|  |  |
| --- | --- |
| ПОЛОЖЕНИЕ \_\_\_\_.\_\_\_\_.20\_\_\_\_ № \_\_\_\_\_\_  г. Чебоксары | **УТВЕРЖДЕНО** Приказом от «\_\_» \_\_\_\_\_\_\_\_\_2023 г.  № \_\_\_\_\_\_\_\_ |
| **Об организации серверных и помещений**  **с контролируемой зоной** |  |

1. **Общие положения**

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 21, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013г. № 17, и «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 ФСБ России 21 февраля 2008 г. № 149/6/6-622.1.3.

1.2. Положение определяет порядок и условия организации серверных комнат и помещений контролируемой зоны для безопасной обработки персональных данных на предприятии.

1.3. Цель разработки настоящего Положения – определение требований по организации серверных и помещений контролируемой зоны, согласно нормативно-правовых актов.

1.4. Перечень помещений, в которых ведется обработка ПДн, и их границы устанавливаются приказом по предприятию. «Об определении границ контролируемой зоны и требований к ее безопасности».

1.5. В настоящем Положении используются следующие понятия, термины и сокращения:

**Информационная система персональных данных** **(далее – ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Контролируемая зона (далее – КЗ)** – пространство (территория, здание, часть здания, помещение), в котором расположены средства автоматизации и защиты ИСПДн, в том числе автоматизированные рабочие места (далее – АРМ), на которых ведется обработка ПДн.

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая МЦК – ЧЭМК Минобразования Чувашии.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Серверное помещение** - это помещение, занимаемое телекоммуникационным и/или серверным оборудованием. Серверная является помещением специального назначения (что подразумевает особую режимность этого объекта), соединяется с внешним миром резервируемыми магистралями связи и считается средством обслуживания здания (офиса), предназначенным для выполнения телекоммуникационных функций.

**Помещение контролируемой зоны –** помещение, где хранится программное обеспечение, содержащее криптографические средства защиты информации, ключевые документы криптографических средств защиты информации.

1.6. Настоящее Положение и изменения к нему утверждаются директором МЦК - ЧЭМК Минобразования Чувашии.

1.7. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

1.8. Настоящее Положение является обязательным для исполнения всеми субъектами предприятия, непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным. Все субъекты предприятия, имеющие доступ к ИСПДн, где обрабатывается информация, содержащая конфиденциальные сведения, в т.ч. ПДн должны быть ознакомлены с настоящим Положением и изменениями к нему под роспись.

1. **Требования и рекомендации к серверному помещению**

Требования и рекомендация к серверному помещению (далее серверная) разработаны на основе стандарта TIA/EIA-569  и Российских нормативных документов.

2.1 Рекомендуемые размеры серверной.

Размер серверного помещения выбирается исходя из размера обслуживаемой рабочей области и количества устанавливаемого оборудования. Высота серверного помещения должна быть не менее 2,44 метра. Рекомендуется выделить под серверное помещение 0,09 м2 площади на каждые 10 м2 обслуживаемой рабочей площади.

2.2 Окна, двери и дверной проем.

Рекомендуется под серверное помещение использовать помещение без окон, так как последние являются дополнительным каналом утечки информации. Если в помещении есть окна, расположенные на первом или последнем этажах здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в **серверные** посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией (датчики на разбитие стекол), или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Дверной проем должен быть в ширину не менее 0.91 м и высотой не менее 2 метров. Дверь должна закрываться на замок, чтобы ограничить доступ в серверную.

Навесная дверь должна открываться наружу, раскрытие двери должно быть не менее 1800.

2.3 Подвесной фальшпотолок.

Не рекомендуется использовать в серверном помещении подвесной фальшпотолок.

2.4 Микроклимат (температура, влажность, вентиляция).

Система контроля и управления микроклиматом должна обеспечить в серверной заданный уровень влажности и температуры, необходимый для нормального функционирования активного оборудования. Рекомендуемая температура в диапазоне от 18 до 25 градусов по Цельсию, рекомендуемая относительная влажность в диапазоне от 40 до 55 процентов.

Система микроклимата должна обеспечить поддержку температурного режима не только летом, но и зимой и рассчитана на круглосуточную непрерывную работу.

Если централизованная система микроклимата в здании не может обеспечить непрерывную работу и заданный уровень температуры и влажности, то необходимо установить в серверной автономную систему кондиционирования – основной и резервный кондиционеры. Если в здании установлена система резервного электропитания, то система поддержки микроклимата в серверном помещении должны быть подключена к системе резервного электропитания.

2.5 Освещение серверной.

Необходимо обеспечить освещение в серверном помещении не менее 500 люкс.

Уровень освещенности измеряется на высоте 1 метра от уровня пола. Рекомендуется использовать для освещения серверной лампы накаливания или галогенные лампы, для снижения количества электромагнитных помех. Электропитание освещения серверной и электропитание телекоммуникационного оборудования, установленного в серверном помещении, должно подаваться от разных распределительных электрических щитов. Светильники необходимо размещать на потолке. Требуется использовать для управления освещением одним или несколькими выключателями и располагать их рядом с дверью на высоте 1.5м от уровня пола.

2.6 Электропитание и электрические розетки.

Рекомендуется установить, как минимум, два отдельных блока двойных электрических розеток с заземлением. Блоки электрических розеток рекомендуется запитать от разных питающих кабелей, электрические розетки должны быть рассчитаны на переменный ток до 16А. Розетками расположить с интервалом 1,8 метра вдоль стены на высоте не ниже 0,15 метра от уровня пола.

Подача электропитания в серверную должна осуществляться по выделенному силовому кабелю напрямую от главного распределительного щита. Требуется установить отдельный электрический распределительный щит для  серверной и установить источник бесперебойного питания (ИБП).

Если установлена система резервного электропитания, то серверная должна быть запитана от системы резервного электропитания.

2.7 Заземление серверной.

В помещении серверной должна быть установлена магистральная телекоммуникационная заземляющая шина, к которой должны быть подключены заземляющие и соединительные проводники от монтажных конструктивов, телекоммуникационного оборудования. Никакая часть заземляющих систем не должна иметь сопротивление свыше 4 Ом относительно самой земли. При организации конструкции заземления сопротивления растеканию тока необходимо составить акт скрытых работ. Шинам заземления следует быть доступными для подключения и визуального осмотра.

Заземляющее устройство необходимо располагать на территории контролируемой зоны. Два раза в год, в холодное и теплое время года, производить замер сопротивления заземления растеканию тока с составлением протокола замера.

2.8 Кабельные вводы в серверную.

Рекомендуется размещать кабельные вводы в серверное помещение рядом с дверью.

2.9 Противопожарная безопасность.

Необходимо после прокладки кабелей заделать огнеупорным материалом все кабельные вводы в серверное помещение.

Для этих целей можно использовать специальные заглушки, устанавливаемые в кабельном вводе, которые в случае возникновения пожара расширяются, перекрывают пространство и не позволяют распространиться огню и дыму.

Потолочные перекрытия, стены и перегородки серверного помещения должны быть несгораемыми и обеспечивать огнестойкость не менее 45 минут. Покрытие стен и потолка должно быть из моющегося негорючего материала, пригодного для проведения влажной уборки.

Дверь должна обеспечить огнестойкость не менее 36 минут. Дверь может быть изготовлена из трудно сгораемого материала толщиной не менее 40 мм без внутренних пустот или можно использовать деревянную дверь, но покрыть ее слоем асбеста или обить листовой сталью толщиной не менее 4 мм с двух сторон. Возможна установка металлической двери.

В серверном помещении без окон для удаления дыма в случае пожара должны устанавливаться вытяжные шахты с ручным или автоматическим открыванием. Площадь шахт должна быть не менее 0.2% от площади помещения и расстояние из любой точки помещения до шахты должно быть не более 20 метров.

Если в серверном помещении устанавливаются сплинкеры, то головки сплинкеров рекомендуется закрывать защитными сетчатыми колпачками, чтобы избежать случайного срабатывания сплинкеров.

Опоры и стойки фальшполов должны быть выполнены из несгораемого материала.

Плиты фальшполов должны быть изготовлены из несгораемого материала или материала с пределом огнестойкости 30 минут. Верхнее покрытие плит фальшпола может быть выполнено из сгораемого материала.

Помещения серверной комнаты должны быть оснащены средствами пожаротушения.

2.10 Ограничения доступа.

Серверное помещение не должна быть проходным помещением. Дверь в серверное помещение должна быть с замком и опечатывающим устройством под номерную печать ответственного за данное помещение.

Доступ в серверное помещение, которое используется несколькими клиентами, должен организовывать и контролировать начальник отдела защиты информации. На двери должен быть список лиц, допущенных в данное помещение, утвержденный руководителем предприятия.

2.11 Маркировка серверной.

Все серверные в корпусах должны иметь маркировку на двери.

2.12 Оборудование серверной системами.

Серверное помещение должна быть оборудована системами:

* охранной сигнализации;
* пожарной сигнализации;
* пожаротушения;
* кондиционирования и вентиляции;
* освещения и аварийного освещения.

1. **Требования к помещениям контролируемой зоны**

3.1. Помещения контролируемой зоны выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время и имеющие приспособления для опечатывания замочных скважин. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в **помещения контролируемой зоны** посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или датчиками на разбитие стекол и другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

3.2 Для предотвращения просмотра извне помещений контролируемой зоны их окна должны быть защищены шторами или жалюзи.

3.3 Помещения контролируемой зоны должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному за организацию защиты информации, совместно с представителем отдела безопасности охраны и вахтером по организации с отметкой в соответствующих журналах.   
 3.4 Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей 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 начальника отдела защиты информации, ответственного за организацию обработки ПДн в коробке, опечатанной печатью ответственного за хранение криптосредств.

3.5 По окончании рабочего дня двери помещений контролируемой зоны и установленные в нем хранилища должны быть закрыты и опечатаны номерными печатями.   
 3.6 Ключи от помещений контролируемой зоны, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ помещений контролируемой зоны, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих помещений контролируемой зоны. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.   
 3.7 При утрате ключа от хранилища или от входной двери в помещение контролируемой зоны 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 ответственный за организацию обработки ПДн на предприятии - начальник отдела защиты информации.   
 3.8 В обычных условиях помещения контролируемой зоны, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки ПДн начальнику отдела защиты информации.   
Прибывший ответственный за организацию обработки ПДн 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.   
 3.9 Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в помещениях контролируемой зоны 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.   
 3.10 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 ответственным за организацию обработки необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

3.11 Серверные помещения должны иметь покрытие стен и потолка из моющегося негорючего материала, пригодного для проведения влажной уборки.

3.12 Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключён.   
 3.13 Все помещения контролируемой зоны должны быть оборудованы охранной и пожарной сигнализациями.   
 3.14 Ограждающие конструкции помещений контролируемой зоны должны предполагать существенные трудности для нарушителя по их преодолению.

**4. Нормы безопасности**

4.1. Меры предосторожности предусматривают применение программных и аппаратных замков и ключей, магнитных карт, периодических проверок эффективности различных аспектов схем защиты.