|  |
| --- |
| «УТВЕРЖДАЮ»Глава Ардатовскогомуниципального района РМА.Н. Антипов «\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_ г. |

**Регламент**

**доступа в помещения с компонентами СКЗИ, обеспечивающими безопасность персональных данных при их обработке в информационных системах администрации**

**Ардатовского муниципального района РМ**

1. **Общие положения**
	1. Настоящий Регламент определяет порядок доступа в помещения, с элементами (АРМ, серверы, сетевое оборудование и т.п.) информационных систем администрации Ардатовского муниципального района РМ (далее – Учреждение), в которых ведется обработка ПДн с использованием компонентов криптосредств (криптографически опасная информация, средства криптографической защиты информации, ключевая и парольная информация) обеспечивающих безопасность хранения, обработки и передачи по каналам связи информации ограниченного распространения.
	2. Выполнение требований настоящего Регламента обязательно для всех сотрудников Учреждения, осуществляющих свою деятельность с использованием криптосредств.
	3. В целях закрепления знаний по вопросам практического исполнения требований Регламента, разъяснения возникающих вопросов ответственным за организацию эксплуатации, обслуживание, хранение СКЗИ, материальных носителей, документации СКЗИ (далее – Ответственный за эксплуатацию СКЗИ) и обеспечения безопасности СКЗИ проводятся семинары (не реже 1 раз в год) и/или персональные инструктажи сотрудников (при необходимости).
	4. Пользователи СКЗИ, назначенные постановлением («Об организации режима криптографической защиты» № 441 от «28» \_08\_2017 г.) имеют свободный доступ в помещения с элементами СКЗИ.
	5. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения. Обучение Пользователей правилам работы с СКЗИ осуществляет ответственный за эксплуатацию СКЗИ.
	6. Ознакомление с требованиями настоящего Регламента ответственный за эксплуатацию СКЗИ проводит под роспись с выдачей электронных копий соответствующих приложений и разделов Регламента непосредственно для повседневного использования в работе.
2. **Организация охранного режима помещений, в которых установлены СКЗИ или хранятся криптографические ключи**
	1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи (далее – режимные помещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.
	2. При обустройстве режимных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.
	3. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.
	4. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.
	5. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также визуальное наблюдение посторонними лицами за проведением работ в помещении.
	6. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает главный врач. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящего Регламента.
	7. Двери режимных помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в специальном сейфе.
	8. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.
	9. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным. Исправность сигнализации периодически необходимо проверять с отметкой в соответствующих журналах.
	10. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ или пользователя, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в специальном сейфе. Дубликат ключа от хранилища ответственного за эксплуатацию СКЗИ в опечатанной упаковке должен быть передан на хранение должностному лицу, назначенному главный врачом.
	11. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей, ответственных за эти хранилища.
	12. В обычных условиях режимные помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями или ответственным за эксплуатацию СКЗИ.
	13. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию СКЗИ. Ответственный за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствий компрометации криптографических ключей и к их замене.
	14. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптографических ключей осуществляются только в отсутствие лиц, не допущенных к работе с данными СКЗИ.
	15. На время отсутствия пользователей, необходимое оборудование при наличии технической возможности, должно быть выключено, отключено от линии связи. В противном случае по согласованию с ответственным за эксплуатацию СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в отсутствие пользователей.
3. **Режим при обслуживании и ремонте режимных помещений**
	1. Обслуживание режимных помещений (уборка или различный ремонт помещения, инженерно-технического оборудования) проводится обслуживающим персоналом только в присутствии и под присмотром хотя бы одного из сотрудников, имеющих право самостоятельного доступа в режимное помещении.
	2. Механические или электронные ключи от замков дверей режимных помещений обслуживающему персоналу и/или другим лицам, не имеющим права самостоятельно находиться в помещении, выдаются только с письменного согласия ответственного за эксплуатацию СКЗИ.
	3. Сотрудники подразделения, обеспечивающие контроль действий обслуживающего персонала в режимных помещениях, обязаны не допускать несанкционированных действий в отношении компонентов криптосредств.
	4. Капитальный и/или иной ремонт, продолжительный по времени и требующий высвобождения рабочей площади режимных помещений, может проводиться и без присмотра, однако при этом в обязательном порядке должны выполняться следующие условия:
	* компоненты криптосредств, должны быть вынесены из ремонтируемого помещения в другое контролируемое помещение;
	* по окончании ремонта должны быть сменены ключи и коды доступа в помещение (организовывает и контролирует исполнение ответственным за эксплуатацию СКЗИ).
4. **Смена кодов и ключей**
	1. При утере основного или запасного комплекта ключей доступа в режимное помещение директор совместно с ответственным за организацию эксплуатации СКЗИ, инициирует служебное расследование, по результатам которого принимается решение или об изготовлении дополнительного комплекта или о смене секрета замка и, соответственно, замене всех комплектов ключей на новые.
	2. Смена кодов доступа и секретов замков в помещениях организуется в следующих случаях:
* увольнение или перемещение из состава подразделения сотрудника, знавшего код доступа в помещение или имеющего доступ к ключам доступа;
* преднамеренное или непреднамеренное разглашение кода доступа в помещения тем лицам, у которых нет производственной необходимости его знать;
* установленный факт бесконтрольного нахождения в помещении лиц, у которых нет производственной необходимости знать код доступа или иметь ключи доступа;
* истечение одного календарного года с момента первичного ввода или последней смены значения кода доступа.
	1. Смена секретов механических замков и/или кодов доступа электромеханических замков производится с оформлением акта, который доводится под роспись до всех сотрудников, имеющих право самостоятельно находиться в данном помещении. Коды доступа доводятся до сотрудников ответственным за эксплуатацию СКЗИ, как правило, устно, с практической демонстрацией правильности работы устройств разграничения и/или контроля доступа. При необходимости код доступа записывается на бумаге, которая при этом оформляется как парольная карта.
1. **Ответственность**
	1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.
	2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам доступа в помещения с элементами ИС, в которых ведется обработка ПДн с использованием компонентов криптосредств возлагается на ответственного за эксплуатацию СКЗИ.
	3. Ответственность за своевременное доведение настоящего Регламента до сотрудников в части их компетенции и обеспечение условий для выполнения требований данного Регламента возлагается на ответственного за эксплуатацию СКЗИ. Ответственность за организацию (полноту и своевременность) материально-технического обеспечения помещений и сотрудников подразделения несет руководитель аппарата администрации управляющий делами А.Н. Антипов
	4. Ответственность за соблюдение требований настоящего Регламента возлагается на сотрудников подразделений.
	5. Ответственный за общее руководство обеспечения безопасности ПДн, орган криптографической защиты и ответственный за эксплуатацию СКЗИ проводят текущий контроль выполнения сотрудниками подразделений требований настоящего Регламента.
	6. В случае неисполнения или ненадлежащего выполнения требований настоящего Регламента пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.

|  |  |
| --- | --- |
| С регламентом ознакомлен(а): |  |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | подпись расшифровка |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | подпись расшифровка |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | подпись расшифровка |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | подпись расшифровка |