-

**АДМИНИСТРАЦИЯ АНУЧИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
 ПРИМОРСКОГО КРАЯ**

 Р А С П О Р Я Ж Е Н И Е

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  16.12.2020 г. |  |  с. Анучино | № |  136 - р  |

|  |
| --- |
| **Об организации контролируемой зоны** |

В целях исполнения Приказа ФСТЭК России от 11 февраля 2013 г.
№ 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 возложить на Первого заместителя главы администрации Анучинского муниципального округа (Янчук).

Глава Анучинского

муниципального округа С.А. Понуровский

УТВЕРЖДЕНА

распоряжением Администрации

Анучинского муниципального округа

Приморского края

от «16» декабря 2020г. № 136-р

**Положение о контролируемой зоне в администрации
Анучинского муниципального округа Приморского края**

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 ПОМЕЩЕНИЯ
	1. Допуск в помещения осуществляется в соответствии с утвержденным в Администрации Анучинского муниципального округа Приморского края документом «Перечень помещений, в которых разрешена работа с ресурсами государственной информационной системы (далее – ГИС), в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения».
	2. Помещения, в которых осуществляется обработка защищаемой информации, оборудованы пожарной сигнализациями, а также прочными дверьми с механическими замками.
	3. Ключи от помещений выдаются и находятся на ответственном хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей.
	4. 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).
	5. При выходе из 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.
	6. 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.
3. ПОРЯДОК ЗАКРЫТИЯ ПОМЕЩЕНИЙ ПО ОКОНЧАНИЮ РАБОЧЕГО ДНЯ
	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, изменение местоположения мебели, включенная техника и т. п.).
	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.
4. 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.