

Положение о контролируемой зоне в МБОУ «СОШ №15» с. Кронштадтка

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Под контролируемой зоной (далее – КЗ) понимается территория, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.
- 1.2. Схемы контролируемой зоны фиксируются в технических паспортах на информационные системы. Администратор информационной безопасности (далее – Администратор) обеспечивает актуальность приведенной в технических паспортах информации.
- 1.3. Охраной помещений во внерабочее время занимается штатный сторож.

2. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

- 2.1. Допуск в охраняемые помещения осуществляется в соответствии с утвержденным в МБОУ «СОШ №15» с. Кронштадтка документом «Перечень помещений, в которых разрешена работа с ресурсами ГИС «ФРДО», в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения» (Приложение № 4 к Политике информационной безопасности в МБОУ «СОШ №15» с. Кронштадтка).
- 2.2. Помещение, в котором осуществляется обработка защищаемой информации, оборудованы пожарной сигнализацией, а также прочными дверьми с механическими замками. На входе в здание пропускной режим с отметкой в журнале посетителей.
- 2.3. Ключи от помещений выдаются и находятся на ответственном хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей.
- 2.4. 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).
- 2.5. 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.

- 2.6. 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.
- 2.7. Нахождение посторонних лиц (в том числе учащихся) 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 ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

- 3.1. 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, запираания сейфов, закрытия окон.
- 3.2. После запираания помещения на ключ, помещение считается принятым под охрану.
- 3.3. 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.
- 3.4. В случае обнаружения нарушений, сотрудник сообщает об этом Администратору, который в свою очередь создает группу реагирования на инциденты информационной безопасности (далее – ГРИИБ). Далее ГРИИБ действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

- 4.1. 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.
- 4.2. За нарушение настоящего положения, сотрудники могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.