УТВЕРЖДЕНА
приказом директора ГУСО
«Хохотуйский центр помощи детям,
оставшимся без попечения родителей
«Берёзка» Забайкальского края
от «08» мая 2024 года № 276

ИНСТРУКЦИЯ

по обеспечению физической защиты помещений контролируемой зоны Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края

г. Хохотуй
2024

I. Назначение

1.1. Настоящая Инструкция определяет порядок осуществления физической защиты в рабочее и нерабочее время помещений Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края (далее – Инструкция, Учреждение соответственно), в которых обрабатывается конфиденциальная информация (в том числе и персональные данные), а также определяет организацию режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.2. Настоящая Инструкция определяет также порядок действий сотрудников Учреждения при наступлении инцидентов информационной безопасности, связанных с угрозами физической безопасности конфиденциальной информации, обрабатываемой в государственных информационных системах Учреждения.

II. Область применения

2.1. Настоящая Инструкция применяется сотрудниками Учреждения, ответственными за помещения контролируемой зоны, а также дежурными охранниками (сторожами), осуществляющими охрану служебных помещений Учреждения.

III. Нормативные ссылки

3.1. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми и внутренними организационно-распорядительными актами:

- п. 1 ч.1 ст.16, п.1 ч.4 ст.16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- п.3) ч.1 ст.18.1, п.8) и п.9) ч.2 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- п. «а» ст. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119;
- ч.4 ст.26 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;

- ст.15 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства Российской Федерации от 15.09.2008 № 687;

- ЗТС.3 Приложения № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный № 28608);

- подпунктом б) п.6 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378 (зарегистрировано в Минюсте России 18.08.2014 № 33620);

- разд.3.12 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);

- п.3.16, п.4.2.10, п.5.1.3, п.6.3.10, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.2002 № 282;

- раздела IV Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34),

- п.7 Программы проведения работ по контролю (надзору) за использованием шифровальных (криптографических) средств, применяемых для обеспечения безопасности персональных данных в информационных системах персональных данных Типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного руководством 8 Центра ФСБ России 08.08.2009 № 149/7/2/6-1173;

- раздела 4 Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;

- разд.А.11 ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

- разд.11 ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности, и др.

IV. Термины, обозначения и сокращения

4.1. В настоящей инструкции используются следующие термины и определения:

4.1.1. **Автоматизированное рабочее место** - диспетчерское рабочее место на основе персональных электронных вычислительных машин либо специализированных контрольных панелей интегрированных систем безопасности, позволяющее дежурному охраннику дистанционно управлять системой охраны и безопасности объекта и регистрировать поступающую информацию.

4.1.2. **Администратор безопасности информации** - лицо, отвечающее за защиту автоматизированных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

4.1.3. **Взятие объекта под охрану -** выполнение установленных организационных и технических процедур по обеспечению охраны объекта.

4.1.4. **Внутри объектовый режим** - порядок, устанавливаемый клиентом или заказчиком, не противоречащий законодательству Российской Федерации, доведенный до сведения персонала и посетителей объектов охраны и обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на объектах охраны, в соответствии с правилами внутреннего трудового распорядка и требованиями пожарной безопасности.

4.1.5. **Должностное лицо** – сотрудник Учреждения, правомочный от имени Учреждения исполнять определенные, предусмотренные должностными регламентами (должностными обязанностями) действия.

4.1.6. **Информационная безопасность организации** – 1) состояние

защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4.1.7. **Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

4.1.8. **Объект охраняемый** - объект, охраняемый сторожами (вахтерами) или подразделением охраны (ОВО, ЧОП, ЧОО) и оборудованный действующими техническими средствами охранной, пожарной и (или) тревожной сигнализации.

4.1.9. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

4.1.10. **Прибор приемо-контрольный (ППК)** - вид технического средства охраны, служащий для приема на отдельный номер извещения о проникновении (попытке проникновения) в охраняемую зону (зоны), а также возгорании на охраняемом объекте.

4.1.11. **Пропускной режим** - порядок, устанавливаемый клиентом или заказчиком, не противоречащий законодательству Российской Федерации, доведенный до сведения персонала и посетителей объектов охраны и обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на объекты охраны (с объектов охраны).

4.1.12. **Рубеж охранной сигнализации** - совокупность технических средств охранной сигнализации, последовательно объединенных электрической цепью, которые позволяют выдать извещение о проникновении (попытке проникновения) в охраняемую зону (зоны) на отдельный номер ППК независимо от других технических средств, не входящих в эту цепь.

4.1.13. **Снятие объекта с охраны** - штатное прекращение выполнения процедур по обеспечению охраны объекта.

4.1.14. **Шлейф охранной (пожарной, тревожной) сигнализации** - электрическая цепь, которая соединяет выходные цепи охранных (пожарных, тревожных) извещателей, включает в себя вспомогательные (выносные) элементы (диоды, резисторы и т.п.) и соединительные провода и предназначена для выдачи в ППК (приборы приемо- контрольные) извещений о проникновении (попытке проникновения), пожаре и неисправности, а в некоторых случаях и для подачи электропитания на

охранные извещатели.

4.2. В настоящей инструкции используются следующие сокращения:

4.2.1. **АС**- автоматизированная система;

4.2.2. **ИС**- информационная система;

4.2.3. **ИСПДн** - информационная система персональных данных;

4.2.4. **СКЗИ** - средства криптографической защиты информации;

4.2.5. **ЛВС** - локальная вычислительная сеть;

4.2.6. **МНИ** - машинный носитель информации;

4.2.7. **ОШ** - оперативный штаб;

4.2.8. **ПДн** - персональные данные;

4.2.9. **РГОШ** - рабочая группа оперативного штаба;

4.2.10. **СЗИИС** - система защиты информации информационной системы;

4.2.11. **СЗИ**- средства защиты информации.

V. Общие положения

5.1. В Учреждении физическая защита помещений, в которых обрабатывается конфиденциальная информация или хранятся СКЗИ, достигается проведением мероприятий, касающихся как внешних, так и внутренних аспектов.

5.2. Физическая безопасность от внешних угроз достигается:

- установлением контролируемой зоны;
- контролем доступа посторонних лиц в помещения контролируемой зоны в рабочее и нерабочее время.

5.3. Физическая безопасность от внутренних угроз достигается:

- прочностью строительных конструкций здания;
- противопожарной защитой и пожарной сигнализацией;
- регламентацией действий персонала при возгорании, предотвращении и (или) минимизации ущерба при затоплении водой/жидкостью, отключении электроэнергии;
- защитой коммуникаций и систем обеспечения энергоносителями в зданиях;
- размещением оборудования, исключающим несанкционированный доступ к нему и несанкционированный доступ к видовой информации.

5.4. Общие вопросы обеспечения физической безопасности помещений контролируемой зоны Учреждения регламентированы Политикой информационной безопасности в Учреждении.

5.5. Настоящая Инструкция определяет режим охраны, порядок доступа в помещения контролируемой зоны Учреждения в рабочее и нерабочее время.

5.6. Руководитель Учреждения своими приказами определяет режим охраны, порядок доступа в помещения контролируемой зоны в рабочее и нерабочее время.

5.7. В рабочее время контроль доступа на территорию Учреждения

осуществляют дежурные охранники (сторожа).

5.8. Помещения, в которых обрабатывается конфиденциальная информация, пожарной сигнализацией и средствами контроля доступом. По периметру здания установлены камеры видеонаблюдения, с выводом на монитор автоматизированного рабочего места дежурного охранника (сторожа).

5.9. Для принятия оперативных мер по минимизации возможного ущерба защищаемой информации, СКЗИ и иным материальным ценностям при пожаре, прорыве системы отопления и наступлении других чрезвычайных ситуаций, ключи (электронные ключи) от помещений контролируемой зоны должны храниться на вахте в специальном опечатываемом хранилище. Администратор безопасности информации перед началом рабочего дня проверяет целостность печати на хранилище с дубликатами ключей (электронных ключей) от помещений контролируемой зоны.

5.10. Для обеспечения сохранности носителей персональных данных должно осуществляться хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае, если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

VI. Порядок сдачи под охрану помещений контролируемой зоны Министерства

6.1. В конце рабочего дня сотрудник Учреждения обязан:

6.1.1. проверить, чтобы в сдаваемых под охрану помещениях контролируемой зоны были выключены электроприборы и отсутствовали персонал Учреждения и посторонние лица;

6.1.2. закрыть все окна, внутренние двери, закрыть и опечатать мастичной печатью металлические хранилища и др.;

6.1.3. опечатать мастичной печатью (пломбиром) входную дверь помещения контролируемой зоны;

6.1.4. сдать под охрану служебные помещения контролируемой зоны, убедившись;

6.1.5. поместить ключи от входных дверей служебных помещений контролируемой зоны в пенал (хранилище), опечатав его мастичной печатью;

6.1.6. сдать дежурному охраннику (сторожу) под охрану ключи от входных дверей служебных помещений контролируемой зоны;

6.1.7. заполнить на посту охраны поля 2-5 Журнала приема и сдачи под охрану объектов Учреждения (Приложение к настоящей Инструкции);

6.1.8. проконтролировать, чтобы при принятии объекта под сотрудником охраны было заполнены поля 6 и 7 Журнала приема и сдачи под охрану объектов Учреждения (Приложение к настоящей Инструкции).

6.2. Дежурный охранник (сторож) обязан:

6.2.1. принять под охрану служебные помещения контролируемой зоны и ключи от них, заполнив поля 6 и 7 Журнала приема и сдачи под охрану объектов Учреждения (Приложение к настоящей Инструкции).

VII. Порядок снятия с охраны помещений контролируемой зоны Учреждения

7.1. При снятии охраняемого объекта с охраны сотрудник Учреждения обязан:

7.1.1. получить у дежурного охранника (сторожа) пенал (хранилище) с ключами, убедившись в целостности мастичной печати;

7.1.2. заполнить поля 8-9 Журнала приема и сдачи под охрану объектов Учреждения (Приложение к настоящей Инструкции) в строке сдачи указанного объекта под охрану;

7.1.3. убедиться в целостности мастичных печатей (пломб) на входной двери помещения контролируемой зоны;

7.1.4. убедиться в отсутствии признаков проникновения посторонних лиц в помещение контролируемой зоны (убедиться в целостности мастичных печатей (пломб) на входных дверях хранилищ, сейфов, целостности окон и др.);

7.1.5. в случае установления признаков проникновения (попытки проникновения) посторонних лиц, сделать об этом запись в поле 10 (Примечания) Журнала приема и сдачи под охрану объектов Учреждения (Приложение к настоящей Инструкции) и вызвать на место происшествия администратора безопасности информации;

7.1.6. доложить о случившемся руководителю Учреждения служебной запиской.

VIII. Действия дежурного охранника ЧОО (ЧОП) при обнаружении возгорания в помещениях контролируемой зоны Министерства в нерабочее время

8.1. При обнаружении возгорания в помещениях контролируемой зоны Учреждения дежурный охранник (сторож) обязан:

8.1.1. сообщить о факте срабатывания пожарной сигнализации по телефону единой службы «112», или «01», или при помощи ручного извещателя («тревожной кнопки»);

8.1.2. взломав мастичную печать, достать из пенала (хранилища) ключи от входной двери помещения контролируемой зоны Учреждения, в котором произошло возгорание;

8.1.3. по возможности, открыв дверь указанного в п.8.1.2. помещения, предпринять с помощью подручных средств пожаротушения максимальные усилия по локализации возгорания;

8.1.4. оказать содействие прибывшим нарядам ГПС по продвижению к месту возгорания.

8.2. После успешного тушения возгорания (с помощью подручных средств или силами пожарного расчета ГПС):

8.2.1. сделать запись о причине вскрытия помещения контролируемой зоны в полях 8-10 (Примечания) Журнала (Приложение к настоящей Инструкции);

8.2.2. вызвать руководство Учреждения и сотрудника, ответственного за помещение, в котором произошло возгорание;

8.2.3. принять меры для сохранности имущества на охраняемом объекте;

8.3. После прибытия сотрудника, указанного в п.8.2.1. и осмотра им места происшествия, совместно с ним составить в двух экземплярах акт, в котором отразить дату, место и время составления акта, кем он составлен, причину вскрытия кабинета контролируемой зоны Учреждения, расположение и площадь возгорания, описать в общих чертах ущерб помещению контролируемой зоны, время принятия объекта вновь под охрану. Один экземпляр акта впоследствии передается руководителю Учреждения, другой экземпляр акта – руководству ЧОО (ЧОП), осуществляющему охрану объекта на договорной основе (при наличии).

8.4. После устранения причин срабатывания пожарной сигнализации принять данный объект под охрану.

IX. Действия дежурного охранника (сторожа) при обнаружении признаков проникновения посторонних лиц в помещения контролируемой зоны в нерабочее время

9.1. Дежурный охранник (сторож) обязан:

9.1.1. внешним осмотром двери и окон охраняемого объекта убедиться, имеются ли признаки взлома или другого незаконного проникновения посторонних лиц;

9.1.2. если обнаружены признаки незаконного проникновения посторонних лиц, охранник обязан:

9.1.2.1. сообщить о факте незаконного проникновения по телефону единой службы «112» или «02»;

9.1.2.2. предпринять меры к задержанию нарушителей;

9.1.2.3. вызвать по телефону:

- следственно-оперативную группу полиции;

- сотрудника, ответственного за помещение контролируемой зоны, в котором обнаружены признаки несанкционированного проникновения посторонних лиц;

- руководителя Учреждения, правомочного делать заявление о возбуждении уголовного дела;

9.1.2.4. сделать запись о причине вскрытия помещения контролируемой зоны в полях 8-10 Журнала (Приложение к настоящей

Инструкции);

9.1.2.5. после прибытия лиц, указанных в п.9.1.2.3, и осмотра ими места происшествия, составить в двух экземплярах акт аналогично п.8.3. настоящей Инструкции;

9.1.2.6. после устранения причин проникновения посторонних лиц в помещения контролируемой зоны Учреждения принять объект под охрану.

X. Действия дежурного охранника (сторожа) в других случаях, когда необходимо срочное вскрытие дверей помещений контролируемой зоны Министерства в нерабочее время

10.1. Дежурный охранник обязан:

10.1.1. взломав мастичную печать, достать из пенала (хранилища) ключи от входной двери помещения контролируемой зоны Учреждения, которое необходимо вскрыть;

10.1.2. устранить причину происшествия;

10.1.3. сделать отметку в полях 8-10 Журнала (Приложение к настоящей Инструкции) отметку о факте, времени и лице, произведшем извлечение ключей и вскрытие служебных помещений;

10.1.4. вызвать по телефону сотрудника, ответственного за указанное помещение контролируемой зоны;

10.1.5. совместно с прибывшим на место происшествия сотрудником составить в двух экземплярах акт в соответствии с п. 8.3. настоящей Инструкции;

10.1.6. после устранения причин, вызвавших неотложное вскрытие дверей помещений контролируемой зоны Учреждения, принять данный объект под охрану.

XI. Действия сотрудников Министерства при получении сообщения о возгорании или ином происшествии в помещении контролируемой зоны в нерабочее время

11.1. При получении сообщения о происшествии в помещении контролируемой зоны сотрудник, ответственный за указанное помещение, обязан:

11.1.1. срочно прибыть на место происшествия;

11.1.2. оценить причиненный ущерб и принять организационные меры к его минимизации;

11.1.3. проверить целостность средств криптографической защиты;

11.1.4. установить, имеются ли признаки проникновения посторонних лиц в ИС;

11.1.5. в случае установления признаков проникновения (попытки проникновения) посторонних лиц в ИС, хищения средств криптографической защиты или в других случаях, связанных с нарушениями информационной безопасности, безопасности персональных данных, вызвать на место происшествия администратора безопасности

информации;

11.1.6. совместно с дежурным охранником (сторожем) (и администратором безопасности информации в случаях, указанных в п.11.1.5) составить в двух экземплярах акт в соответствии с п. 8.3. настоящей Инструкции;

11.1.7. о случившемся доложить руководителю Учреждения служебной запиской.

XII. Действия персонала Учреждения при обнаружении возгорания в помещениях контролируемой зоны в рабочее время

12.1. Сотрудник Учреждения, обнаруживший возгорание в помещениях Учреждения, обязан:

12.1.1. поставить в известность руководство и персонал Учреждения;

12.1.2. о возгорании сообщить в ГПС по телефону спасательной службы и на пост охраны Учреждения;

12.1.3. сообщить голосом о возгорании и организовать выход сотрудников Учреждения согласно плану эвакуации.

12.2. Рабочая группа оперативного штаба по возможности:

12.2.1. организует:

- эвакуацию персонала, посетителей и резервных копий баз данных ИС из административного здания;

- содействие прибывшим нарядам ГПС по продвижению к месту возгорания;

- отключение электричества в административном здании.

12.3. После погашения возгорания:

12.3.1. собирается оперативный штаб и рабочая группа оперативного штаба, выясняются причины и обстоятельства инцидента информационной безопасности, принимаются меры по минимизации ущерба, определяется фронт работы и исполнители;

12.3.2. членами рабочей группы оперативного штаба проводятся мероприятия по восстановлению работы ИС и СЗИИС;

12.3.3. по указанию руководителя Учреждения администратор безопасности информации проводит служебную проверку для выяснения причин возгорания и ответственности виновных;

12.3.4. членами рабочей группы оперативного штаба проводится анализ причин возникновения инцидента (ЧС);

12.3.5. проводится оперативное совещание при министре труда и социальной защиты населения Забайкальского края с разбором действий должностных лиц при кризисном управлении;

12.3.6. администратором безопасности информации, или членами рабочей группы оперативного штаба проводится дополнительный инструктаж персонала по действиям при обнаружении инцидента информационной безопасности;

XIII. Организация повседневного контроля исполнения настоящей

Инструкции

13.1. Организация повседневного контроля исполнения настоящей Инструкции возлагается на начальников управления и отделов Министерства и администраторов безопасности информации.

XIV. Ответственность и полномочия персонала

14.1. Ответственность персонала

14.1.1. За нарушение требований настоящей Инструкции должностные лица Учреждения несут ответственность в соответствии с действующим законодательством.

14.2. Полномочия персонала

14.2.1. Сотрудники Министерства имеют право выходить с предложениями к министру труда и социальной защиты населения Забайкальского края по вопросам защиты конфиденциальной информации.

XV. Заключительные положения

15.1. Изменения в настоящую Инструкцию вносятся приказом Учреждения после обязательного согласования вносимых изменений с ответственным за организацию обработки персональных данных в Учреждении, ответственного за организацию обеспечения безопасности информации в информационных системах Учреждения, отвечающими за соответствие вносимых изменений требованиям законодательства и нормативно-правовых актов Регуляторов.

15.2. Положения настоящей Инструкции применяются совместно с положениями Инструкции по криптографической защите и обращению с криптосредствами в Учреждении утвержденным приказом Учреждения от 8 мая 2024 года №272 (далее – Инструкция),

15.3. Положения настоящей Инструкции имеют приоритет над положениями указанной Инструкции.

Приложение к Инструкции,
утвержденной приказом
Учреждения
от 08.05.2024г. №276
(к.п.6.1.7)
(Образец формы)

Журнал
приема и сдачи под охрану объектов Государственного учреждения социального обслуживания «Хохотуйский центр помощи детям, оставшимся без попечения родителей «Берёзка» Забайкальского края

№ п/п	№ сдаваемых под охрану кабинетов и хранилищ с ключами	Номер печати	Дата и время сдачи под охрану	Фамилия, инициалы и подпись лица, сдавшего под охрану, № телефона	Отметка о включении сигнализации[1]	Фамилия, инициалы и подпись лица, принявшего под охрану	Дата и время вскрытия помещения и хранилища с ключами	Фамилия, инициалы и подпись лица, вскрывшего помещение или получившего ключи	Примечания
1	2	3	4	5	6	7	8	9	10

[1] Поле 6 заполняется при наличии пожарной и (или) охранной сигнализации