ТЫВА РЕСПУБЛИКАНЫН МУНИЦИПАЛДЫГ РАЙОН «ОВУР КОЖУУН»
ЧАГЫРГАЗЫНЫН
АЙТЫЫШКЫНЫ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «ОВЮРСКИЙ КОЖУУН» РЕСПУБЛИКИ ТЫВА
РАСПОРЯЖЕНИЕ

с. Хандагайты

от 15 апреля 2021 года № 105

О защите информации

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. Возложить обязанности по защите информации:

1.1. Назначить ответственным за организацию обработки персональных данных: Монгуш Чодураа Когеловну – заместителя председателя по экономике и инвестиционной политике.

1.2. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах (далее – ИС) персональных данных: Айыжы Айланмаа Константиновна – начальника отдела организационного и кадрового обеспечения.

1.3. Назначить ответственным за эксплуатацию ИС: Ооржак Долаана Яношовна – консультант по экономике, предпринимательству и торгам.

1.4. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно приложению 1 к настоящему распоряжению.

1.5. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации согласно приложению 2 к настоящему распоряжению.

1.6. Утвердить перечень лиц, ответственных за обезличивание персональных данных согласно приложению 3 к настоящему распоряжению.

2. Создать комиссию по защите информации:

2.1. Утвердить состав комиссии по защите информации согласно приложению 4 к настоящему распоряжению.

2.2. Утвердить положение о комиссии по защите информации согласно приложению 5 к настоящему распоряжению.

3. Утвердить типовые формы документов по защите информации:

3.1. Согласие на обработку персональных данных согласно приложению 6 к настоящему распоряжению.

3.2. Разъяснение субъекту персональных данных согласно приложению 7 к настоящему распоряжению.

3.3. Обязательство о неразглашении информации, содержащей персональные данные, согласно приложению 8 к настоящему распоряжению.

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

3.5. Протокол заседания комиссии по защите информации согласно приложению 10 к настоящему распоряжению.

3.6. Акт определения уровня защищенности персональных данных (далее –ПДн) при их обработке в информационных системах по обработке персональных данных (далее – ИСПДн) и класса защищенности ИС согласно приложению 11 к настоящему распоряжению.

3.7. Акт об уничтожении персональных данных субъектов персональных данных согласно приложению 12 к настоящему распоряжению.

3.8. Перечень объектов защиты информационных системах администрации Овюрского кожууна (приложение 30);

3.9. Описание технологического процесса обработки информации в государственной информационной системе «Локальная вычислительная сеть администрации Овюрского 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 Овюрского 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 Овюрского 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 Овюрского кожууна (приложение 37);

3.13. Границы контролируемой зоны (приложение 41);

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

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

4. Утвердить политику в отношении обработки персональных данных согласно приложению 13.

5. Утвердить инструкции и правила по защите информации:

– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 14 к настоящему распоряжению.

– Правила рассмотрения запросов субъектов персональных данных согласно приложению 15 к настоящему распоряжению.

– Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно приложению 16 к настоящему распоряжению;

– Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно приложению 17 к настоящему распоряжению;

– Инструкцию по организации резервного копирования, согласно приложению 18 к настоящему распоряжению;

– Инструкцию по организации парольной защиты, согласно приложению 19 к настоящему распоряжению;

– Инструкцию по организации антивирусной защиты, согласно приложению 20 к настоящему распоряжению;

– Инструкцию по проверке электронного журнала обращений к информационной системе персональных данных, согласно приложению 21 к настоящему распоряжению;

– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно приложению 22 к настоящему распоряжению;

– Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно приложению 23 к настоящему распоряжению;

– Инструкцию по обращению с криптосредствами согласно приложению 24 к настоящему распоряжению;

– Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 25 к настоящему распоряжению;

– Правила работы с обезличенными данными согласно приложению 26 к настоящему распоряжению;

– Инструкцию по работе с инцидентами информационной безопасности согласно приложению 27 к настоящему распоряжению;

– Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно приложению 28 к настоящему распоряжению.

– 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 Овюрского кожууна (приложение 35);

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

– администрации Овюрского 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 Овюрского кожууна (приложение 39);

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

– ИНСТРУКЦИЯ администратора безопасности информации (приложение 49);

6. Утвердить план мероприятий по защите информации согласно приложению 29 к настоящему распоряжению.

Председатель А.Н. Ооржак

Приложение 1
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Должность	ИСПДн
Председатель администрации	Без ограничений
Заместители председателя администрации	Без ограничений
Начальник отдела финансового и материально-технического обеспечения	1С, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация, ФСС личный кабинет. СЭД
Консультант по земельным отношениям, архитектуре и градостроительству	ФГИС ТП, Технокад муниципалитет, ФИАС, ГИС ЖКХ, СЭД
Начальник отдела экономики, проектного управления и развития туризма	ГАСУ,СЭД
Ведущий специалист по ГО и ЧС- руководитель ЕДДС	СЭД, ГАСУ
Консультант по юридическим вопросам	Контур-Экстерн, Spu-orb, СЭД
Начальник отдела организационного и кадрового обеспечения	Контур-Экстерн, Spu-orb, СЭД
Консультант по экономике, предпринимательству и торгам	Без ограничений
Управляющий делами	Без ограничений
Начальник отдела по земельным, имущественным отношениям, архитектуре и градостроительству	Torgi.gov.ru, ФГИС «Единый реестр проверок», ГАСУ, ГИС ГМП, Технокад, ФГИС ТП, СЭД
Главный специалист организационного и документационного обеспечения	СЭД
Начальника отдела по делам молодежи и спорта и информационной политики	СЭД

Ведущий специалист по бюджетному учету, отчетности и информационным технологиям	1С, СУФД, Единый портал бюджетной системы, ГИС ГМП, Spu-orb, Налогоплательщик ЮЛ, Контур-Экстерн, Web-консолидация, ФСС личный кабинет. СЭД
Ведущий специалист по земельному контролю и имущественным отношениям	Torgi.gov.ru, ФГИС «Единый реестр проверок», ГАСУ, ГИС ГМП, Технокад, ФГИС ТП, СЭД
Ведущий специалист по архиву	СЭД, ГАСУ
Ответственный секретарь административной комиссии	СЭД
Главный специалист по информационной политике и СМИ	ССТУ, СЭД
Ведущий специалист по социальным вопросам с. Хандагайты	СЭД
Ведущий специалист ВУС	СЭД
Ответственный секретарь административной и антитеррористической комиссии	СЭД
Главный специалист по спорту	СЭД
Ответственный секретарь КДН и ЗП	СЭД
Ведущий специалист с.Хандагайты	СЭД
Ведущий специалист по делопроизводству -секретарь председателя	СЭД
Ведущий специалист по ЖКХ и благоустройству	СЭД

Приложение 2
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

Должность
Председатель администрации
Заместители председателя администрации
Начальник отдела финансового и материально-технического обеспечения
Консультант по земельным отношениям, архитектуре и градостроительству
Начальник отдела экономики, проектного управления и развития туризма
Ведущий специалист по ГО и ЧС- руководитель ЕДДС
Консультант по юридическим вопросам
Начальник отдела организационного и кадрового обеспечения
Консультант по экономике, предпринимательству и торгам
Управляющий делами
Начальник отдела по земельным, имущественным отношениям, архитектуре и градостроительству
Главный специалист организационного и документационного обеспечения
Начальника отдела по делам молодежи и спорта и информационной политики
Ведущий специалист по бюджетному учету, отчетности и информационным технологиям
Ведущий специалист по земельному контролю и имущественным отношениям
Ведущий специалист по архиву
Ответственный секретарь административной комиссии
Главный специалист по информационной политике и СМИ
Ведущий специалист по социальным вопросам с. Хандагайты
Ведущий специалист ВУС
Ответственный секретарь административной и антитеррористической комиссии
Главный специалист по спорту
Ответственный секретарь КДН и ЗП
Ведущий специалист с.Хандагайты

Приложение 3
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Перечень лиц, ответственных за обезличивание персональных данных

Должность	Ф.И.О.
Председатель администрации	Ооржак Аржаан Никифорович
заместитель председателя администрации	Монгуш Чодураа Когеловна
начальник отдела финансового и материально-технического обеспечения	Сат Саида Юрьевна
Начальник отдела организационного и кадрового обеспечения	Айыжы Айланмаа Константиновна
Консультант по юридическим вопросам	Монгуш Чаяна Владимировна
Управляющий делами	Самбуу Аржана Николаевна
Начальник отдела по земельным, имущественным отношениям, архитектуре и градостроительству	Ортеней Эльза Викторовна
Главный специалист организационного и документационного обеспечения	Монгуш Сильвия Радиевна
Консультант по земельным отношениям, архитектуре и градостроительству	Тюлюш Дан-Хаяа Анашовна
Ведущий специалист по земельному контролю и имущественным отношениям	Ондар Сырга Алдын-Хереловна
Ведущий специалист по архиву	Очур-оол Айза Робертовна
Ответственный секретарь административной и антитеррористической комиссии	Монгуш Орлан Эрес-оолович
Главный специалист по информационной политике и СМИ	Маадыр-оол Айдысмаа Оруй-ооловна
Начальник отдела экономики, проектного управления и развития туризма	Донгак Херелмаа Шулду-Доржуевна

Приложение 4
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Состав комиссии по защите информации

Председатель комиссии	Ооржак Аржаан Никифорович
Члены комиссии	Монгуш Чодураа Когеловна
	Самбуу Аржана Николаевна
	Айыжы Айланмаа Константиновна
	Куулар Мерген-Херел Мергенович

Приложение 5
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных администрации Овюрского кожууна Республики Тыва.

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Определение класса защищенности информационных систем персональных данных администрации Овюрского кожууна Республики Тыва на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников администрации Овюрского кожууна Республики Тыва, участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются распоряжением председателя администрации Овюрского кожууна Республики Тыва.

3.4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников администрации Овюрского кожууна Республики Тыва, участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети администрации Овюрского кожууна Республики Тыва.

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Отчетность комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

Приложение 6
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

СОГЛАСИЕ
на обработку персональных данных

с. Хандагайты «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан_____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных _____
_____
(наименование и адрес оператора)

и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей _____
_____
_____
(цель обработки персональных данных)

и распространяется на следующую информацию: _____
_____
_____
_____
_____
_____,

полученных лично от меня для обработки и передачи в документальной и электронной форме в различные государственные органы власти, если этого требует законодательство Российской Федерации или Республики Тыва, а также третьим лицам _____
_____
_____
(наименование и адреса третьих лиц)

с целью исполнения обязательств представителя нанимателя в рамках трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления. Также не возражаю против обработки сведений обо мне, содержащих данные об имени, фамилии, отчестве, должности, телефонном номере и адресе электронной почты, полученных мною для их использования в служебных целях, в т. ч. размещения в государственных информационных системах, используемых в рамках обеспечения доступа к информации о деятельности администрации Овюрского кожууна Республики Тыва.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных с учетом федерального законодательства.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Примечание:

1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность субъекта персональных данных.
2. Письменное согласие заполняется и подписывается субъектом персональных данных собственноручно в присутствии должностного лица оператора.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

Приложение 7
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Разъяснение
субъекту персональных данных

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в администрации Овюрского кожууна Республики Тыва.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в администрации Овюрского кожууна Республики Тыва в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Приложение 8
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _______
(фамилия, имя, отчество полностью)

являясь работником администрации Овюрского кожууна Республики Тыва, в должности
_____
_____,
(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____	_____	_____
дата	подпись	расшифровка

Приложение 9
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

ЖУРНАЛ
учета средств криптографической защиты информации

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечания
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кот-рым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие	Номер акта или расписка Об уничтожении	

ЖУРНАЛ
учета согласий субъектов персональных данных

№ п/п	Дата и номер согласия	Ф.И.О. субъекта персональных данных

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатаци	Примечание

ЖУРНАЛ
учета ЭП

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

ЖУРНАЛ
учета выдачи паролей

№ п/п	Дата получения пароля	Ф.И.О. получателя	Подпись получателя

ЖУРНАЛ
антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответсвенного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение 10
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения _____

Место проведения _____

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих администрации Овюрского кожууна Республики Тыва.

1. Слушали: _____
доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:
Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

2. Слушали: _____
доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

Приложение 11
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн «Наименование» и класса защищенности ИС «Наименование»

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____2021 г.

АКТ

определения уровня защищенности ПДн при их обработке в ИСПДн «Наименование» и класса защищенности ИС «Наименование»

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение),

целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____2021 г.

Приложение 12
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

АКТ
Об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____ _____
(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____
подпись расшифровка

Члены комиссии: _____ _____
подпись расшифровка

_____ _____
подпись расшифровка

Приложение 13
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПОЛИТИКА
в отношении обработки персональных данных

1. Общие положения

1.1. Политика в отношении обработки персональных данных в администрации Овюрского кожууна Республики Тыва (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Конституцией Российской Федерации, Трудовым кодексом Российской Федерации.

1.2. Политика определяет порядок и условия обработки персональных данных в администрации Овюрского кожууна Республики Тыва (далее – Оператор) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в целях приема и регистрации обращений (или запросов) граждан, организаций и общественных объединений, поступивших в администрацию МО, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2. Основные понятия, используемые в настоящей Политике

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.10. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

4.1.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

5. Конфиденциальность персональных данных

5.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Право субъекта персональных данных на доступ к его персональным данным

6.1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их

блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в п. 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных

6.3. Сведения, указанные в п. 6.7 настоящей политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае, если сведения, указанные в п. 6.7 настоящей Политики, а также обрабатываемы персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемы персональные данные не были предоставлены ему для

ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.

6.6. Оператор в праве отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

6.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

6.7.1. Подтверждение факта обработки персональных данных Оператором;

6.7.2. Правовые основания и цели обработки персональных данных;

6.7.3. Цели и применяемые Оператором способы обработки персональных данных;

6.7.4. Наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

6.7.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.7.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

6.7.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7. Право на обжалование действий или бездействий Оператора

7.1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Обязанности Оператора при сборе персональных данных

8.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящей Политики.

8.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

8.3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных п. 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

8.3.1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;

8.3.2. Цель обработки персональных данных и ее правовое основание;

8.3.3. Предполагаемые пользователи персональных данных;

8.3.4. Установленные настоящим Федеральным законом права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:

8.4.1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;

8.4.2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

8.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

8.4.4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.

9. Меры направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»

9.1. Назначен ответственный за организацию обработки персональных данных.

9.2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.

9.4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых оператором мер.

9.5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

10. Меры по обеспечению безопасности персональных данных при их обработке

10.1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

10.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

10.4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.

10.5. Ведется учет машинных носителей персональных данных.

10.6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

10.7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

10.8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

Приложение 14
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

– Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

– Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

– Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

– Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

– Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 15
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– Подтверждение факта обработки персональных данных;

– Правовые основания и цели обработки персональных данных;

– Цели и применяемые оператором способы обработки персональных данных;

– Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);

– Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

– Сроки обработки персональных данных, в том числе сроки их хранения;

– Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для

раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его

представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

– Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

– В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

– Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

– Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 16
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

– Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

– Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

– Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

– Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

– Некорректного функционирования установленных на АРМ технических средств защиты;

– Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

– Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

– Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

– Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

– Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

– Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

– Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Приложение 17
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
ответственного за обеспечение
безопасности персональных данных в информационных системах
персональных данных

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн),

мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– Обязан проводить мероприятия по организации антивирусной защиты;

– Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– Установить причины, по которым стал возможным НСД;

– Установить последствия, к которым привел НСД;

– Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

– Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 18
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по организации резервирования

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

– Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

– Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

– Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

– Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств

защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

Приложение 19
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

– Длина пароля должна быть не менее 8 символов;

– В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– При смене пароля новое значение должно отличаться от предыдущих;

– Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

Приложение 20
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

2. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

– Приостановить работу в ИСПДн;

– Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

– Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– Провести лечение или уничтожение зараженных файлов.

3. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 21
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по проверке электронного журнала обращений к информационной системе персональных данных

1. Задачи проверки.

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

– Контролирование состояния защищенности системы;

– Выявление причин произошедших изменений;

– Определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

– Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2. Журналы записей о событиях.

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

– Штатные журналы операционной системы Windows;

– Журналы событий средств защиты информации.

3. Штатные журналы операционной систем.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

– Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

– Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

– Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

4. Журнал событий средств защиты информации.

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

5. Аудит.

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

6. Просмотр событий электронных журналов.

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

Приложение 22
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например,

утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение 23
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в администрации Овюрского кожууна Республики Тыва требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.

3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

4. Плановые проверки проводятся не чаще чем один раз в три месяца.

5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

6. Основанием для проведения проверки служит издание приказа «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

– соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;

– соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

– отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

– порядок и условия применения средств защиты информации;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих полномочий;

– требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес председателя администрации результаты проведения проверки в форме служебной записки.

Приложение 24
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по обращению с криптосредствами

1. Общие положения

Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, передачи клиентам, а также порядок допуска к работам с шифровальными средствами.

Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа.

Разработка и проведение мероприятий по обеспечению безопасности при работе с СКЗИ осуществляется ответственным за эксплуатацию СКЗИ.

Работы с СКЗИ должны проводиться с учетом Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Требования по размещению, оборудованию и охране помещений

Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем лиц, допущенных в кабинеты.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Для предотвращения просмотра извне окна помещений должны быть защищены (жалюзи, шторы и т.п.).

3. Порядок обращения с СКЗИ

Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать установки ключевых документов в другие ПЭВМ.

Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в журнале установленной формы (Приложение). Ведет журналы администратор информационной безопасности.

Единицей поэкземплярного учета СКЗИ является:

- для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;
- для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности при обращении с СКЗИ.

Ответственным за эксплуатацию СКЗИ периодически должен проводиться контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов.

4.Ответственность за нарушение требований Инструкции

За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную, либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Приложение 25
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в администрации Овюрского кожууна Республики Тыва, или сотруднику (далее – субъекту персональных данных) администрации Овюрского кожууна Республики Тыва.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники администрации Овюрского кожууна Республики Тыва или лица, осуществляющие такую обработку по договору с администрации Овюрского кожууна Республики Тыва), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется в администрации Овюрского кожууна Республики Тыва без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами администрации Овюрского кожууна Республики Тыва.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

− типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

− типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

− типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения администрации Овюрского кожууна Республики Тыва или в иных аналогичных целях, должны соблюдаться следующие условия:

− необходимость ведения такого журнала должна быть предусмотрена актом администрации Овюрского кожууна Республики Тыва, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

− копирование содержащейся в таких журналах информации не допускается;

− персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

1. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Приложение 26
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПРАВИЛА
работы с обезличенными данными

1.Общие положения

Настоящие Правила работы с обезличенными персональными данными администрации Овюрского кожууна Республики Тыва разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными администрации Овюрского кожууна Республики Тыва.

2.Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
- обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3.Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации Овюрского кожууна Республики Тыва и

по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

2. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Приложение 27
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в администрации Овюрского кожууна Республики Тыва возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем администрации Овюрского кожууна Республики Тыва) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для администрации Овюрского кожууна Республики Тыва и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных

данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных председателем администрации Овюрского кожууна Республики Тыва накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами администрации Овюрского кожууна Республики Тыва, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов администрации Овюрского кожууна Республики Тыва, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение 28
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в администрации Овюрского кожууна Республики Тыва назначается Председателем администрации.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в администрации Овюрского кожууна Республики Тыва.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 29
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПЛАН
мероприятий по защите информации в администрации Овюрского кожууна Республики Тыва

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах персональных данных администрации Овюрского кожууна Республики Тыва.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИСПДн.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- периодичность мероприятия (разовое/периодическое);
- исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных администрации Овюрского кожууна Республики Тыва.

План мероприятий по защите информации в 2021г.

Мероприятие	Периодичность	Ответственные исполнители
Организационные мероприятия		
Обследование информационных систем	Разовое срок до 15.04.2021г.	Айыжы А.К., Куулар М-Х.М.
Определение перечня ИСПДн	Разовое срок до 15.04.2021г.	Куулар М-Х.М.
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до 15.04.2021г.	Айыжы А.К., Куулар М-Х.М.
Определение круга лиц, участвующих в обработке ПДн	Разовое срок до 15.04.2021г.	Куулар М-Х.М. , Айыжы А.К.
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до 15.04.2021г.	Айыжы А.К., Куулар М-Х.М.
Назначение ответственного за обеспечение безопасности ПДн	Разовое срок до 15.04.2021г.	Айыжы А.К..
Классификация всех выявленных ИСПДн	Разовое срок до 15.04.2021г.	Куулар М-Х.М.
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое срок до 15.04.2021г.	Айыжы А.К.
Организация порядка резервного копирования защищаемой информации на твердые носители	Разовое срок до 15.04.2021г.	Куулар М-Х.М.
Организация информирования сотрудников о порядке обработки ПДн и их обучения	Разовое срок до 15.05.2021г	Куулар М-Х.М. , Айыжы А.К.
Организация информирования сотрудников о введенном режиме защиты ПДн	Разовое срок до 15.05.2021г	Айыжы А.К.
Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн	Разовое срок до 15.05.2021г	Айыжы А.К.
Физические мероприятия		
Установление границ контролируемой зоны ИСПДн	Разовое срок до 15.05.2021г	Айыжы А.К.

Мероприятие	Периодичность	Ответственные исполнители
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до 15.05.2021г	Айыжы А.К.
Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания	Разовое срок до 15.05.2021г	Айыжы А.К.
Технические мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета	Разовое срок до 15.12.2021г.	Куулар М-Х.М.
Внедрение межсетевого экранирования	Разовое срок до 15.12.2021г.	Куулар М-Х.М.
Внедрение криптографической защиты	Разовое срок до 15.12.2021г.	Куулар М-Х.М.
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Еженедельно	Куулар М-Х.М. , Айыжы А.К.
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	Куулар М-Х.М. , Айыжы А.К.
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Куулар М-Х.М.
Контроль за обеспечением резервного копирования	Ежемесячно	Айыжы А.К., Куулар М-Х.М.
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Куулар М-Х.М. , Айыжы А.К.
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Куулар М-Х.М., Айыжы А.К.

Приложение 30
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ПЕРЕЧЕНЬ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМАХ АДМИНИСТРАЦИИ ОВЮРСКОГО 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ОБРАБОТКИ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ АДМИНИСТРАЦИИ ОВЮРСКОГО КОЖУУНА РЕСПУБЛИКИ ТЫВА»

2021 г.

1. 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, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

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.

12. НАЗНАЧЕНИЕ ГИС «ЛВС АДМИНИСТРАЦИИ ОВЮРСКОГО КОЖУУНА РТ»

2.1. ГИС «ЛВС Администрации Овюрского кожууна РТ» предназначена для реализации полномочий администрации Овюрского кожууна Республики Тыва (далее – администрации ОВЮРСКОГО кожууна РТ), для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации ОВЮРСКОГО 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 Овюрского кожууна РТ» может включать в себя ресурсы и предоставлять их другим лицам на основе договоров об информационном взаимодействии в соответствии с действующим законодательством.

2.2. Информация конфиденциального характера, обрабатываемая в ГИС «ЛВС Администрации Овюрского кожууна РТ» в Организации, используется при решении следующих основных задач:

– обеспечение реализации полномочий председателя администрации Овюрского кожууна Республики Тыва и для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации Овюрского 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 Овюрского кожууна Республики Тыва и для обеспечения доступа пользователей – муниципальных служащих структурных подразделений администрации Овюрского кожууна РТ, подведомственных учреждений иных возложенных на него федеральным и республиканским законодательством полномочий.

3. РАСПОЛОЖЕНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. ГИС «ЛВС Администрации Овюрского кожууна РТ» расположена по адресу:

– Юридический адрес: 668130, Республика Тыва, Овюрский района, с. Хандагайты, ул. Ленина, д.2;

– Юридический адрес: 668130, Республика Тыва, Овюрский района, с. Хандагайты, ул. Ленина, д.2;

–

3.2. 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 Овюрского кожууна РТ, в которых осуществляется обработка конфиденциальной информации.

3.3. Доступ сотрудников и других лиц в помещения администрации Овюрского кожууна РТ осуществляется в соответствии с утвержденным списком лиц, имеющих доступ в данное помещение.

4. ОПИСАНИЕ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ ОБЪЕКТА

4.1. Структура администрации Овюрского кожууна РТ является иерархической. Организационная структура администрации Овюрского кожууна РТ представлена на рисунке 1.

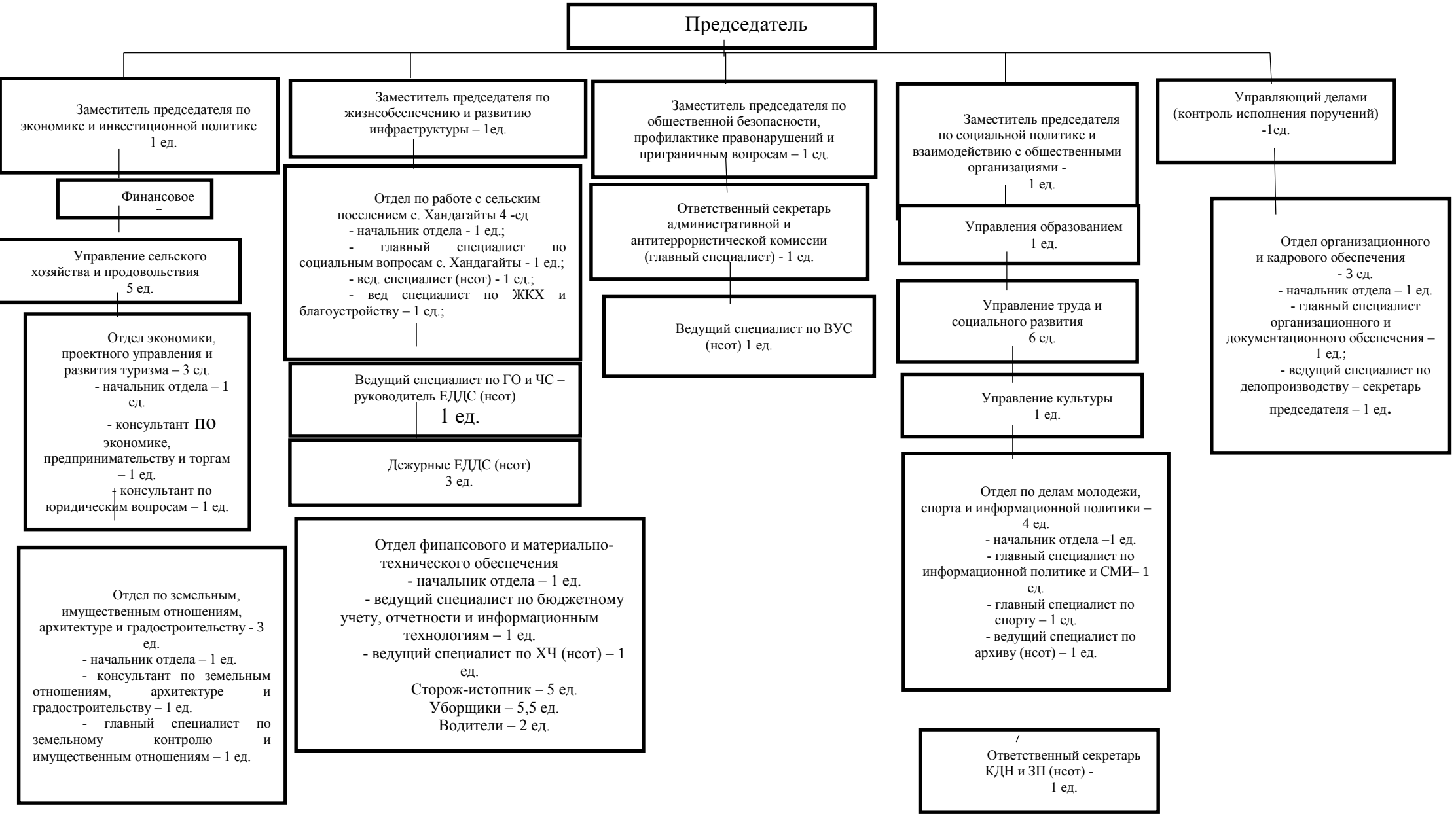
5. ПЕРЕЧЕНЬ ПОДСИСТЕМ ГИС «ЛВС АДМИНИСТРАЦИИ ОВЮРСКОГО КОЖУУНА РТ»

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

Таблица 1. – Перечень подсистем ГИС «ЛВС администрации Овюрского кожууна РТ»

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

Структура администрации муниципального района «Овюрский кожуун» Республики Тыва
Утверждена решением Хурала представителей Овюрского кожууна от 28.12.2020 г. №37



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
2. 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 Овюрского кожууна РТ» своими силами.

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

Ввод конфиденциальной информации в подсистеме ГИС «ЛВС администрации Овюрского кожууна РТ» с использованием внешних устройств типа сканеров и т. п. не предусмотрен.

На учтенном внешнем flash-накопителе («Т_____», 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 Овюрского кожууна РТ» к ресурсам выполняется только администратором подсистем ГИС «ЛВС администрации Овюрского кожууна РТ».

Каждый пользователь подсистем ГИС «ЛВС администрации Овюрского 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 вручную 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, 2.

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 производителя. 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, 2, 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 Овюрского 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 Овюрского 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, MAC- адресам) устройства;

– или по комбинации имени, логического и (или) физического адресов устройства.

1.6 Аутентификация устройств в информационной системе обеспечивается с использованием:

– соответствующих протоколов аутентификации;

– с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

1.7 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.

2. 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).

3. 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.

4. 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).

5. 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.

6. 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.

6.6 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.

7. 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 неправомерного 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 вовремя, 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.

8. 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.

9. 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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

1.1. 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 Овюрского кожууна и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1. 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 Овюрского 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 Овюрского 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 Овюрского 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 Овюрского кожууна. Для каждого внутреннего пользователя в ИС администрации Овюрского кожууна должны быть заведены учетные записи.

2.2. Пользователи ИС администрации Овюрского 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 Овюрского кожууна.

2.3. Аутентификация пользователя в администрации Овюрского кожууна осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

2.4. В Программах обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

2.5. 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).

3. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

3.1. В Программах до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация устройств (технических средств).

3.2. Идентификации и аутентификации до начала информационного взаимодействия подлежат следующие типы устройств:

- АРМ пользователя;
- Серверы;
- Ноутбуки;
- Тонкие клиенты;
- Принтер;
- Сканер.

3.3. 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, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства. Аутентификация устройств в ИС администрации Овюрского кожууна обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

4. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

4.1. В ИС администрации Овюрского 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.

4.2. В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ.

5. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

5.1. В ИС администрации Овюрского 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 Овюрского 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 неправомерного доступа к ней и модифицирования.

5.2. В случае компрометации личного пароля пользователя ИС администрации Овюрского кожууна должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- Внеплановая смена личного пароля или удаление учетной записи пользователя ИС администрации Овюрского 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 Овюрского кожууна.

5.3. 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.

6. Защита обратной связи при вводе аутентификационной информации

6.1. В ИС администрации Овюрского кожууна осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

6.2. 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.

7. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре (при наличии)

7.1. В ИС администрации Овюрского 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 неправомерного 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. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с настоящими Правилами.

8. Ответственность при организации идентификации и аутентификации

8.1. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ.

8.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ и пользователей администрации Овюрского кожууна.

8.3. 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
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

Приложение 34
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 Овюрского кожууна

1.1 Настоящее Положение определяет правила управления доступом субъектов доступа к объектам доступа в государственной информационной системе 1С: Бухгалтерия администрации Овюрского 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 (___).

1.2 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения в государственной информационной системах администрации Овюрского кожууна

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие правила регламентируют процесс установки (инсталляции) программного обеспечения вычислительной техники в администрации Овюрского кожууна.

1.2. Настоящие правила и процедуры управления установкой (инсталляцией) программного обеспечения обязательны для соблюдения работниками администрации Овюрского 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.

3. УСТАНОВКА (ИНСТАЛЛЯЦИЯ) ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И (ИЛИ) ЕГО КОМПОНЕНТОВ

3.1. Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов осуществляется только от имени администратора.

3.2. 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.

3.3. В администрации Овюрского 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.

3.4.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.

3.5. 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 Овюрского 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 Овюрского 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 распоряжению № ___ от «___» _____ 20__ г. «Об организации обработки персональных данных в государственной информационной системе администрации Овюрского кожууна

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

№ п/п	Программное обеспечение	Издатель	Наименование сегмента ГИС
1			
2			
3			

Приложение 36
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

ИНСТРУКЦИЯ
по модификации и техническому обслуживанию программного обеспечения и аппаратных средств государственной информационных системах администрации Овюрского 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 Овюрского кожууна.

1.1. 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 Овюрского кожууна.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников структурных подразделений Организации, использующих в работе государственных информационных систем администрации Овюрского кожууна, в которой осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

1.3. Сотрудники администрации Овюрского кожууна, задействованные в обеспечении функционирования ГИС администрации Овюрского кожууна, знакомятся с основными положениями Инструкции в части, их касающейся, по мере необходимости.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ

2.1. Все изменения конфигурации технических и программных средств АРМ администрации Овюрского кожууна должны производиться только на основании заявок руководителей структурных подразделений Организации (Приложение № 1), согласованных с руководителем администрации Овюрского кожууна. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения.

2.2. 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.

2.3. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ГИС Организации предоставляется Администратору ИБ, а также ответственному лицу за защиту ПДн.

2.4. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме Администратора ИБ и/или ответственного лица за защиту ПДн, запрещено.

2.5. Установка и настройка программного средства осуществляется администратором ГИС согласно эксплуатационной документации.

2.6. Руководители структурных подразделений осуществляют контроль за отсутствием на АРМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.7. 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 Овюрского кожууна.

2.8. 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 Овюрского кожууна»

2.9. 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.

2.10. 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.

2.11. После завершения работ по внесению изменений в состав аппаратных средств, защищенных АРМ системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) Администратором ИБ ГИС.

2.12. 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.

2.13. 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.

3. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

3.1. Инструкция подлежит пересмотру при изменении перечня решаемых задач, состава технических и программных средств ГИС администрации Овюрского кожууна, приводящих к существенным изменениям технологии обработки информации.

3.2. Пересмотр Настоящей инструкции проводится <ответственным лицом > с целью проверки соответствия положений настоящей Инструкции реальным условиям применения их в ГИС администрации Овюрского кожууна.

3.3. Вносимые изменения не должны противоречить другим положениям Инструкции.

4. ОТВЕТСТВЕННОСТЬ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

4.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Организации.

4.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на Администратора ИБ ГИС.

4.3. 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 Овюрского 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 Овюрского 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 Овюрского 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 Овюрского 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.

8.10 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.

8.11 Запрещается предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.

Приложение 38
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

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:

5.1. 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 Овюрского 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 Овюрского 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 Овюрского 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 Овюрского 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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								

Приложение 41
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 распоряжению № __ от «___» _____ 20__ г.
«Об утверждении границ контролируемой зоны»

1. Граница контролируемой зоны: отдел по земельным, имущественным отношениям, архитектуре и градостроительству 2 этаж, с. Хандагайты, ул. Ленина д.2 (**ТЕХНОКАД ОТНОСИТЕЛЬНО ГРАНИЦ КОНТРОЛИРУЕМОЙ ЗОНЫ**)
2. Граница контролируемой зоны: отдел финансового и материально-технического обеспечения 3 этаж, с. Хандагайты, ул. Ленина д.2 **(СИСТЕМЫ 1С: БУХГАЛТЕРИЯ, ЗАРПЛАТА И КАДРЫ, СУФД, ЕДИНЫЙ ПОРТАЛ БЮДЖЕТНОЙ СИСТЕМЫ, ГИС ГМП, SPU-ORB, НАЛОГОПЛАТЕЛЬЩИК ЮЛ, КОНТУР-ЭКСТЕРН, WEB-КОНСОЛИДАЦИЯ,ФСС (ЛИЧНЫЙ КАБИНЕТ))**

Приложение 42
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Список должностей, лиц, допущенных (имеющих доступ) в помещения Администрации Овюрского 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 Овюрского 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 Овюрского 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 Овюрского кожууна, имеющими постоянный доступ в помещения.
3. Ремонтные, наладочные и другие виды работ осуществляются только в присутствии сотрудников Администрации Овюрского кожууна, имеющих постоянный доступ в помещения.

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

Перечень должностей лиц, допущенных (имеющих доступ) в помещения Администрации Овюрского 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	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
Овюрского кожууна
от 15 апреля 2021 г. № 105

Правила доступа в помещения администрации Овюрского кожууна в рабочее и нерабочее время, а также в нештатных ситуациях

1. Общие положения

1.1. Настоящие Правила устанавливают условия и порядок осуществления доступа в помещения администрации Овюрского 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.

1.2. 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».

1.3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

1.4. 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

2.1. Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень должностей лиц, допущенных (имеющих доступ) в помещения администрации Овюрского кожууна, в которых ведется обработка конфиденциальной информации, утвержденный администрацией Овюрского кожууна.

2.2. В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок, подписанных руководителем подразделения или лицами допущенных (имеющих доступ) в помещения.

2.3. Допуск лиц, не указанных в «Перечне должностей лиц, допущенных (имеющих доступ) в помещения, в которых ведется обработка конфиденциальной информации»,

осуществляется сотрудниками администрации Овюрского кожууна, имеющими постоянный доступ в помещения администрации Овюрского кожууна.

2.4. Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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.

2.10. Уборка помещений, в которых ведется обработка конфиденциальной информации и хранятся документы и носители защищаемой информации, должна производиться в присутствии сотрудников администрации Овюрского кожууна.

2.11. Установка оборудования, его замена или ремонт в защищаемых помещениях должны проводиться по согласованию с лицом, ответственным за проведение соответствующих работ (установку оборудования) в администрации Овюрского кожууна.

2.12. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителю подразделения администрации Овюрского кожууна.

2.13. 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

Журнал учета сейфов, металлических шкафов, специальных хранилищ и ключей от них администрации Овюрского 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.)
3								
…								
№								

Приложение 45
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Журнал
поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов
администрации Овюрского 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 получены	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	
	2	3	4	5	6	7	8	9	10	11	12	13	14	15

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	

Приложение 46
к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Журнал
ознакомления работников администрации Овюрского 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					
…					
№					
2. **Наименование документа, реквизиты**					
1					
2					

№ п/п	ФИО работника	Должность	Структурное подразделение	Дата ознакомления	Подпись
3					
…					
№					
…					

Приложение 47

к распоряжению председателя
администрации
Овюрского кожууна
от 15 апреля 2021 г. № 105

Журнал
инструктажа сотрудников администрации Овюрского 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

Матрица доступа к сведениям конфиденциального характера, обрабатываемым в администрации Овюрского 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 2, 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 2, 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
Овюрского кожууна
от 15 апреля 2021 г. № 105

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 Овюрского 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 Овюрского 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 Овюрского кожууна и подведомственных организациях администрации Овюрского кожууна;

– методическую помощь всем работникам администрации Овюрского кожууна и подведомственных организациях администрации Овюрского 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 Овюрского кожууна и подведомственных организациях администрации Овюрского 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 Овюрского 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 Овюрского кожууна и подведомственных организациях администрации Овюрского 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 Овюрского кожууна и подведомственных организациях администрации Овюрского 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.