АДМИНИСТРАЦИЯ ГОРОДА КОВРОВА
ВЛАДИМИРСКОЙ ОБЛАСТИ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ

П Р И К А З

«11» ноября 2022 г. № 435

Ковров

Об организации контролируемой зоны в управлении образования администрации города Коврова

В целях исполнения требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России от 11.02.2013 № 17, в части мер ЗТС.2 и ЗТС.3 **приказываю**:

1. Определить контролируемую зону в управлении образования администрации города Коврова (далее – управление образования) по периметрам помещений (кабинетов), в которых производится обработка защищаемой информации управления образования (в том числе персональные данные).
2. Утвердить прилагаемое положение «О контролируемой зоне в управлении образования администрации города Коврова» согласно приложению к настоящему приказу.
3. Контроль исполнения настоящего приказа возложить на заведующего отдела организационной и кадровой работы управления образования Ежикову Е.Н.

Начальник управления С.Г. Павлюк

Приложение
к приказу управления образования
от «11» ноября 2022 № 735

Положение о контролируемой зоне в управлении образования администрации города Коврова

1. Общие положения

1.1. Под контролируемой зоной (далее – КЗ) понимается территория управления образования администрации города Коврова (далее – управление образования), на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска к защищаемой информации управления образования (в том числе персональных данных (далее – ПДн)).

1.2. Перечень помещений (кабинетов) управления образования, входящие в состав контролируемой зоны, фиксируются в приказах управления образования об утверждении документов по защите информации, о допуске лиц, осуществляющих обработку ПДн без использования средств автоматизации, и допуске лиц, имеющих право доступа и вскрытия помещений управления образования, где хранятся средства криптографической защиты информации (далее – СКЗИ). Администраторы информационной безопасности (далее – АИБ) обеспечивают актуальность приведенной в вышеуказанных документах информации.

1.3. Охраной помещений во внерабочее время занимается штатные вахтеры.

2. Порядок доступа и сдачи под охрану охраняемых помещений управления образования, в которых осуществляется обработка защищаемой информации управления образования, в том числе ПДн.

2.1. Допуск в охраняемые помещения управления образования осуществляется в соответствии с приказами управления образования об утверждении документов по защите информации, о допуске лиц, осуществляющих обработку ПДн без использования средств автоматизации, и допуске лиц, имеющих право доступа и вскрытия помещений управления образования, где хранятся СКЗИ.

2.2. Помещения, в которых осуществляется обработка защищаемой информации управления образования, в том числе ПДн, оборудованы пожарной сигнализациями, а также дверьми с механическими замками.

2.3. Ключи от помещений выдаются и находятся на ответственном хранении у работников управления образования, которым необходим доступ в эти помещения для выполнения своих должностных обязанностей.

2.4. Работникам управления образования, 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, работник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.

2.6. Нахождение посторонних лиц в помещениях, в которых осуществляется обработка защищаемой информации управления образования, допускается только в присутствии сотрудников, работающих в данном помещении и при условии соблюдения правил ограничения доступа к обрабатываемой информации.

2.7. Закрытие помещений, в которых обрабатывается защищаемая информация, осуществляется по окончании рабочего дня последним работником, покидающим помещение. Закрытие помещения осуществляется после проведения в нем уборки, обесточивания оборудования, запирания сейфов, закрытия окон.

2.8. После запирания помещения на ключ и сдачи ключа от помещения под роспись вахтеру помещение считается принятым под охрану.

2.9. При вскрытии помещения, допущенные в него работники осуществляют осмотр на предмет выявления признаков несанкционированных действий в помещении в их отсутствие (повреждения дверей, изменение местоположения мебели, включенная техника и т.п.). При отсутствии нарушений, помещение считается снятым с охраны.

2.10. В случае обнаружения нарушений, сотрудник сообщает об этом АИБ, 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.

3. Заключительные положения

3.1. 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.

3.2. За нарушение настоящего положения, работники управления образования могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.