**ГЛАВА КРЫЛОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**КИРОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**ПРИМОРСКОГО КРАЯ**

**РАСПОРЯЖЕНИЕ**

**28.05.2021 с. Крыловка № 08 -од**

**Об организации контролируемой зоны**

В целях исполнения Приказа ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (мер ЗТС.2 и ЗТС.3)

1. Определить контролируемую зону по периметрам помещений (кабинетов), в которых производится обработка защищаемой информации.
2. Схемы помещений и расположение основных технических средств и систем относительно их границ зафиксировать в технических паспортах на информационные системы.
3. Утвердить прилагаемое положение «О контролируемой зоне».
4. Контроль за исполнением настоящего распоряжения оставляю за собой.

|  |  |  |
| --- | --- | --- |
| Глава Крыловского сельского поселения |  | И.С. Ахременко |

УТВЕРЖДЕНА

распоряжением администрации Крыловского сельского поселения

от «28» мая 2021г. № 08-од

**Положение о контролируемой зоне в** администрация Крыловского сельского поселения

1. ОБЩИЕ ПОЛОЖЕНИЯ
	1. Под контролируемой зоной (далее – КЗ) понимается территория, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.
	2. Схема контролируемой зоны фиксируются в техническом паспорте на информационную систему. Администратор безопасности (далее – Администратор) обеспечивает актуальность приведенной в технических паспортах информации.
2. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

Допуск в охраняемые помещения осуществляется в соответствии с утвержденным в администрации Крыловского сельского поселения документом «Перечень помещений, в которых разрешена работа с ресурсами сегмента ГИС «Автоматизированная информационная система архивной службы Приморского края» (далее - ГИС), в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения» (Приложение № 4 к Политике информационной безопасности в администрация Крыловского сельского поселения).

* 1. Сотрудникам, которым необходим временный доступ в помещения, к которым у них нет допуска, может быть предоставлен такой доступ, но только в присутствии сотрудников, работающих в этом помещении (имеющих доступ в это помещение).
	2. При покидании помещения и при отсутствии в нем других лиц, допущенных в это помещение, сотрудник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.
	3. Перед началом рабочего дня помещения снимаются с охраны. После окончания рабочего дня, помещения устанавливаются под охрану в соответствии с установленным в разделе 3 настоящего положения порядком.
	4. Нахождение посторонних лиц в помещениях, в которых осуществляется обработка защищаемой информации, допускается только в присутствии сотрудников, работающих в данном помещении и при условии соблюдения правил ограничения доступа к обрабатываемой информации.
1. ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ
	1. Закрытие помещений, в которых обрабатывается защищаемая информация, осуществляется по окончании рабочего дня последним сотрудником, покидающим помещение. Закрытие помещения осуществляется после проведения в нем уборки, обесточивания оборудования, запирания сейфов, закрытия окон.
	2. При вскрытии помещения, допущенные в него сотрудники осуществляют осмотр на предмет выявления признаков несанкционированных действий в помещении в их отсутствие (повреждения дверей, повреждения пломб, изменение местоположения мебели, включенная техника и т. п.). При отсутствии нарушений, помещение считается снятым с охраны.
	3. В случае обнаружения нарушений, сотрудник сообщает об этом Администратору, который в свою очередь созывает группу реагирования на инциденты информационной безопасности (далее – ГРИИБ). Далее ГРИИБ действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
2. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ
	1. Настоящее положение может быть изменено и дополнено по следующим причинам:
* появление информации о новых угрозах безопасности информации, связанных с физическим доступом к техническим средствам информационных систем;
* при возникновении инцидентов информационной безопасности, связанных с физическим доступом, извлечения из них уроков и понимания необходимости пересмотра настоящего положения;
* при изменении законодательства в сфере защиты информации.
	1. За нарушение настоящего положения, сотрудники могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.