" | Служебная информация |
|  | Система удаленного финансового документооборота(Далее – СУФД) | Персональные данные |
|  | Единый портал бюджетной системы | Персональные данные |
|  | Госуда́рственная информацио́нная систе́ма о госуда́рственных и муниципа́льных платежа́х (далее - ГИС ГМП) | Персональные данные |
|  | Программа Spu\_orb Пенсионного Фонда РФ. | Персональные данные |
|  | Налогоплательщик ЮЛ | Персональные данные |
|  | Контур-Экстерн | Персональные данные |
|  | Web-консолидация | Служебная информация |
|  | Фонд социального страхования российской федерации | Персональные данные |
|  | Технокад | Персональные данные |

**7. Характеристика основных информационных потоков**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Передаваемые данные, входной формат данных** | **Откуда поступают данные** | **Где (в какой СУБД) хранятся поступившие данные** | **Формат хранения данных** | **Чем и как обрабатываются данные, выходной формат данных** | **Куда передаются обработанные данные** | **Шифрование передаваемых данных (Да/Нет)** | | | **Использование электронной подписи** | **Использование ViPNet** |
| **Канальное шифрование** | **Шифрование файлов (сообщений)** | |
| 1. **Обмен с пенсионным фондом** | | | | | | | | | | |
| xml | Пенсионный фонд | Spu\_orb | xml | Клон | ФСС | Нет | | Да | Да | Да |
| 1. **Обмен с Федеральным казначейством** | | | | | | | | | | |
|  | Федеральное казначейство | 1С: Бухгалтерия, СУФД, ГИС ГМП |  | Клиент приема-передачи Сбербанка | Сбербанк | Да | | Да | Да | Да |
|  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |

**8. Ввод, хранение, обработка и вывод информации**

Ввод конфиденциальной информации осуществляется следующим образом:

– информация вводится пользователями подсистем ГИС «ЛВС администрации Д-Х кожууна РТ» своими силами.

Ввод конфиденциальной информации в подсистем ГИС «ЛВС администрации Д-Х кожууна РТ» с внешних машинных носителей (flash-накопителей, жестких дисков и т. д.) технологическим процессом не предусмотрен.

Ввод конфиденциальной информации в подсистем ГИС «ЛВС администрации Д-Х кожууна РТ» с использованием внешних устройств типа сканеров и т. п. не предусмотрен.

На учтенном внешнем flash-накопителе («T\_\_\_\_\_\_\_\_», сер. № \_\_\_\_\_\_) хранятся файлы резервных копий.

Вывод конфиденциальной информации в ИС осуществляется на бумажные носители с использованием многофункционального устройства/принтера «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_».

Вывод конфиденциальной информации на любые внешние машинные носители запрещен.

**9. Управление доступом**

Управление доступом пользователей подсистем ГИС «ЛВС администрации Д-Х кожууна РТ» к ресурсам выполняется только администратором подсистем ГИС «ЛВС администрации Д-Х кожууна РТ».

Каждый пользователь подсистем ГИС «ЛВС администрации Д-Х кожууна РТ» имеет свою учетную запись, вход в которую осуществляется с помощью персональных логина и пароля или персонального ключа-идентификатора eToken.

При помощи средств защиты информации от несанкционированного доступа установлен запрет на подключение пользователями внешних устройств, кроме администратора. Администратор АС имеет право подключать к ИС учтенный flash-накопитель («\_\_\_\_\_\_\_», сер. № \_\_\_\_\_\_\_\_\_\_).

**10. Резервирование**

Под резервированием понимается служебная процедура, при которой информация переносится (копируется) на внешний машинный носитель. При этом данный машинный носитель не используется для передачи конфиденциальной информации за пределы Организации.

Резервная копия создается для восстановления информации на случай сбоя системы или иных ситуаций, при которых доступ к жесткому диску в составе СВТ, невозможен.

Резервное копирование информации производится в ручную один раз в неделю администратором ИС. Резервная копия добавляется в архив с использованием файлового архиватора «7-Rar», затем помещается на учтенный flash-накопитель («\_\_\_\_\_\_\_», сер. № \_\_\_\_\_\_\_), который хранится в сейфе, инв. № \_\_\_\_\_, офис № \_\_\_, ул. Ленина , 42.

**11. Обновление программного обеспечения**

Под обновлением программного обеспечения понимается установка новых версий программного обеспечения по причине исправления ошибок в старых версиях программ или совершенствования функционала ПО.

Периодичность обновления программного обеспечения зависит от выпуска новой версии ПО его производителем. Обновление антивирусных баз осуществляется раз в неделю.

Обновление программного обеспечения ИС осуществляется только администратором ИС с использованием учтенного flash-накопителя («\_\_\_\_\_\_», сер. № \_\_\_\_\_\_\_), который хранится в сейфе, инв. № \_\_\_\_\_\_\_\_\_\_, офис № \_\_\_\_\_, ул. Ленина, 42, и регламентируется в организационно-распорядительной документации Организации.

**12. Устранение сбоев**

Под сбоями в работе ИС понимаются любые нарушения работоспособности каких-либо аппаратных или программных средств ИС, которые приводят к частичной или полной недоступности информации или снижению уровня ее защищенности.

Устранение сбоев осуществляется администратором ИС. При необходимости производится восстановление информации с резервных копий.

**Приложение 32**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**Положение об обеспечении мер защиты информации в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад администрации Дзун-Хемчикского кожууна**

Настоящее Положение определяет содержание и правила реализации организационных и технических мер защиты информации, применяемых в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад (Далее – Программы) администрации Дзун-Хемчикского кожууна в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

В соответствии с актом классификации № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_ г. для Программ \_\_\_\_\_ класс защищенности (\_\_\_).

1. **Идентификация и аутентификация субъектов доступа и объектов доступа**

1.1 В Программах должна обеспечиваться идентификация и аутентификация пользователей, выполняющих свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ГИС в соответствии с должностными регламентами (инструкциями), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

1.2 Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа.

1.3 Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств.

1.4 В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

1.5 Идентификация устройств в информационной системе обеспечивается:

* по логическим именам (имя устройства и (или) ID);
* логическим адресам (например, IP-адресам);
* и (или) по физическим адресам (например, МАС- адресам) устройства;
* или по комбинации имени, логического и (или) физического адресов устройства.
  1. Аутентификация устройств в информационной системе обеспечивается с использованием:
* соответствующих протоколов аутентификации;
* с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.
  1. В Программах установлены и реализованы следующие функции управления идентификаторами пользователей и устройств:
* определение должностного лица (администратора), ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
* формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
* присвоение идентификатора пользователю и (или) устройству;
* исключение повторного использования идентификатора пользователя в течение: не менее одного года;
* блокирование идентификатора пользователя через период времени неиспользования: не более 90 дней.

1. **Защита машинных носителей информации**

2.1 В Программах учету подлежат:

* съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
* портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
* машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

2.2 Носителям присваиваются регистрационные (учетные) номера. В качестве регистрационных номеров используются:

* идентификационные (серийные) номера машинных носителей, присвоенные производителями этих машинных носителей информации;
* номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации;
* иные номера.

2.3 Учет съемных машинных носителей информации ведется в журнале учета машинных носителей информации.

2.4 Учет встроенных в портативные или стационарные технические средства машинных носителей информации ведется в журналах материально- технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, присваивается регистрационный номер техническому средству в целом.

2.5 Регистрационные или иные номера подлежат занесению в журнал учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

2.6 Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш- накопители, съемные жесткие диски).

2.7 Обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая информацию о возможности использования машинного носителя информации вне информационной системы.

2.8 Физический доступ к машинным носителям предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

2.9 В ГИС осуществляется контроль использования интерфейсов ввода (вывода) путем определения интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации.

2.10 В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), применяются:

* опечатывание интерфейсов ввода (вывода);
* использование механических запирающих устройств;
* удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);
* применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

2.11 При передаче машинных носителей между пользователями, в сторонние организации для ремонта и утилизации обеспечивается уничтожение (стирание) информации, исключающее возможность восстановления защищаемой информации путем очистки всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

2.12 В Программах обеспечивается регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации следующим образом:

– Регистрация действий пользователя(введение системных журналов).

- Ограничение прав, доступа на удаление объектов.

- Установка фильтров ограничивающих действий пользователя(по необходимости).

1. **Регистрация событий безопасности**

3.1 В Программах подлежат регистрации следующие события безопасности:

– при регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы: дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

* при регистрации подключения машинных носителей информации и вывода информации на носители информации: дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации;
* при регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации: дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);
* при регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам: дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип);
* при регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей): дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого объекта доступа (логическое имя (номер);
* при регистрации попыток удаленного доступа к информационной системе: дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе;
* события, связанные с изменением привилегий учетных записей.

3.2 Пересмотр перечня событий безопасности, подлежащих регистрации, осуществляется не менее чем один раз в год и по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

3.3 Срок хранения информации о зарегистрированных событиях безопасности составляет не менее трех месяцев, при этом осуществляется хранение только записей о выявленных событиях безопасности.

3.4 В информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающая полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).

3.5 Объем памяти для хранения информации о событиях безопасности рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

3.6 В информационной системе обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

3.7 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти предусматривает:

* предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
* реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

3.8 В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

3.9 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

3.10 В информационной системе обеспечивается резервное копирование записей регистрации (аудита).

3.11 Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам.

3.12 Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

1. **Обнаружение вторжений**

4.1 Обеспечение обнаружения (предотвращения) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, осуществляется с использованием систем обнаружения вторжений.

4.2 Применяемая система обнаружения вторжений включает компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

4.3 Обнаружение (предотвращение) вторжений осуществляется на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах).

4.4 Права по управлению (администрированию) системами обнаружения вторжений предоставляются только уполномоченным должностным лицам.

4.5 В информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.

4.6 Обновление базы решающих правил системы обнаружения вторжений предусматривает:

* получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;
* получение из доверенных источников и установку обновлений базы решающих правил;
* контроль целостности обновлений базы решающих правил.

4.7 В информационной системе обеспечивается возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов).

1. **Контроль (анализ) защищенности информации**

5.1 При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

* выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
* разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
* анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
* устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
* информирование должностных лиц (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

5.2 В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

5.3 В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

5.4 Для выявления (поиска) уязвимостей используется средство анализа (контроля) защищенности (сканер безопасности), имеющий стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно- аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

5.5 Уточнение перечня сканируемых в информационной системе уязвимостей с происходит с периодичностью: …, а также после появления информации о новых уязвимостях.

5.6 Доступ к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности) предоставляется только администраторам.

5.7 Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода проводится с периодичностью: … и фиксируется в соответствующих журналах.

5.8 Получение обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода, осуществляется из доверенных источников.

5.9 При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

5.10 При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

* контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
* проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
* контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
* восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

5.11 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичность: ….

5.12 В информационной системе обеспечивается регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

5.13 При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

* контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
* контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
* контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
* исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.14 Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью: ….

5.15 В информационной системе обеспечивается регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

5.16 При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

* контроль правил генерации и смены паролей пользователей;
* контроль заведения и удаления учетных записей пользователей;
* контроль реализации правил разграничения доступом;
* контроль реализации полномочий пользователей;
* контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;
* устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

5.17 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью: ….

5.18 В информационной системе обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

1. **Обеспечение целостности информационной системы и информации**

6.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, предусматривает:

* контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;
* контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;
* контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;
* тестирование с периодичностью: … функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;
* обеспечение физической защиты технических средств информационной системы.

6.2 Контроль целостности средств защиты информации осуществляется по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

6.3 Исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды.

6.4 Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

6.5 Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

* восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
* восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
* возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.
  1. Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

1. **Защита среды виртуализации**

7.1 При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре обеспечивается:

* идентификация и аутентификация администраторов управления средствами виртуализации;
* идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;
* блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
* защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;
* защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий; идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

7.2 Обеспечивается взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.

7.3 Обеспечивается управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин.

7.4 По управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре информационной системы обеспечивается:

* контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;
* контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;
* управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;
* контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил)
* разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);
* разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.

7.5 В информационной системе обеспечивается доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры;

7.6 Доступ к конфигурации виртуальных машин предоставляется только администраторам виртуальной инфраструктуры.

7.7 В виртуальной инфраструктуре дополнительно к событиям, установленным в п. 3.1 Настоящего положения, подлежат регистрации следующие события:

* запуск (завершение) работы компонентов виртуальной инфраструктуры;
* доступ субъектов доступа к компонентам виртуальной инфраструктуры;
* изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
* изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

7.8 При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

7.9 При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

7.10 При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, включают дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

7.11 При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам- образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

7.12 При управлении потоками информации между компонентами виртуальной инфраструктуры обеспечиваются:

* фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;
* обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);
* контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;
* отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети; обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;
* обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;
* семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

7.13 При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных обеспечиваются:

* регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);
* управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);
* управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации; управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

7.14 Управление перемещением виртуальных машин (контейнеров) предусматривает:

* полный запрет перемещения виртуальных машин (контейнеров);
* ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
* ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

7.15 Перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных осуществляется в пределах информационной системы только на контролируемые технические средства (сервера виртуализации, носители, системы хранения данных).

7.16 В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с гл. 6 настоящего Положения.

7.17 При контроле целостности компонентов виртуальной инфраструктуры обеспечивается:

* контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);
* контроль целостности состава и конфигурации виртуального оборудования;
* контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;
* контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

7.18 В информационной системе обеспечивается контроль целостности резервных копий виртуальных машин (контейнеров).

7.19 В информационной системе обеспечивается контроль состава аппаратной части компонентов виртуальной инфраструктуры.

7.20 В информационной системе обеспечивается резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с Инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты в ГИС 1С: Бухгалтерия.

7.21 При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры обеспечивается:

* определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;
* резервное копирование виртуальных машин (контейнеров);
* резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;
* резервирование программного обеспечения виртуальной инфраструктуры; резервирование каналов связи, используемых в виртуальной инфраструктуре;
* периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

7.22 Реализация и управление антивирусной защитой в виртуальной инфраструктуре обеспечивается в соответствии с Инструкцией по организации антивирусной защиты в Программах, при этом обеспечивается:

* проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
* проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

7.23 В информационной системе обеспечивается разграничение доступа к управлению средствами антивирусной защиты.

1. **Защита технических средств**

8.1 Оператором обеспечивается контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

8.2 Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

8.3 Границы контролируемой зоны определены в Приказе об определении границ контролируемой зоны.

8.4 Контроль и управление физическим доступом предусматривают:

* определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
* санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
* учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

8.5 Размещение устройств вывода (отображения, печати) информации исключает возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

1. **Защита информационной системы, ее средств и систем связи и передачи данных**

9.1 В информационной системе обеспечивается разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

9.2 Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

9.3 Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

9.4 В информационной системе обеспечивается выделение автоматизированных рабочих мест для администраторов безопасности.

9.5 Защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

9.6 Для исключения возможности отрицания пользователем факта отправки информации другому пользователю осуществляется:

* определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);
* обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи;
* регистрация событий, связанных с отправкой информации другому пользователю.

9.7 Для исключения возможности отрицания пользователем факта получения информации осуществляется:

* определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);
* обеспечение целостности полученной информации;
* регистрация событий, связанных с получением информации от другого пользователя.

9.8 В информационной системе обеспечивается защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

9.9 Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе.

9.10 Защита беспроводных соединений включает:

* предоставление доступа к параметрам(изменению параметров) настройки беспроводных соединений только администраторам информационной системы;
* обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);
* регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

9.11 В информационной системе осуществляется защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

* управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);
* обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

9.12 В информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

9.13 В информационной системе применяется отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса.

9.14 В информационной системе обеспечивается защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов.

9.15 В информационной системе исключается выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»).

**Приложение 33**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация, ФСС (личный кабинет),** **Технокад**

1. **Общие положения**
   1. Данные Правила регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах администрации Дзун-Хемчикского кожууна и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.
2. **Идентификация и аутентификация пользователей, являющихся внутренними пользователями**
   1. При доступе в ИС **1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация, ФСС (личный кабинет),** **Технокад(далее - Программы)** осуществляется идентификация и аутентификация пользователей, являющихся работниками администрации Дзун-Хемчикского кожууна (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица администрации Дзун-Хемчикского кожууна:

* администратор ИС;
* администратор информационной безопасности (ИБ);
* ответственные работники по работе с ИС, выполняющие свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в организации и которым в администрации Дзун-Хемчикского кожууна присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования Программы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами администрации Дзун-Хемчикского кожууна. Для каждого внутреннего пользователя в ИС администрации Дзун-Хемчикского кожууна должны быть заведены учетные записи.

* 1. Пользователи ИС администрации Дзун-Хемчикского кожууна однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИС администрации Дзун-Хемчикского кожууна.
  2. Аутентификация пользователя в администрации Дзун-Хемчикского кожууна осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.
  3. В Программах обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.
  4. В Программах обеспечена многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов; пользователей), с использованием сети связи общего пользования, в том числе сети Интернет и с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, для локального доступа в систему с правами привилегированных учетных записей (администраторов; пользователей).

1. **Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных**
   1. В Программах до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация устройств (технических средств).
   2. Идентификации и аутентификации до начала информационного взаимодействия подлежат следующие типы устройств:
      * + АРМ пользователя;
        + Серверы;
        + Ноутбуки;
        + Тонкие клиенты;
        + Принтер;
        + Сканер.
   3. Идентификация устройств в ИС 1С: Бухгалтерия обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, МАС-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства. Аутентификация устройств в ИС администрации Дзун-Хемчикского кожууна обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.
2. **Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов**
   1. В ИС администрации Дзун-Хемчикского кожууна устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

* формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
* присвоение идентификатора пользователю и (или) устройству;
* предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года.
* блокирование идентификатора пользователя после 90 дней неиспользования.
  1. В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ.

1. **Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации**
   1. В ИС администрации Дзун-Хемчикского кожууна устанавливаются и реализуются функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

* изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты ИС администрации Дзун-Хемчикского кожууна;
* выдача средств аутентификации пользователям;
* генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
* установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 70 символов максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на 5 минут, смена паролей не более чем через 180 дней;
* блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
* назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
* обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 90 дней;
* защита аутентификационной информации от неправомерных доступа к ней и модифицирования.
  1. В случае компрометации личного пароля пользователя ИС администрации Дзун-Хемчикского кожууна должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:
     + Внеплановая смена личного пароля или удаление учетной записи пользователя ИС администрации Дзун-Хемчикского кожууна в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.
     + Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС администрации Дзун-Хемчикского кожууна.
  2. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ.

1. **Защита обратной связи при вводе аутентификационной информации**
   1. В ИС администрации Дзун-Хемчикского кожууна осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.
   2. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «\*», «•» или иными знаками.
2. **Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре (при наличии)**
   1. В ИС администрации Дзун-Хемчикского кожууна обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администратора ИС в соответствии с настоящими Правилами, в том числе:
      * идентификация и аутентификация администратора ВИ;
      * идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;
      * блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
      * защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;
      * защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;
      * идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.
   2. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с настоящими Правилами.
3. **Ответственность при организации идентификации и аутентификации**
   1. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ.
   2. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ и пользователей администрации Дзун-Хемчикского кожууна.
   3. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите информации.

**Лист ознакомления**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата**  **ознакомления** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Приложение 34**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**Положение о разграничении прав доступа к информации, обрабатываемой в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад администрации Дзун-Хемчикского кожууна**

1.1 Настоящее Положение определяет правила управления доступом субъектов доступа к объектам доступа в государственной информационной системе 1С: Бухгалтерия администрации Дзун-Хемчикского кожууна в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 согласно установленному классу защищенности (\_\_\_).

* 1. В государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад(далее - Программы) установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:
* определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
* объединение учетных записей в группы (при необходимости);
* верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
* заведение, активация, блокирование и уничтожение учетных записей пользователей; пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;
* порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
* уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
* предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

1.3 Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

1.4 В информационной системе используются автоматизированные средства поддержки управления учетными записями пользователей.

1.5 В информационной системе осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

1.6 В информационной системе осуществляется автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования: более 90 дней.

1.7 Для управления доступом субъектов доступа к объектам доступа в информационной системе реализуется(ются) следующий метод управления доступом:

* дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
* ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);
* мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

1.8 Правила разграничения доступа реализуются на основе установленных списков доступа или матриц доступа.

1.9 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов при входе в информационную систему.

1.10 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов к техническим средствам, устройствам, внешним устройствам.

1.11 В информационной системе правила разграничения доступа обеспечивают управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением.

1.12 Управление информационными потоками должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками. Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

1.13 В информационной системе обеспечивается разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями).

1.14 В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя до 15 минут или по запросу пользователя.

1.15 Перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации:

- Ввод информации идентификации и аутентификации.

1.16 Администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

1.17 Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

1.18 Защита удаленного доступа обеспечивается при всех видах доступа и включает:

* установление видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;
* предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
* мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;
* контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

1.19 В информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы.

1.20 В информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации.

1.21 В информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой.

1.22 Регламентация и контроль использования технологий беспроводного доступа включают:

* ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа;
* предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
* мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
* контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

1.23 В информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств;

1.24 В информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы.

1.25 Управление взаимодействием с внешними информационными системами включает:

* предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям;
* определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
* определение системных учетных записей, используемых в рамках данного взаимодействия; определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
* определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

1.26 Доступ к информационной системе предоставляется авторизованным (уполномоченным) пользователям внешних информационных систем или разрешение на обработку, хранение и передачу информации с использованием внешней информационной системы осуществляется при выполнении следующих условий:

* при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;
* при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

1.27 В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

1.28 В информационной системе доверенная загрузка обеспечивает:

* блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
* контроль доступа пользователей к процессу загрузки операционной системы;
* контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

1.29 В информационной системе осуществляется доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения.

**Приложение 35**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения в государственной информационной системах администрации Дзун-Хемчикского кожууна**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Настоящие правила регламентируют процесс установки (инсталляции) программного обеспечения вычислительной техники в администрации Дзун-Хемчикского кожууна.
   2. Настоящие правила и процедуры управления установкой (инсталляцией) программного обеспечения обязательны для соблюдения работниками администрации Дзун-Хемчикского кожууна.
2. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

Автоматизированное рабочее место (АРМ) – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.

Пользователь информационной системы (ИС) – работник Организации, использующий ПО (в составе АРМ) для выполнения своих трудовых обязанностей.

Программное обеспечение (ПО) – программное обеспечение вычислительной техники, базы данных.

1. **УСТАНОВКА (ИНСТАЛЛЯЦИЯ) ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И (ИЛИ) ЕГО КОМПОНЕНТОВ**
   1. Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов осуществляется только от имени администратора.
   2. Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке («белый список»), представленного в приложении № 1.
   3. В администрации Дзун-Хемчикского кожууна реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

* определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;
* настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);
* выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен);
* контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);
* определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.
  1. Установка программного обеспечения по просьбе сотрудника:
* в случае отсутствия программного обеспечения в перечне, представленном в Приложении № 1, <Администратор/подразделение по ЗИ> определяет возможность и целесообразность использования данного программного обеспечения в информационной системе Организации; в случае положительного решения новое программное обеспечение вносится в перечень разрешенного к установке.
  1. Периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе, проводится с периодичностью <…>.

**4. ПОРЯДОК ЭКСПЛУАТАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

4.1. В целях исполнения требований Законодательства в области защиты информации в администрации Дзун-Хемчикского кожууна разрешено применение ограниченного перечня коммерческого и бесплатного программного обеспечения (Приложение № 1), необходимого для выполнения производственных задач.

4.2. В состав каждого АРМ входит набор программного обеспечения для выполнения определенного вида деятельности. Первоначальная комплектация АРМ определяется начальником структурного подразделения совместно с специалистом по защите информации. ПО, не входящее в состав АРМ, не может быть установлено и использовано работниками администрации Дзун-Хемчикского кожууна без процедуры согласования.

4.3. Конкретный состав установленного ПО на каждом АРМ определяется на основании перечня программного обеспечения и перечня информационных ресурсов организации.

4.4. Изменение конфигурации аппаратно-программных средств защищенных рабочих станций и серверов без согласования с начальником отдела по защите информации категорически запрещается. Работы по изменению конфигурации защищенных рабочих станций и серверов производятся в присутствии работников отдела по защите информации и пользователя данной рабочей станции.

4.5. При эксплуатации программного обеспечения необходимо:

* использовать имеющееся в распоряжении ПО исключительно для выполнения своих служебных обязанностей;
* обеспечивать сохранность переданных в составе АРМ носителей с ключевой информацией, сертификатов подлинности коммерческого ПО, наклеенных на корпус системного блока АРМ;
* содействовать отделу по ЗИ в выполнении работ по установке, настройке, устранению неисправностей и аудита установленного ПО;
* ставить в известность отдел по защите информации о любых фактах нарушения требований настоящего Положения.

4.6. При эксплуатации программного обеспечения запрещено:

* использовать АРМ не по назначению;
* самостоятельно вносить изменения в конструкцию, конфигурацию, размещение АРМ ИС и другого оборудования ИС;
* изменять состав установленного на АРМ ПО (устанавливать новое ПО, изменять состав компонент пакетов ПО и удалять ПО);
* приносить на внешних носителях, загружать и не санкционированно запускать на своем или другом АРМ любые системные или прикладные программы.

**Приложение № 1 к приказу № \_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г. «Об организации обработки персональных данных в государственной информационной системе администрации Дзун-Хемчикского кожууна**

**Перечень программного обеспечения и (или) его компонентов, разрешенных к установке («белый список») в государственной информационной системе администрации Дзун-Хемчикского кожууна**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Программное обеспечение** | **Издатель** | **Наименование сегмента ГИС** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| … |  |  |  |
| № |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Приложение 36**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**ИНСТРУКЦИЯ**

**по модификации и техническому обслуживанию программного обеспечения и аппаратных средств государственной информационных системах**

**администрации Дзун-Хемчикского кожууна**

1. **Общие положения**

1.1. Настоящая инструкция регламентирует обеспечение безопасности информации при проведении модификации программного обеспечения, технического обслуживания и аппаратных средств государственных информационных системах администрации Дзун-Хемчикского кожууна.

* 1. Настоящая Инструкция регламентирует организацию мероприятий по обеспечению безопасности информации при проведении модификаций, технического обслуживания программного обеспечения, технического обслуживания средств вычислительной техники в работе государственных информационных системах администрации Дзун-Хемчикского кожууна.
  2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников структурных подразделений Организации, использующих в работе государственных информационных систем администрации Дзун-Хемчикского кожууна, в которой осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.
  3. Сотрудники администрации Дзун-Хемчикского кожууна, задействованные в обеспечении функционирования ГИС администрации Дзун-Хемчикского кожууна, знакомятся с основными положениями Инструкции в части, их касающейся, по мере необходимости.

# 

# ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ

* 1. Все изменения конфигурации технических и программных средств АРМ администрации Дзун-Хемчикского кожууна должны производиться только на основании заявок руководителей структурных подразделений Организации (Приложение № 1), согласованных с руководителем администрации Дзун-Хемчикского кожууна. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения.
  2. В заявке указываются наименование АРМ и ответственный за него сотрудник. После чего заявка передается Администратору ГИС для выполнения работ по внесению изменений в конфигурацию АРМ ГИС Организации.
  3. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ГИС Организации предоставляется Администратору ИБ, а также ответственному лицу за защиту ПДн.
  4. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме Администратора ИБ и/или ответственного лица за защиту ПДн, запрещено.
  5. Установка и настройка программного средства осуществляется администратором ГИС согласно эксплуатационной документации.
  6. Руководители структурных подразделений осуществляют контроль за отсутствием на АРМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.
  7. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится в соответствии с «Правилами и процедурами управления установкой (инсталляцией) компонентов программного обеспечения в государственных информационных системах администрации Дзун-Хемчикского кожууна.
  8. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с «Инструкцией по организации антивирусной защиты государственных информационных системах администрации Дзун-Хемчикского кожууна»
  9. После установки (обновления) ПО Администратор ИБ ГИС должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем АРМ, проверить правильность настройки средств защиты.
  10. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю своего подразделения и Администратору ИБ ГИС. Использование программного средства до получения специальных указаний запрещается.
  11. После завершения работ по внесению изменений в состав аппаратных средств защищенных АРМ системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) Администратором ИБ ГИС.
  12. При изъятии АРМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор ИБ ГИС снимет с данного АРМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации. Факт уничтожения данных оформляется актом.
  13. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств АРМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у Администратора ИБ ГИС.

# ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

* 1. Инструкция подлежит пересмотру при изменении перечня решаемых задач, состава технических и программных средств ГИС администрации Дзун-Хемчикского кожууна, приводящих к существенным изменениям технологии обработки информации.
  2. Пересмотр Настоящей инструкции проводится <ответственным лицом …> с целью проверки соответствия положений настоящей Инструкции реальным условиям применения их в ГИС администрации Дзун-Хемчикского кожууна.
  3. Вносимые изменения не должны противоречить другим положениям Инструкции.

# ОТВЕТСТВЕННОСТЬ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

* 1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Организации.
  2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на Администратора ИБ ГИС.
  3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту ПДн Организации.

**Приложение № 1 к Инструкции по модификации и техническому обслуживанию программного обеспечения и аппаратных средств государственных информационных системах администрации Дзун-Хемчикского кожууна**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г.**

<специалист по защите информации>

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**ЗАЯВКА**

**на внесение изменений в состав аппаратно-программных средств рабочей станции**

В связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование задач)

на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ с инвентарным № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ прошу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(наименование изменений)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

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

(должность) (подпись) (фамилия, инициалы)

**Приложение 37**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**ПОЛОЖЕНИЕ**

об использовании сети Интернет в автоматизированном рабочем месте государственной информационной системы **1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад**  администрации Дзун-Хемчикского кожууна

1. Работа в сетях общего доступа и (или) международного обмена (сети "Интернет" и других) в ГИС **1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад** (далее – Программы) должна осуществляться для выполнения должностных обязанностей.
2. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).
3. Вся информация о ресурсах, посещаемых сотрудниками администрации Дзун-Хемчикского кожууна, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений для детального изучения и принятия решения о мерах дисциплинарной ответственности.
4. Программные средства, используемые для доступа к сети Интернет, должны быть утверждены администратором информационной безопасности.
5. Пользователи сети обязаны обеспечивать беспрепятственный доступ администратора ИБ к сетевому оборудованию и компьютерам пользователей для организации профилактических и ремонтных работ.
6. Пользователи сети обязаны выполнять предписания администраторов ИБ, направленные на обеспечение безопасности сети.
7. При работе в Сети запрещается:

* осуществлять работу при отключенных средствах защиты;
* передавать по Сети защищаемую информацию без использования средств шифрования;
* посещать сайты сомнительной репутации (порносайты, сайты, содержащие нелегально распространяемое ПО, и другие);
* скачивать и запускать с любых ресурсов любые неизвестные исполняемые файлы без согласования с администратором информационной безопасности;
* использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором ИБ;
* умышленное распространение и получение материалов в/из сети интернет, противоречащих законодательству Российской Федерации;
* фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть интернет.
* предоставлять доступ в сеть интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть администрации Дзун-Хемчикского кожууна
* осуществлять несанкционированный доступ к ресурсам и сервисам сети интернет;
* выполнять действия, направленные на нарушение функционирования элементов сети интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения и т. д.).

8. Правила работы с электронной почтой:

8.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

8.2. Запрещается отправлять файлы, содержащие конфиденциальную информацию в открытом виде (не зашифрованном).

8.3. Запрещается массовая рассылка почтовых сообщений (более 40) внешним адресатам без согласования с руководством (спама).

8.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

8.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat). В случае необходимости отправки таких файлов, помещать их в архив.

8.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

8.7 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

8.8 Запрещается использовать адрес электронной почты для оформления подписок.

8.9 Запрещается публиковать свой электронный адрес либо адреса других сотрудников Организации на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости.

* 1. Запрещается рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа.
  2. Запрещается предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

**Приложение 38**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

от \_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_

**ПОРЯДОК**

**действий при обнаружении отказов функционирования технических средств государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад**

1. Оператором информационной системы должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.
2. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).
3. При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с пунктами 4, 5-5.9 Настоящего порядка, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в журнале регистрации событий, связанных со сбоями и отказами в функционировании технических средств государственной информационной системы **1С: Бухгалтерия** (Приложение № 1).
4. В ГИС 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад (далее – Программы) должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.
5. План действий персонала при возникновении нештатных ситуаций:
   1. Сбой программного обеспечения:

Администратор безопасности совместно с уполномоченным работником по ЗИ выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения по ЗИ для принятия решения.

5.2. Отключение электропитания технических средств ГИС:

Администратор безопасности совместно с уполномоченным работником по ЗИ проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор безопасности сообщает руководителю по ЗИ для принятия решения.

5.3. Выход из строя технических средств ГИС (серверов, рабочих станций):

Уполномоченный работник по ЗИ совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ГИС (замене рабочей станции).

О выходе из строя сервера (рабочей станции) уполномоченный работник подразделения по ЗИ, ответственный за эксплуатацию сервера (рабочей станции), сообщает специалисту по ЗИ.

При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте администратор безопасности сообщает специалисту по ЗИ для принятия решения.

5.4. Потеря данных:

При обнаружении потери данных уполномоченный работник по ЗИ проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

При необходимости уполномоченным работником по ЗИ производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте уполномоченный работник по ЗИ сообщает администратору безопасности. Администратор безопасности сообщает специалисту по ЗИ для принятия решения.

5.5. Обнаружение вредоносной программы в программной среде средств автоматизации Программ:

При обнаружении вредоносной программы производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, и уполномоченным работником по ЗИ и администратором безопасности проводится анализ состояния рабочей станции (сервера).

В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции (сервера) данные могут быть потеряны. После успешной ликвидации вредоносной программы сохраненные данные подвергаются повторной проверке на наличие вредоносной программы. Кроме того, при обнаружении вредоносной программы следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

После ликвидации вредоносной программы проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

По факту появления вредоносной программы в локальной вычислительной сети Группой реагирования на инциденты ИБ проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается специалист по ЗИ.

5.6. Утечка информации:

5.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и начальник структурного подразделения. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов Программ: и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

5.7. Взлом операционной системы средств автоматизации ГИС (несанкционированное получение доступа к ресурсам операционной системы):

При обнаружении взлома сервера ставится в известность руководитель подразделения по ЗИ.

По возможности производится временное отключение сервера от локальной вычислительной сети администрации Дзун-Хемчикского кожууна для проверки на наличие вредоносной программы. Возможен временный переход на резервный сервер.

Уполномоченным работником подразделения по ЗИ проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Уполномоченным работником подразделения по ЗИ проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

В случае необходимости уполномоченным работником подразделения по ЗИ производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ГИС.

5.8. Попытка несанкционированного доступа (НСД):

При попытке НСД уполномоченным работником подразделения по ЗИ и администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, уполномоченным работником по ЗИ устанавливаются такие обновления.

По факту попытки НСД Группой реагирования на инциденты ИБ проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем подразделения по ЗИ.

В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ГИС субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

5.9. Отказ в обслуживании:

Работником, обнаружившим отказ в обслуживании, ставятся в известность: специалиста по ЗИ.

Уполномоченным работником по ЗИ проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

Уполномоченным работником по ЗИ проводится проверка программного обеспечения на целостность и на наличие вредоносных программ, а также проверка целостности данных и анализ электронных журналов.

При необходимости, уполномоченным работником по ЗИ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

О причинах инцидента и принятых мерах уполномоченный работник по ЗИ информирует специалиста по ЗИ.

**Приложение 39**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Регламент порядка проведения проверок состояния защиты государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад администрации Дзун-Хемчикского кожууна**

**1. Общие положения**

1.1 Настоящий документ определяет порядок проведения проверок состояния защиты государственной информационной системы **1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад** (далее – ГИС **Программы**).

1.2 Проведение проверок состояния ГИС **Программы** осуществляется в целях выявления нарушений требований нормативной документации, установление причин нарушений, разработка плана корректирующих действий, направленных на устранение и предотвращение нарушений.

1.3 Приказом назначается рабочая группа (комиссия) по проведению проверки состояния защищенности государственной информационной системы **Программы**.

1.4. Сотрудники администрации Дзун-Хемчикского кожууна знакомятся с основными положениями и приложениями регламента в части, их касающейся, по мере необходимости.

**2. Порядок проведения внутренних проверок**

2.1. При проведении внутренней проверки производится:

* актуальность организационно-распорядительной документации;
* проверка соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
* ….

2.2 Внутренние проверки проводятся в соответствии с планом внутренних проверок состояния защиты государственной информационной системы **Программы**. План формируется в конце текущего года на последующий. Форма Плана представлена в Приложении 1.

2.3 План составляется администратором ИБ.

2.4 План должен содержать перечень мероприятий по проверке, перечень проверяемых подразделений и сроки проведения проверок, составленные с учетом требований руководителей отделов и администраторов ИС.

2.5 На основании утвержденного Плана проведения внутренних проверок состояния защиты государственной информационной системы **Программы** составляется приказ о проведении проверки ГИС **Программы**. Приказ издается не позднее, чем за десять дней до даты проверки.

2.6 В ходе проверки должна быть получена объективная и полная информация по состоянию защиты ГИС.

2.7 Проверяющие имеют право осматривать помещения, где производится обработка защищаемой информации, получать доступ к техническим средствам, участвующим в обработке, просматривать настройки средств защиты информации, а также проводить беседы и консультации с работниками отделов.

2.8 При проведении проверок, в общем случае, должно проверяться:

* выполнение пользователями и администраторами требований инструктивных материалов по защите конфиденциальной информации;
* исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
* правильность организации работы со сведениями конфиденциального характера;
* соответствие системы защиты информации реальному положению дел и т.п.

Для проверки эффективности системы защиты ГИС **Программы** должны использоваться средства выявления уязвимостей.

2.9 По результатам проверки составляется акт о результатах (Приложение № 2) выявленных недостатков и нарушений, предложений по их устранению. Руководитель Организации должен быть поставлен в известность о выявленных несоответствиях в течение трех дней после проведенной проверки.

 

# 3. Корректирующие мероприятия и контроль за их исполнением

3.1. Руководитель анализирует акт о результатах внутренней проверки и в трехдневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

3.2. Если определить корректирующие мероприятия самостоятельно невозможно, то к анализу привлекаются специалисты соответствующих областей.

3.3. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки защищаемой информации и администратором ИБ.

3.4. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

# 4. Порядок пересмотра регламента

4.1. Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ГИС **Программы**.

4.2. Частичный пересмотр данного документа проводится по письменному предложению администратора информационной безопасности.

4.3. Вносимые изменения не должны противоречить другим положениям Регламента.

**Приложение № 1 к Регламенту порядка проведения проверок состояния защиты государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад администрации Дзун-Хемчикского кожууна от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**ФОРМА ПЛАНА ВНУТРЕННИХ ПРОВЕРОК СОСТОЯНИЯ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад**

**УТВЕРЖДАЮ**

<Должность руководителя организации>

\_\_\_\_\_\_\_\_\_\_\_\_\_ /<ФИО руководителя>

«\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г.

**План внутренних проверок состояния защиты государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад на 20\_\_ год**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Наименование информационной системы** | **Наименование мероприятия** | **Период проведения проверки** | **Отметка о выполнении (№ акта проверки)** | **Отметка о проведении корректирующих мероприятий** | **Примечание** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |

**Приложение № 2 к Регламенту порядка проведения проверок состояния защиты государственной информационной системы <Наименование ИС> <Наименование организации> от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**ФОРМА АКТА ВНУТРЕННЕЙ ПРОВЕРКИ**

**АКТ**

**о результатах внутренней проверки состояния защищенности государственной информационной системы** <Наименование ИС> <Наименование организации>

№\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г.

1. *Цели проверки:* выявления нарушений требований нормативной документации, установление причин нарушений, разработка плана корректирующих действий, направленных на устранение и предотвращение нарушений.

2. *Основание:* приказ о проведении проверки ГИС <Наименование ИС> от «\_\_» \_\_\_\_\_\_ 20\_\_г.

3. *Дата проведения проверки: \_\_\_\_\_\_\_\_\_\_\_*

4. *Результаты проверки:*

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

5. *Рекомендации по устранению нарушений:*

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

Члены рабочей группы:

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

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

**Приложение 40**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Журнал регистрации событий, связанных со сбоями и отказами в функционировании технических средств государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет),** **Технокад**

Журнал начат «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г.

Ответственный за ведение журнала (должность)

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал завершен «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г.

Должность

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал составлен на \_\_\_\_\_ листах

Место хранения в процессе работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **№ п/п** | **Дата (число, месяц, год)** | **Инвентарный (заводской) номер технического средства** | **Местонахождение технического средства (адрес здания, номер кабинета, подразделение)** | **Признаки (характер) сбоя/отказа** | **Должность, ФИО и подпись работника, обнаружившего сбой/отказ** | **Решение о реагировании на сбой/отказ** | **Отметка об устранении сбоя/отказа.**  **Дата, подпись работника, ответственного за устранения сбоя/отказа.** | **Примечание** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |

**Приложение 41**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Границы контролируемой зоны**

С целью выполнения требований Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

1. Устанавливается границы контролируемой зоны государственной информационной системы 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад в соответствии со схемой, представленной в Приложении №

2. Обеспечение контролируемой зоны возлагается на Ответственного по защите информации.

**Приложение № 1 к приказу № \_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ г. «Об утверждении границ контролируемой зоны»**

Схема размещения ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад относительно границ контролируемой зоны



Граница контролируемой зоны (2эт. Жизнеобеспечение по адресу: г.Чадан, ул. Ленина 42)

Граница контролируемой зоны (2эт. Бухгалтерия , земельный отдел по адресу: г.Чадан, ул. Ленина 42)

**Приложение 42**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Список должностей, лиц, допущенных (имеющих доступ) в помещения Администрации Дзун-Хемчикского кожууна, в которых ведется обработка конфиденциальной информации**

В целях обеспечения защиты конфиденциальной информации, обрабатывающейся в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад Администрации Дзун-Хемчикского кожууна в соответствии с Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания 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»

Утверждается:

1. Список должностей лиц, имеющих доступ в помещения **Администрации Дзун-Хемчикского кожууна**, в которых ведется обработка конфиденциальной информации, согласно Приложению № 1.
2. Допуск лиц, не указанных в «Перечне должностей лиц, допущенных (имеющих доступ) в помещения, в которых ведется обработка конфиденциальной информации», осуществляется сотрудниками Администрации Дзун-Хемчикского кожууна, имеющими постоянный доступ в помещения.
3. Ремонтные, наладочные и другие виды работ осуществляются только в присутствии сотрудников Администрации Дзун-Хемчикского кожууна, имеющих постоянный доступ в помещения.

**Приложение № 1 к списку должностей, лиц, допущенных (имеющих доступ) в помещения Администрации Дзун-Хемчикского кожуу, в которых ведется обработка конфиденциальной информации»**

**Перечень должностей лиц, допущенных (имеющих доступ) в помещения Администрации Дзун-Хемчикского кожуу, в которых ведется обработка конфиденциальной информации**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование отдела** | **Должность** |
| 1 | **Администрация(без ограничений)** | Председатель администрации |
| 2 | **Администрация(без ограничений)** | Заместители председателя администрации |
| 3 | **Бухгалтерия каб. 210** | Начальник отдела (главный бухгалтер) |
| … | **Бухгалтерия каб 211** | Заместитель главного бухгалтера |
| № | **Бухгалтерия каб 211** | Расчетный бухгалтер |
|  | **Бухгалтерия каб 211** | Материальный бухгалтер |
|  | **Бухгалтерия каб 211** | Экономист |
|  | **Жизнеобеспечения каб. 201** | Консультант по архитектуре и строительству |
|  | **Экономический отдел каб. 305** | Главный специалист по экономическому анализу и стратегическому развитию |
|  | **Жизнеобеспечения каб 201** | Начальник отдела ГО и ЧС |
|  | **Отдел кадров каб 307** | Начальник отдела по правовым и кадровым вопросам |
|  | **Отдел кадров каб 307** | Главный специалист по кадрам |
|  | **Администрация(без ограничений** | Консультант по тендерным торгам и программному обеспечению |
|  | **Администрация(без ограничений** | Руководитель аппарата – управляющего делами |
|  | **УМИ и ЗО(земельный отдел) 213** | Ведущий специалист по муниципальному земельному контролю |
|  | **Приемная администрации каб 301,302** | Консультант по документационному обеспечению |
|  | **Каб 304** | Консультант по делам молодежи и спорта |
|  | **Каб 106** | Консультант по внутреннему муниципальному контролю |
|  | **УМИ и ЗО(земельный отдел) 213** | Начальник отдела УМИ и ЗО |
|  | **Каб 101** | Главный специалист по архивному делу |
|  | **Каб 313** | Ответственный секретарь административной комиссии |
|  | **Каб 305** | Главный специалист по обращению граждан и СМИ |
|  | **Каб 308** | Главный специалист по работе с ОМСУ |
|  | **Каб 309** | Специалист по проектному управлению |

**Приложение 43**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Правила доступа в помещения администрации Дзун-Хемчикского кожууна в рабочее и нерабочее время, а также в нештатных ситуациях**

1. Общие положения
   1. Настоящие Правила устанавливают условия и порядок осуществления доступа в помещения администрации Дзун-Хемчикского кожууна, в которых осуществляется обработка конфиденциальной информации, в том числе персональных данных (далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в эти Помещения.
   2. Настоящие Правила разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания 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».
   3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.
   4. Помещения должны оснащаться входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода.
2. Правила доступа в помещения в рабочее, нерабочее время, в нештатных ситуациях
   1. Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень должностей лиц, допущенных (имеющих доступ) в помещения администрации Дзун-Хемчикского кожууна, в которых ведется обработка конфиденциальной информации, утвержденный администрацией Дзун-Хемчикского кожууна.
   2. В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок, подписанных руководителем подразделения или лицами допущенных (имеющих доступ) в помещения.
   3. Допуск лиц, не указанных в «Перечне должностей лиц, допущенных (имеющих доступ) в помещения, в которых ведется обработка конфиденциальной информации», осуществляется сотрудниками администрации Дзун-Хемчикского кожууна, имеющими постоянный доступ в помещения администрации Дзун-Хемчикского кожууна.
   4. Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.
   5. Перед началом рабочего дня, если кабинет был запечатан, вскрытие помещения сотрудником осуществляется следующим образом:

* на посту охраны в журнале приема-сдачи помещений под охрану делается запись о снятии помещения с сигнализации (если имеются) и о его вскрытии, при этом указываются: время, № кабинета, фамилия, имя, отчество сотрудника и подпись;
* при вскрытии помещения проверяется целостность печати и исправность замков;
* при обнаружении нарушения целостности оттисков печатей, повреждения замков, а также других признаков, указывающих на возможное проникновение в защищаемое помещение посторонних лиц, вскрытие не производят, о случившемся составляют акт и немедленно ставят в известность руководителя предприятия и орган безопасности. Одновременно принимаются меры по охране места происшествия, до прибытия сотрудников органа безопасности.
  1. По окончанию рабочего времени сотрудник, ответственный за сдачу помещения под охрану, выполняет следующие действия:
* закрывает в металлических шкафах служебную документацию, литературу, предназначенную для служебного пользования;
* закрывает окна;
* выключает освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения;
* закрывает дверь на замок, проверяет прочность закрытия двери, опечатывает кабинет(если необходимо);
* лично информирует охрану о постановке помещения на сигнализацию и о его закрытии, при этом в журнале приема-сдачи помещений под охрану делается запись о постановке на охрану помещения, при этом указываются: время, № кабинета, свою фамилию, имя и отчество.
  1. На посту охраны должны находиться списки сотрудников, подписанные председателем администрации, которым разрешено вскрытие и сдача под охрану защищаемого помещения, с фотографиями сотрудников и образцами подписей этих сотрудников.
  2. Все ключи учитываются в журнале учета ключей от защищаемого помещения (далее - журнал). Листы журнала должны быть пронумерованы, прошнурованы и скреплены мастичной печатью на последней странице.
  3. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение или руководителю структурного подразделения. Помещения вскрывать запрещается. Помещения вскрываются ответственным за помещение или руководителем структурного подразделения в присутствии сотрудника охраны с составлением акта.
  4. Уборка помещений, в которых ведется обработка конфиденциальной информации и хранятся документы и носители защищаемой информации, должна производиться в присутствии сотрудников администрации Дзун-Хемчикского кожууна.
  5. Установка оборудования, его замена или ремонт в защищаемых помещениях должны проводиться по согласованию с лицом, ответственным за проведение соответствующих работ (установку оборудования) в администрации Дзун-Хемчикского кожууна.
  6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю подразделения администрации Дзун-Хемчикского кожууна.
  7. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Министерства.

**Приложение 44**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Журнал учета сейфов, металлических шкафов, специальных хранилищ и ключей от них**

**администрации Дзун-Хемчикского кожууна**

Журнал начат «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г.

Ответственный за ведение журнала (должность)

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал завершен «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г.

Должность

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал составлен на \_\_\_\_\_ листах

Место хранения в процессе работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **№ п/п** | **Наименование хранилища (сейф, металлический шкаф, специальное хранилище)** | **Инвентарный (заводской) номер хранилища** | **Местонахождение хранилища (адрес здания, номер кабинета, подразделение)** | **ФИО ответственного за хранилище** | **Количество комплектов ключей** | **Номер экземпляра ключа (печати)** | **Дата, фамилия, имя, отчество получившего ключ, подпись** | **Сведения об утрате/ замене ключа (№ акта, служебной записки и т. д. )** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |
| № |  |  |  |  |  |  |  |  |

**Приложение 45**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Журнал**

**поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов**

**администрации Дзун-Хемчикского кожууна**

Журнал начат «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г.

Ответственный за ведение журнала (должность)

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал завершен «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г.

Должность

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал составлен на \_\_\_\_\_ листах

Место хранения в процессе работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **№ п/п** | **Наимено-вание СКЗИ, эксплуата-ционной и технической документации к ним, ключевых документов** | **Серийный номер СКЗИ, эксплуата-ционной и технической документации к ним, номера серий ключевых документов** | **Номер экземпляров (криптогра-фические номера) ключевых документов** | **Отметка о получении** | | **Отметка о выдаче** | | **Отметка о подключении (установке СКЗИ)** | | | **Отметка об изъятии СКЗИ из аппаратных средств , уничтожении ключевых документов** | | | **Примечание** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **От кого получе-ны** | **Дата и номер сопроводи-тельного письма** | **ФИО пользова-теля СКЗИ** | **Дата и расписка в получении** | **ФИО сотрудников органа криптогра-фической защиты, пользователя СКЗИ, произведших подключение (установку)** | **Дата подклю-чения (установки), подписи лиц, произведших подключение (установку)** | **Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ** | **Дата изъятия (унич-тожения)** | **ФИО сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожения)** | **Номер акта или расписка об уничтожении** |  |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| № |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Приложение 46**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Журнал**

**ознакомления работников администрации Дзун-Хемчикского кожууна с локальными нормативными актами в области защиты информации**

Журнал начат «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г.

Ответственный за ведение журнала (должность)

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал завершен «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г.

Должность

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал составлен на \_\_\_\_\_ листах

Место хранения в процессе работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

| **№ п/п** | **ФИО работника** | **Должность** | **Структурное подразделение** | **Дата ознакомления** | **Подпись** |
| --- | --- | --- | --- | --- | --- |
| 1. **Наименование документа, реквизиты** | | | | | |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| … |  |  |  |  |  |
| № |  |  |  |  |  |
| 1. **Наименование документа, реквизиты** | | | | | |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| … |  |  |  |  |  |
| № |  |  |  |  |  |
| … | | | | | |

**Приложение 47**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Журнал**

**инструктажа сотрудников администрации Дзун-Хемчикского кожууна с документами в области обеспечения информационной безопасности с использованием средств защиты информации и средств криптографической защиты информации**

Журнал начат «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г.

Ответственный за ведение журнала (должность)

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал завершен «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г.

Должность

/\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Журнал составлен на \_\_\_\_\_ листах

Место хранения в процессе работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Инструктаж получил:** | | | **Инструктаж провел:** | | |
| **ФИО работника** | **Должность** | **Подпись** | **ФИО** | **Подпись** | **Дата** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
| № |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Приложение 48**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**Матрица доступа к сведениям конфиденциального характера, обрабатываемым в администрации Дзун-Хемчикского кожууна**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование АРМ** | **Месторасположение АРМ (улица, № дома, № кабинета)** | **Имя пользователя (группы)** | **Наименование защищаемых информационных ресурсов**  **(логические диски, каталоги, программы, устройства и т. д.)** | **Тип доступа** | **Примечание** |
| 1 | АРМ1-8 | Ул.Ленина 42, каб. № 211,212,101,106,213,201 | Администратор | Компьютер(системный блок- информационные системы) | Чтение |  |
| Запись |
| Выполнение |
| Изменения настроек |  |
| Принтер | Печать |  |
| Сканер | Сканирование |  |
| … | … |  |
| 2 | АРМ1-8 | Ул.Ленина 42, каб. № 211,212,101,106,213,201 | пользователь | Компьютер(системный блок- информационные системы) | Чтение |  |
|  | Запись |  |
|  | Выполнение |  |
| Принтер | Печать |  |
| Сканер | Сканирование |  |
|  |  |  |  |  |  |  |

**Приложение 49**

к распоряжению председателя

администрации

Дзун-Хемчикского кожууна

**ИНСТРУКЦИЯ**

**администратора безопасности информации**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящая Инструкция определяет обязанности администратора безопасности информации, обрабатываемой в государственной информационной системе 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад (далее - администратора безопасности).

1.2. Администратор безопасности назначается распоряжением председателя администрации Дзун-Хемчикского кожууна из числа подготовленных работников подразделения по защите информации (ЗИ).

1.3. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю подразделения по ЗИ, назначаемым ответственным за обеспечение безопасности информации в администрации Дзун-Хемчикского кожууна.

1.4. Администратор безопасности отвечает за поддержание установленного уровня защищенности обрабатываемой в информационной системе информации, в том числе персональных данных.

1.5. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ГИС 1С: Бухгалтерия, зарплата и кадры, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация,ФСС (личный кабинет), Технокад (далее-Программа) в вопросах обеспечения безопасности информации.

1.6. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями Программы.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в Программах, состояние и поддержание установленного уровня защиты информации, обрабатываемой в Программах.

**2. ЗАДАЧИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

2.1. Основными задачами администратора безопасности являются:

* поддержание необходимого уровня защищенности обрабатываемых в сегментах Программы персональных данных от несанкционированного доступа (НСД) к информации;
* обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
* установка средств защиты информации и контроль выполнения правил их эксплуатации;
* сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) Программы;
* периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
* оперативное реагирование на нарушения требований по ИБ в Программах и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

* текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
* текущий контроль технологического процесса автоматизированной обработки конфиденциальной информации, в том числе персональных данных;
* участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности защищаемой информации;
* контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в структурных подразделениях администрации Дзун-Хемчикского кожууна и подведомственных организациях администрации Дзун-Хемчикского кожууна;
* методическую помощь всем работникам администрации Дзун-Хемчикского кожууна и подведомственных организациях администрации Дзун-Хемчикского кожууна по вопросам обеспечения безопасности защищаемой информации.

**3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

Администратор безопасности обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в Программах.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям Программ согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Вести контроль осуществления резервного копирования информации.

3.6. Анализировать состояние защиты Программ.

3.7. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.8. Контролировать физическую сохранность технических средств обработки информации.

3.9. Контролировать исполнение пользователями Программ введенного режима безопасности, а также правильность работы с элементами ГИС и средствами защиты информации.

3.10. Контролировать исполнение пользователями правил парольной политики.

3.11. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.12. Не допускать установку, использование, хранение и размножение в Программах программных средств, не связанных с выполнением функциональных задач.

3.13. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) Программы.

3.14. Оказывать помощь пользователям Программ в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.15. Периодически представлять руководству отчет о состоянии защиты Программ и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.16. В случае отказа работоспособности технических средств и программного обеспечения Программ, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.17. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.18. Принимать участие в проведении работ по оценке соответствия Программ требованиям безопасности информации .

**4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

Администратор безопасности имеет право:

4.1. Отключать от ресурсов Программ работников, осуществивших НСД к защищаемым ресурсам ГИС или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств Программ.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями администрации Дзун-Хемчикского кожууна и подведомственных организациях администрации Дзун-Хемчикского кожууна телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями Программ при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом подведомственных организациях администрации Дзун-Хемчикского кожууна по вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ защищаемой информации, обрабатываемой в Программе.

**5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ**

Администратор безопасности несет ответственность (дисциплинарную, гражданскую, административную, уголовную и иную, предусмотренную законодательством Российской Федерации ответственность):

5.1. За организацию защиты информационных ресурсов и технических средств Программ

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ГИС, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов Программ.

5.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

**6. ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД**

6.1. К попыткам НСД относятся:

* сеансы работы с телекоммуникационными ресурсами администрации Дзун-Хемчикского кожууна и подведомственных организациях администрации Дзун-Хемчикского кожууна незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;
* действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам Программ с использованием учетной записи администратора или другого пользователя ГИС, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор безопасности обязан:

* прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:
* доложить руководству подразделения по ЗИ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
* известить Руководителя структурного подразделения администрации Дзун-Хемчикского кожууна и подведомственных организациях администрации Дзун-Хемчикского кожууна, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
* проанализировать характер НСД;
* по решению руководства подразделения по ЗИ осуществить действия по выяснению причин, приведших к НСД;
* предпринять меры по предотвращению подобных инцидентов в дальнейшем.