ПРИЛОЖЕНИЕ № 8

УТВЕРЖДЕН
приказом государственного
казенного учреждения
социального обслуживания
Краснодарского края
«Гулькевичский комплексный центр
реабилитации инвалидов»
от 16.12 2022 № 112

ПОРЯДОК ДОПУСКА
работников государственного казенного учреждения социального обслуживания Краснодарского края «Гулькевичский комплексный центр реабилитации инвалидов»впомещения, в которых ведется обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а так же обеспечения внутриобъектового режима.

Объектами охраны государственного казенного учреждения социального обслуживания Краснодарского края «Гулькевичский комплексный центр реабилитации инвалидов» (далее – Учреждение) являются:

помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых;

помещения, аттестованные по требованиям безопасности речевой информации (далее – защищаемые помещения (ЗП));

помещения, в которых установлены компьютеры, сервера и коммутационное оборудование, участвующее в обработке персональных данных;

помещения, в которых хранятся материальные носители персональных данных;

помещения, в которых хранятся резервные копии персональных данных.

Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключен.

К следующим категориям объектов охраны Учреждения(далее – спецпомещения) предъявляются ужесточенные требования по безопасности: помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных (в том числе носители ключевой информации).

Ответственность за соблюдение положений настоящего порядка несут сотрудники структурных подразделений, обрабатывающих персональные данные, а так же руководители структурных подразделений.

Контроль за соблюдением требований порядка обеспечивает ответственный за организацию обработки персональных данных. Контроль за соблюдение требований к спецпомещениям обеспечивает ответственный пользователь криптосредств.

Некоторые положения данного порядка могут не применяться в зависимости от специфики обработки персональных данных структурными подразделениями Учреждения по согласованию с ответственным за организацию обработки персональных данных.

Все объекты охраны Учреждения должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению. Пример: металлические решетки на окнах, металлическая дверь, система контроля и управления доступом и т.д.

2. Допуск в помещения, в которых ведется обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, должен осуществляется только ввиду служебной необходимости.

При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

Допуск сотрудников в помещения, в которых ведется обработка персональных данных, оформляется после подписания сотрудником обязательства о неразглашении и инструктажа ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности информационных систем персональных данных.

В нерабочее время помещения, в которых ведется обработка персональных данных, должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

3. Допуск в серверные помещения

Доступ в серверные помещения разрешен только ответственному за техническое обслуживание информационных систем персональных данных (ИСПДн), ответственному за обеспечение безопасности информационных систем персональных данных и ответственному за организацию обработки персональных данных. Уборка серверных помещений происходит только при строгом контроле указанных лиц.

Серверное помещение в обязательном порядке оснащается охранной сигнализацией, системой видеонаблюдения и системой автономного питания средств охраны.

Доступ в серверные помещения посторонних лиц допускается строго по согласованию с ответственным за организацию обработки персональных данных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

4. Допуск лиц в спецпомещения

Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение, специальное оборудование, охрана и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое количество надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Второй экземпляр ключа от хранилища должен находиться у ответственного пользователя криптосредств.

По окончании рабочего дня спецпомещение и установленные в нём хранилища должны быть закрыты, хранилища опечатаны.

Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ спецпомещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны

или дежурному по организации одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственного пользователя криптосредств.

В обычных условиях спецпомещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственного пользователя криптосредств.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственного пользователя криптосредств. Прибывший ответственный за организацию обработки персональных данных должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в спецпомещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственного пользователя криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Заместитель директора Н.Б. Матяш