федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«19» 09 2024 г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ДОСТУПА РАБОТНИКОВ ФГБОУ ВО ОмГМУ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, И РАСПОЛОЖЕНЫ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТО ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНО в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение регламентирует условия и порядок осуществления доступа работников ФГБОУ ВО ОмГМУ Минздрава России (далее – организация) в помещения, в которых ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – Информация), и расположены средства криптографической защиты информации (далее – Порядок).

1.2 Требования настоящего Положения обязательны для пользователей (далее – Пользователи) и администраторов (далее – Администраторы) информационных систем персональных данных ФГБОУ ВО ОмГМУ Минздрава России.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Положении использованы ссылки на следующие документы:

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается в том числе установлением правил доступа в помещения, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

3.2 Размещение информационных систем персональных данных Организации (далее – ИСПДн), в которой обрабатывается Информация, должно

осуществляться в пределах контролируемой зоны, границы которой утверждены распоряжением Организации. Для помещений, в которых обрабатывается Информация и расположены средства криптографической защиты информации (далее – Помещения), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

3.3 В помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только работники Организации, утвержденные Ректором в Перечне лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем персональных данных Организации, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах персональных данных Организации.

3.4 При оборудовании Помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

3.5 Нахождение в помещениях с информационными системами персональных данных Организации, не включенных в Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем персональных данных Организации, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах персональных данных Организации, возможно только в присутствии работников Организации. Время нахождения в помещениях ограничивается

временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

3.6 Работники Организации, допущенные к обработке Информации, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители с Информацией без присмотра в незапертом помещении.

3.7 В нерабочее время дверь каждого помещения, в котором ведется обработка Информации, закрывается на ключ. Ключ ответственный сдает/получает дежурному работнику охраны под роспись в журнале.

3.8 Помещения Организации, в которых ведется обработка Информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

3.9 Для предотвращения просмотра защищаемой информации извне окна Помещений должны быть защищены шторами или жалюзи.

3.10 Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

3.11 Внутренний контроль за соблюдением порядка доступа в Помещения проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите, утвержденном в Организации. Контроль и

управление физическим доступом к ИСПДн и средствам криптографической защиты должны предусматривать:

– определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – поддерживание в актуальном состоянии Перечня лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем персональных данных Организации, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах персональных данных Организации;

– санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;

– учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений под роспись в соответствующем журнале, проверка раз в месяц данного журнала.

3.12 При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка Информации и расположены средства криптографической информации, эти помещения не вскрываются, а составляется акт о случившемся. При этом немедленно ставятся в известность Ответственный за обработку и защиту информации и отдел комплексной безопасности Организации. Одновременно принимаются меры по охране места происшествия.

3.13 Ответственность за соблюдение порядка доступа в помещения Организации, в которых ведется обработка Информации и расположены средства

криптографической информации, возлагается на отдел комплексной безопасности Организации.

3.14 В случае нарушения настоящего Порядка работники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ А

Лист ознакомления
с Регламентом обеспечения целостности информационных систем персональных данных

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию
_____ А.С. Колчин
«12» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«11» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ
_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«12» 09 2024 г.