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.

ИНСТРУКЦИЯ

ОТВЕТСВЕННОГО ЗА ОБРАБОТКУ И ЗАЩИТУ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЙ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

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

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

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

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1.Настоящая Инструкция устанавливает определяет основные права и обязанности ответственного за обработку и защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – Информация), в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организация, ИСПДн).

1.2 Требования настоящей Инструкции обязательны для ответственного за обработку и защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну ФГБОУ ВО ОмГМУ Минздрава России.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящей Инструкции 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 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Ответственного за обработку и защиту Информации утверждает Ректор ФГБОУ ВО ОмГМУ Минздрава России из числа работников Организации.

4.2 Ответственный за обработку и защиту Информации получает указания непосредственно от Ректора или иного уполномоченного лица и подотчетно ему.

4.3 Ответственный за обработку и защиту Информации в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами и методическими документами Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации (далее - ФСБ России) и регламентирующими документами Организации и отвечает за поддержание необходимого уровня безопасности при обработке информации.

5 ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБРАБОТКУ И ЗАЩИТУ ИНФОРМАЦИИ

5.1 Знать и соблюдать требования действующих нормативных правовых актов, а также внутренних инструкций, правил и положений, регламентирующих

порядок действий по защите информации при ее обработке в ИСПДн.

5.2 Доводить до сведения работников Организации положения законодательства Российской Федерации об Информации, локальных актов Организации по вопросам обработки Информации, требований к защите Информации.

5.3 Осуществлять внутренний контроль (проверки) за соблюдением работников Организации законодательства Российской Федерации об Информации, в том числе требований к защите Информации.

5.4 Осуществлять анализ угроз безопасности информации и проводить периодический пересмотр и при необходимости уточнение Модели угроз безопасности информации в ИСПДн.

5.5 Организовать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль над приемом и обработкой таких обращений и запросов.

5.6 Осуществлять ведение Журнала обучения работников в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и Журнала проверок осведомленности работников в области защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

5.7 Осуществлять ведение Журнала учета обращений субъектов ПДн по вопросам обработки их ПДн в ИСПДн.

5.8 Сообщать обо всех зафиксированных попытках посторонних лиц получить НСД к Информации Ректору или иному уполномоченному лицу.

5.9 Вести учет машинных носителей информации в Журнале регистрации, учета и выдачи машинных носителей информации в ИСПДн и осуществлять контроль перемещения используемых в ИСПДн машинных носителей информации за пределы контролируемой зоны в соответствии с Правилами

обращения с машинными носителями информации в ИСПДн.

5.10 Осуществлять регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесением соответствующих записей в Журнал регистрации, учета и выдачи машинных носителей информации в ИСПДн.

5.11 Осуществлять контроль за обеспечением уровня защиты информации в ИСПДн.

5.12 Организовать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в порядке, определенном ФСБ России, обеспечивать информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

5.13 Уведомлять Управление Роскомнадзора по Омской области о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, в течение 24 часов с момента выявления такого инцидента (включая информирование о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставление сведений о лице, уполномоченном оператором на взаимодействие с Управлением Роскомнадзора по Омской области, по вопросам, связанным с выявленным инцидентом).

5.14 Уведомлять Управление Роскомнадзора по Омской области в течение 72 двух часов с момента выявления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей

нарушение прав субъектов персональных данных, о результатах внутреннего расследования выявленного инцидента, а также предоставлять сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6 ПОРЯДОК ОБУЧЕНИЯ И ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

6.1 Под обучением в настоящей Инструкции понимается информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации.

6.2 Ответственный за обработку и защиту Информации организовывает с работниками Организации работу, направленную на повышение осведомленности работников в области защиты Информации.

6.3 Обучение работников начинается с разработки планов и программ обучения и повышения осведомленности в области защиты Информации. В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности. Программы обучения и повышения осведомленности должны включать информацию:

– о положениях законодательства Российской Федерации об Информации;

– о требованиях организационно-распорядительной документации, регламентирующей вопросы обработки и защиты Информации в Организации;

– о применяемых в Организации мерах защиты Информации;

– о правильном использовании средств защиты (в том числе криптографических) в соответствии с внутренними документами Организации;

– о значимости и важности деятельности работников для обеспечения

защиты Информации.

6.4 Свидетельством выполнения программ обучения и повышения осведомленности в области защиты Информации являются:

– ведение журнала, подтверждающего прохождение работниками Организации обучения в области защиты Информации с указанием темы обучения;

– ведение журнала, содержащего результаты проверок осведомленности работников Организации в области защиты Информации.

6.5 Для работника, принимаемого на работу в Организации или получающего новую роль, должно быть организовано обучение или инструктаж в области защиты Информации, соответствующие полученной роли.

6.6 Обучение и повышение осведомленности работников в области защиты Информации проводится не реже одного раза в год.

6.7 В случае изменения законодательной базы, внутренних нормативных актов Организации в области защиты Информации обучение работников должно быть проведено не позднее одного месяца с момента изменений.

6.8 Проверка осведомленности работников в области защиты Информации проводится не реже одного раза в полгода. В случае если результаты проверки покажут отсутствие у работников необходимых знаний, должно быть проведено внеочередное обучение работников.

7 ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ИНФОРМАЦИИ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА

7.1 Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности Информации требованиям положений, указанных в пункте 2.1 настоящей Инструкции законов и принятых в соответствии

с ними нормативных правовых актов, политики ФГБОУ ВО ОмГМУ Минздрава России обработки персональных данных, локальных актов ФГБОУ ВО ОмГМУ Минздрава России, регламентирующих обработку и защиту Информации.

7.2 Основными целями контроля обеспечения безопасности Информации являются сбор, анализ и обработка данных, необходимых для:

– контроля над реализацией положений законодательной базы и внутренних нормативных актов по обеспечению безопасности Информации в Организации;

– выявления нештатных (или злоумышленных) действий с Информацией;

– обнаружения фактов НСД к Информации.

7.3 При проведении контроля должны использоваться стандартные процедуры документальной проверки, опрос с руководством и работниками Организации. При необходимости уточнения результатов документальной проверки, опросов в рамках внутреннего контроля в качестве дополнительного способа может применяться «проверка на месте», которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

7.4 При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

– политика в отношении обработки Информации удовлетворяет требованиям законодательства Российской Федерации;

– организационная структура обеспечения безопасности Информации создана;

– процессы выполнения требований безопасности Информации исполняются и удовлетворяют поставленным целям;

– защитные меры (например, межсетевые экраны, средства защиты информации от НСД и т.п.) настроены и используются правильно;

– остаточные риски безопасности Информации оценены и остаются

приемлемыми;

– рекомендации предшествующих проверок реализованы.

7.5 При проведении контроля могут использоваться журналы учета событий средств защиты информации для выявления попыток НСД к защищаемым ресурсам.

7.6 Для целей сбора информации о событиях безопасности на объектах контроля могут использоваться как специализированные средства (например, средства анализа защищенности), так и штатные (входящие в другие продукты и системы) средства регистрации действий пользователей и процессов.

7.7 Ответственный за обработку и защиту Информации для проведения контроля имеет право привлекать администратора информационной безопасности и членов комиссии по проведению мероприятий по защите информации.

7.8 Внутренняя проверка завершается подведением итогов (обобщением) результатов проверки и составлением отчета о результате проверки состояния защищенности ИСПДн.

Отчет должен содержать:

– сведения о дате, времени и месте составления отчета;

– сведения о дате и месте проведения проверки;

– сведения о результатах проверки, в том числе о выявленных нарушениях и их характере.

– достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

8 ПРАВА ОТВЕТСТВЕННОГО ЗА ОБРАБОТКУ И ЗАЩИТУ ИНФОРМАЦИИ

8.1 Проходить обучение (переподготовку) по защите информации в учебных центрах и на курсах повышения квалификации.

8.2 Требовать от работников Организации знания и выполнения требований законодательства по защите Информации, локальных актов Организации по вопросам обработки Информации, требований по защите Информации в части их касающейся.

8.3 Инициировать разбирательство и составление заключений по фактам нарушения работниками Организации законодательства Российской Федерации о защите Информации, в том числе требований по защите ПДн, которые могут привести к снижению уровня защищенности ПДн.

8.4 Требовать прекращения обработки Информации в случае нарушения требований по защите Информации.

8.5 Участвовать в анализе ситуаций, касающихся нарушения требований по защите Информации и расследования фактов НСД к Информации.

8.6 Привлекать в случае необходимости работников любых подразделений.

9 ПОРЯДОК РАБОТЫ С ОБРАЩЕНИЯМИ И ЗАПРОСАМИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 Ответственный за обработку и защиту информации организует прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществляет контроль над приемом и обработкой таких обращений и запросов в соответствии с Правилами рассмотрения запросов субъектов персональных данных или их представителей по поводу обработки их персональных данных в ИСПДн.

10 ОТВЕТСТВЕННОСТЬ

10.1 Ответственный за обработку и защиту Информации несет материальную, дисциплинарную, административную и уголовную ответственность:

- за неисполнение либо ненадлежащее исполнение должностных обязанностей;

- за нарушение законодательства, распоряжений, распоряжений руководства Организации, действующих нормативных документов по защите Информации;

- за превышение должностных полномочий и злоупотребление ими;

- за разглашение информации, к которой он допущен в рамках выполнения своих функциональных обязанностей, посторонним лицам.

ПРИЛОЖЕНИЕ А

Лист ознакомления
с Инструкцией ответственного за обработку и защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в информационных системах 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
«_09_» _____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
«_11_» _____09_____ 2024 г.