Приложение 2

к приказу управления здравоохранения

Липецкой области

от\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_\_\_\_\_

**ПОЛОЖЕНИЕ**

**об организации режима безопасности помещений, в которых ведется обработка персональных данных и (или) расположены средства криптографической защиты информации и (или) носители ключевой информации управления здравоохранения Липецкой области**

1. **Общие положения**

Настоящее Положение определяет порядок доступа и правила обеспечения безопасности помещений, в которых обрабатываются персональные данные (ПДн) и (или) размещаются средства криптографической защиты информации (далее – Помещения) в управлении здравоохранения Липецкой области (далее – Учреждение).

1. **Перечень помещений, в которых ведется обработка ПДн**

Обработка ПДн осуществляется в следующих помещениях Учреждения:

* ул. Зегеля, 6, 1 этаж, серверное помещение;
* ул. Зегеля, 6, к. 1;
* ул. Зегеля, 6, к. 2;
* ул. Зегеля, 6, к. 3;
* ул. Зегеля, 6, к. 6;
* ул. Зегеля, 6, к. 7;
* ул. Зегеля, 6, к. 11;
* ул. Зегеля, 6, к. 12;
* ул. Зегеля, 6, к. 13;
* ул. Зегеля, 6, к. 17;
* ул. Зегеля, 6, к. 18;
* ул. Зегеля, 6, к. 24;
* ул. Зегеля, 6, к. 25;
* ул. Зегеля, 6, приемная;
* ул. Зегеля, 6, к. 34;
* ул. Зегеля, 6, к. 35.

При изменении перечня помещений, в которых ведется обработка ПДн, перечень помещений переутверждается руководителем Учреждения отдельно и прикладывается к данному Положению.

1. **Перечень помещений, в которых размещаются средства криптографической защиты информации (СКЗИ)** **и (или) носители ключевой информации**

СКЗИ размещаются в следующих помещениях Учреждения:

* ул. Зегеля, 6, 1 этаж, серверное помещение;
* ул. Зегеля, 6, к. 1;
* ул. Зегеля, 6, к. 2;
* ул. Зегеля, 6, к. 3;
* ул. Зегеля, 6, к. 6;
* ул. Зегеля, 6, к. 7;
* ул. Зегеля, 6, к. 8;
* ул. Зегеля, 6, к. 9;
* ул. Зегеля, 6, к. 10;
* ул. Зегеля, 6, к. 11;
* ул. Зегеля, 6, к. 12;
* ул. Зегеля, 6, к. 13;
* ул. Зегеля, 6, к. 17;
* ул. Зегеля, 6, к. 18;
* ул. Зегеля, 6, к. 19;
* ул. Зегеля, 6, к. 21;
* ул. Зегеля, 6, к. 24;
* ул. Зегеля, 6, к. 23;
* ул. Зегеля, 6, к. 25;
* ул. Зегеля, 6, приемная;
* ул. Зегеля, 6, к. 27;
* ул. Зегеля, 6, к. 28;
* ул. Зегеля, 6, к. 29;
* ул. Зегеля, 6, к. 30;
* ул. Зегеля, 6, к. 32;
* ул. Зегеля, 6, к. 35;
* ул. Зегеля, 6, к. 40;
* ул. Зегеля, 6, к. 42;
* ул. Зегеля, 6, к. 43;
* ул. Зегеля, 2, к.40а;
* ул. Зегеля, 2, к. 35;
* ул. Зегеля, 2, к. 34;
* ул. Зегеля, 6, к. 36.

При изменении перечня помещений, в которых размещаются СКЗИ, перечень помещений переутверждается руководителем Учреждения отдельно и прикладывается к данному Положению.

1. **Правила доступа и обеспечение безопасности помещений, в которых ведется обработка ПДн и (или) размещаются СКЗИ** **и (или) носители ключевой информации**

Целью организации режима обеспечения безопасности в помещениях обработки ПДн и (или) размещения СКЗИ является обеспечение конфиденциальности ПДн, сохранности носителей ПДн и средств защиты информации (СЗИ, в том числе СКЗИ), обеспечивающих техническую защиту ПДн. Правила обеспечения безопасности помещений должны исключать возможность неконтролируемого проникновения или пребывания в помещениях посторонних лиц.

Для обеспечения безопасности Помещений должны выполняться следующие мероприятия и правила безопасности:

* 1. Приказом по Учреждению утверждается уполномоченное лицо и/или структурное подразделение, несущее ответственность за порядок и организацию режима безопасности Помещений Учреждения.
  2. В качестве технических средств физической охраны в Учреждении должны использоваться централизованная система охранной сигнализации с выводом на центральный пульт здания. К данной системе охранной сигнализации здания должны быть подключены датчики охранной сигнализации, установленные в помещениях объекта, в которых размещены средства обработки персональных данных (ПДн). На первом этаже, при входе в здание, на местах дежурных лиц, должен осуществляться контрольно-пропускной режим в помещения здания Учреждения, осуществление видеонаблюдения коридоров и входной группы здания Учреждения. Контроль доступа в Помещения ведется назначенными штатными сотрудниками объекта.
  3. Допуск в Помещения должен осуществляться по согласованию с руководителем подразделения (отдела), или по распоряжению ответственного за обеспечение безопасности ПДн в Учреждении. Перечни лиц, имеющих право доступа в Помещения, могут утверждаться руководителями подразделений и храниться в подразделениях.
  4. Запрещается нахождение в Помещениях посторонних лиц, не имеющих полномочий по доступу к ПДн и (или) к СКЗИ, если на то нет специального разрешения руководителя подразделения (отдела) или ответственного за обеспечение безопасности ПДн в Учреждении.
  5. В рабочее время, в случае ухода всех сотрудников, или в нерабочее время, Помещения должны закрываться на ключ.
  6. Должны выполняться все предписания на эксплуатацию СКЗИ, связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении, где происходит обработка ПДн.
  7. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.
  8. Выносить технические средства обработки ПДн за пределы контролируемой зоны Учреждения с целью их ремонта, замены и т. п. без согласования с ответственным за обеспечение безопасности персональных данных запрещено. При принятии решения о выносе компьютеров жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.
  9. Входные двери Помещений должны быть оснащены замками, обеспечивающие постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.
  10. Мониторы технических средств обработки ПДн должны быть размещены таким образом, чтобы исключалась возможность случайного или преднамеренного визуального просмотра отображаемой на них информации посторонними лицами.

1. **Ответственность за режим безопасности**

Ответственность за режим безопасности в Помещениях отдела (подразделения) и правильность использования установленных в нем технических средств, в том числе средств защиты информации, несет руководитель подразделения, а также ответственный за обеспечение безопасности ПДн в Учреждении, уполномоченный на то соответствующим приказом.

Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением или ответственным за обеспечение безопасности ПДн в Учреждении.