ПРИКАЗ

«___» _____ 20__ г. №_____

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),

ПРИКАЗЫВАЮ:

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 приказа оставляю за собой.

Руководитель _____ {И. О. Фамилия}
{Название Организации}

УТВЕРЖДЕНА
приказом {Название Организации}
от «___» _____20__г. № ___

Положение о контролируемой зоне в {Название Организации}

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 охранник (ЧОП «Охранник» на основании договора от _____ № _____).

2. ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

2.1. Допуск в охраняемые помещения осуществляется в соответствии с утвержденным в {Название Организации} документом «Перечень помещений, в которых разрешена работа с ресурсами ГИС «Бухгалтерия и кадры», в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения» (Приложение № 4 к Политике информационной безопасности в {Название Организации}).

2.2. Помещения, в которых осуществляется обработка защищаемой информации, оборудованы охранной и пожарной сигнализациями, а также прочными дверьми с механическими замками.

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 клиентов, абонентов, пациентов) 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, запирания сейфов, закрытия окон.

3.2. После запирания помещения на ключ, установки охранной сигнализации и сдачи ключа от помещения под роспись вахтеру, 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 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

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.