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 КОНТРОЛИРУЕМЫХ ЗОНАХ

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 порядок доступа и передачу помещений под охрану, в которых ведется обработка и хранение персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Омский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ВО ОмГМУ Минздрава России).

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

2.1 Настоящее Положение разработано с учетом следующих положений, законодательных и нормативно-правовых актов:

– Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении 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»;

– Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для исключения неконтролируемого пребывания посторонних лиц в местах обработки персональных данных.

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 В настоящем Положении применяются следующие обозначения и сокращения:

– Под контролируемой зоной (далее – КЗ) понимается территория, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Схемы контролируемой зоны фиксируются в технических паспортах на информационные системы персональных данных, используемые сотрудниками ФГБОУ ВО ОмГМУ Минздрава России. Администратор информационной безопасности (далее – Администратор) обеспечивает актуальность приведенной в технических паспортах информации.

5 ПОРЯДОК ДОСТУПА В ОХРАНЯЕМЫЕ ПОМЕЩЕНИЯ

5.1 Допуск в охраняемые помещения осуществляется в соответствии с утвержденным в ФГБОУ ВО ОмГМУ перечнем помещений, в которых разрешена работа с ресурсами, в которых размещены технические средства ИС, а также перечнем лиц, допущенных в эти помещения.

5.2 Помещения, в которых осуществляется обработка защищаемой информации, оборудованы охранной и пожарной сигнализациями, а также прочными дверьми с механическими замками.

5.3 Ключи от помещений выдаются и находятся на ответственном хранении у сотрудников, которым необходим доступ в эти помещения для выполнения своих служебных (должностных) обязанностей.

5.4 Сотрудникам, которым необходим временный доступ в помещения, к которым у них нет допуска, может быть предоставлен такой доступ, но только в присутствии сотрудников, работающих в этом помещении (имеющих доступ в это помещение).

5.5 При покидании помещения и при отсутствии в нем других лиц, допущенных в это помещение, сотрудник обязан проследить, чтобы в помещении не было посторонних лиц, и закрыть помещение на ключ.

5.6 Перед началом рабочего дня помещения снимаются с охраны. После окончания рабочего дня, помещения устанавливаются под охрану в соответствии с установленным в разделе 3 настоящего положения порядком.

5.7 Нахождение посторонних лиц в помещениях, в которых осуществляется обработка защищаемой информации, допускается только в присутствии сотрудников, работающих в данном помещении и при условии соблюдения правил ограничения доступа к обрабатываемой информации.

6 ПОРЯДОК ПЕРЕДАЧИ ПОМЕЩЕНИЙ ПОД ОХРАНУ

6.1 Закрытие помещений, в которых обрабатывается защищаемая информация, осуществляется по окончании рабочего дня последним сотрудником, покидающим помещение. Закрытие помещения осуществляется после проведения в нем уборки, запирания сейфов, закрытия окон.

6.2 После запирания помещения на ключ, установки охранной сигнализации и в установленных случаях, сдачи ключа от помещения под роспись вахтеру, помещение считается принятым под охрану.

6.3 При вскрытии помещения, допущенные в него сотрудники осуществляют осмотр на предмет выявления признаков несанкционированных действий в помещении в их отсутствие (повреждения дверей, повреждения пломб, изменение местоположения мебели, включенная техника и т. п.). При отсутствии нарушений, помещение считается снятым с охраны.

6.4 В случае обнаружения нарушений, сотрудник сообщает об этом Администратору, который в свою очередь созывает группу реагирования на инциденты информационной безопасности (далее – ГРИИБ). Далее ГРИИБ действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

7 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1 Настоящее Положение может быть изменено и дополнено по следующим причинам:

– появление информации о новых угрозах безопасности информации, связанных с физическим доступом к техническим средствам информационных систем;

– при возникновении инцидентов информационной безопасности, связанных с физическим доступом, извлечения из них уроков и понимания необходимости пересмотра настоящего Положения;

– при изменении законодательства в сфере защиты информации.

7.2 За нарушение настоящего Положения, сотрудники могут нести дисциплинарную ответственность или иную ответственность (уголовную, административную) в соответствии с законодательством Российской Федерации.

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.