УТВЕРЖДАЮ
Заведующая МБДОУ № 30
«Березка» ст. Фастовецкой

_____А.В.Тарасова
17 июля 2015 года

ПРАВИЛА
доступа в Помещения
муниципального бюджетного дошкольного образовательного учреждения детского сада комбинированного вида № 30 «Березка» станицы Фастовецкой муниципального образования Тихорецкий район, в которых ведется эксплуатация средств криптографической защиты информации

Оглавление

1. Общие положения

1.1. Настоящая инструкция разработана в целях обеспечения безопасности конфиденциальной информации и информации, содержащей персональные данные (далее – информация ограниченного доступа), средств вычислительной техники информационных систем, обрабатывающих информацию ограниченного доступа, материальных носителей информации ограниченного доступа, а также обеспечения внутриобъектного режима.

Объектами охраны муниципального бюджетного дошкольного образовательного учреждения детского сада комбинированного вида№ 30 «Березка» станицы Фастовецкой муниципального образования Тихорецкий район (далее – Учреждение) являются:

1) помещения, в которых происходит обработка информации ограниченного доступа с использованием средств автоматизации;

2) помещения, в которых установлены компьютеры, серверы и коммутационное оборудование, защищенные средствами криптографической защиты (далее – СКЗИ), участвующие в обработке информации ограниченного доступа;

3) помещения, в которых хранятся ключевые документы СКЗИ.

1.2. Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.

1.3. К следующим категориям объектов охраны Учреждения (далее – спецпомещения) предъявляются ужесточённые требования по безопасности: помещения, в которых установлены СКЗИ, предназначенные для шифрования информации ограниченного доступа (в том числе ключевые документы).

1.4. Ответственность за соблюдение положений настоящей инструкции несут сотрудники структурных подразделений, обрабатывающих информацию ограниченного доступа, а также руководители структурных подразделений.

1.5. Контроль соблюдения требований настоящей инструкции возлагается на ответственного пользователя СКЗИ.

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

1.7. Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. Доступ посторонних лиц в помещения, в которых ведётся обработка информации ограниченного доступа, 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 информацией ограниченного доступа.

2.2. Допуск сотрудников в помещения, в которых ведётся обработка

информации ограниченного доступа, оформляется после подписания сотрудником обязательства о неразглашении и проведении инструктажа ответственным пользователем СКЗИ, либо администратора информационной безопасности.

2.3. В нерабочее время помещения, в которых осуществляется функционирования СКЗИ, должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, ключевые документы убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

3. Допуск в серверные помещения

3.1. Доступ в серверные помещения разрешён только ответственному пользователю СКЗИ, ответственному за техническое обслуживание информационной системы, администратору информационной безопасности и ответственному за обработку информации ограниченного доступа. Уборка серверных помещений происходит только при строгом контроле указанных лиц.

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

3.3. Доступ в серверные помещения посторонних лиц допускается строго по согласованию с вышеперечисленными лицами.

3.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

4. Допуск лиц в спецпомещения

4.1. Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное запирание 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 посторонних лиц в спецпомещения, необходимо оборудовать металлическими решётками или ставнями, охранной сигнализацией и другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

4.2. 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.

4.3. Для предотвращения просмотра извне спецпомещений их окна

должны быть защищены жалюзями или плотными занавесками.

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

4.5. Для хранения ключевых документов, эксплуатационной и технической документации, установочных пакетов СКЗИ должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного пользователя СКЗИ, второй на посту охраны.

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

4.7. 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 Учреждению одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища.

4.8. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей быть документально оформлением в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых документов и технической и эксплуатационной документации к СКЗИ в хранилище, от которого утрачен ключ, устанавливает ответственный пользователь СКЗИ.

4.9. В обычных условиях спецпомещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

4.10. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, 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 СКЗИ.

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