ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ (ФГБОУ ВО БГМУ МИНЗДРАВА РОССИИ)

ПРИКАЗ

08.12.2021 № 191

г. Уфа

Об утверждении комплекта документов по защите информации

В соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСБ России от 10.07.2014 № 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», в целях утверждения комплекта организационно-распорядительных документов в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» Клиники БГМУ, п р и к а з ы в а ю:

1. Утвердить контролируемой зоной ограждающие конструкции помещений ФГБОУ ВО БГМУ Минздрава России по адресу: Республика Башкортостан, г. Уфа, ул. Шафиева, д. 2.

2. Утвердить Перечень обрабатываемой информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее

компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 1).

3. Утвердить Перечень пользователей, допущенных к обработке информации и лиц, допущенных в помещение трансфузиологического кабинета, в котором расположены технические средства сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 2).

4. Утвердить План мероприятий по приведению деятельности трансфузиологического кабинета в соответствие требованиям по защите информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 3).

5. Утвердить План проведения контроля обеспечения безопасности информации и персональных данных в трансфузиологическом кабинете в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 4).

6. Утвердить Политику в отношении обработки информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 5).

7. Утвердить Положение о порядке хранения и уничтожения носителей информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 6).

8. Утвердить Положение о порядке организации и проведения работ по защите информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 7).

9. Утвердить Положение о комиссии по классификации информационных систем (Приложение № 8).

10. Утвердить Порядок резервного копирования информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 9).

11. Утвердить Форму согласия пациента (донора) на обработку персональных данных, включая биометрических персональные данные (Приложение № 10).

12. Утвердить Инструкцию по антивирусной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 11).

13. Утвердить Инструкцию по парольной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 12).

14. Утвердить Инструкцию о порядке обращения с носителями информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 13).

15. Утвердить Инструкцию пользователя системы защиты информации сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 14).

16. Утвердить Инструкцию ответственного за организацию обработки информации и персональных данных (Приложение № 15).

17. Утвердить Инструкцию администратора информационной безопасности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 16).

18. Утвердить Форму журнала учета машинных носителей информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов,

развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 17).

19. Утвердить Перечень лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 18).

20. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов», и криптоключам к ним (Приложение № 19).

21. Утвердить Инструкцию ответственного пользователя криптосредств в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 20).

22. Утвердить Форму журнала поэкземплярного учёта средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов (Приложение № 21).

23. Утвердить Регламент управления (администрирования) системой защиты информации сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 22).

24. Утвердить Регламент управления конфигурацией комплекса средств обеспечения информационной безопасности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 23).

25. Утвердить Регламент контроля за обеспечением уровня защищенности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 24).

26. Утвердить Правила и процедуры анализа угроз безопасности информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (Приложение № 25).

27. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей в трансфузиологическом кабинете (Приложение № 26).

28. Утвердить Форму журнала учета обращений субъектов персональных данных или их представителей о выполнении их законных прав, при обработке их персональных данных (Приложение № 27).

29. Контроль за исполнением требований настоящего приказа оставляю за собой.

Ректор В. Н. Павлов

Приказ подготовлен:

Главный врач Клиники БГМУ А.А. Бакиров

Согласовано

Проректор по безопасности Р.К. Асадуллин

Начальник УИТ А.Р. Билялов

Начальник ОПУ Е.Г. Сухова

Начальник ЮО Р.В. Нижегородова

Начальник ОД Ю.Н. Арамелева

Согласовано в СЭД
Начальник отдела документации
Ю.Н. Арамелева

Приложение № 1
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08. 12. 2021 № 191

ПЕРЕЧЕНЬ
обрабатываемой информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

п/п	Содержание защищаемого ресурса	Наименование защищаемого ресурса
1.	Персональные данные доноров в электронной форме	Автоматизированная информационная система трансфузиологии (далее – «АИСТ»)
		– фамилия, имя, отчество; – место и дата рождения; – пол; – информация о регистрации по месту жительства или пребывания; – адрес проживания, адрес временной регистрации; – реквизиты паспорта (серия, номер паспорта, кем и когда выдан) или иного удостоверяющего личность документа; – информация о трудовой деятельности (место работы или учебное заведение, должность); – телефонный номер (домашний, рабочий, мобильный); – адрес электронной почты; – личная фотография; – группа крови, резус-принадлежность, информация об исследованных антигенах и о наличии иммунных антител; – результаты клинического исследования крови; – информация о состоянии здоровья (инфекционные и паразитарные заболевания, передающиеся через кровь); – информация о перенесенных инфекционных заболеваниях, нахождении в контакте с инфекционными больными, пребывании на территориях, на которых существует угроза возникновения и (или) распространения массовых инфекционных заболеваний или эпидемий, об употреблении наркотических средств, психотропных веществ, о работе с вредными и (или) опасными условиями труда, а также вакцинациях, хирургических и иных вмешательствах; – информация о предыдущих донациях и клинических исследованиях; – информация о награждении нагрудными знаками "Почетный донор СССР" и "Почетный донор России"; – биометрические персональные данные; – история изменений персональных данных.
		Резервные копии защищаемых ресурсов

2.	Сведения, содержащие способы и методы защиты информации	Пароли, идентификаторы
		Конфигурация и параметры СЗИ сегмента ГИС ЕИБД
		Журналы регистрации событий
		Дистрибутивы средств защиты информации и резервные копии этих дистрибутивов

Приложение № 2
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПЕРЕЧЕНЬ
пользователей, допущенных к обработке информации, и лиц, допущенных в помещение трансфузиологического кабинета, в котором расположены технические средства сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

№ п/п	Ф.И.О	Должность	Номер помещения, доступ в которое разрешен	Исключен из перечня на основании
1.	Валеев Рустэм Фанилевич	И.о. начальника ОИКТ	Трансфузиологический кабинет	
2.	Болдырева Татьяна Евгеньевна	Врач-трансфузиолог	Трансфузиологический кабинет	
3.	Гатауллин Артур Ильдарович	Врач-хирург	Трансфузиологический кабинет	
4.	Осипов Эмиль Андреевич	Заведующий акушерским отделением	Трансфузиологический кабинет	
5.	Гражданкин Александр Александрович	Заведующий отделением анестезиологии-реанимации	Трансфузиологический кабинет	

Приложение № 3
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПЛАН

мероприятий по приведению деятельности трансфузиологического кабинета в соответствие требованиям по защите информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
ПДн	– персональные данные
СЗИ	– система защиты информации
СКЗИ	– средство криптографической защиты информации

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
I. Подготовительные организационные мероприятия				
1	Назначить ответственного за организацию обработки информации и персональных данных	Уполномоченное лицо трансфузиологического кабинета		Приказ о назначении ответственных лиц за обеспечение безопасности информации и персональных данных

№ п/п	Наименование мероприятия
2	Назначить администратора информационной безопасности сегмента ГИС ЕИБД, ответственного за эксплуатацию средств защиты информации
3	Утвердить инструкцию администратора информационной безопасности
4	Утвердить инструкцию о порядке обращения с носителями информации в сегменте ГИС ЕИБД
5	Утвердить журнал учета машинных носителей информации
6	Утвердить перечень обрабатываемой информации и персональных данных в сегменте ГИС ЕИБД
7	Утвердить перечень пользователей, допущенных к обработке информации и лиц, допущенных в помещение
8	Утвердить план мероприятий по приведению деятельности трансфузиологического кабинета в соответствие требованиям законодательства в области защиты информации и персональных данных
9	Утвердить план проведения контроля обеспечения безопасности информации и персональных данных в трансфузиологическом кабинете

Исполнитель	Срок выполнения	Документальное оформление результатов работ
Уполномоченное лицо трансфузиологического кабинета		Приказ о назначении ответственных лиц за обеспечение безопасности информации и персональных данных. Инструкция администратора ИБ.
Уполномоченное лицо трансфузиологического кабинета		Инструкция о порядке обращения с носителями информации. Журнал учета машинных носителей информации. Перечень обрабатываемой информации и ПДн. Перечень пользователей, допущенных к обработке информации и лиц, допущенных в помещение.
Уполномоченное лицо трансфузиологического кабинета		План мероприятий по приведению деятельности трансфузиологического кабинета в соответствие требованиям по защите информации и ПДн. План проведения контроля обеспечения безопасности информации и ПДн в трансфузиологическом кабинете.

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
10	Создать комиссию по классификации информационных систем	Уполномоченное лицо трансфузиологического кабинета		Приказ о создании комиссии по классификации информационных систем. Положение о комиссии по классификации.
II. Организация криптографической защиты информации				
11	Назначить ответственного пользователя криптосредств	Уполномоченное лицо трансфузиологического кабинета		Приказ о назначении ответственных лиц за обеспечение безопасности информации и персональных данных. Инструкция по обращению с СКЗИ. Инструкция ответственного пользователя криптосредств. Перечень лиц, допущенных к работе с СКЗИ. Журнал учёта СКЗИ.
12	Утвердить инструкцию о порядке обращения со средствами криптографической защиты информации, предназначенными для защиты информации и персональных данных, обрабатываемых в сегменте ГИС ЕИБД			
13	Утвердить перечень лиц, допущенных к работе со средствами криптографической защиты информации, ознакомить их с Инструкцией о порядке обращения со средствами криптографической защиты информации, предназначенными для защиты информации и персональных данных, обрабатываемых в сегменте ГИС ЕИБД			
14	Утвердить журнал поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов			

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
	III. Предпроектная стадия			
15	Проведение анализа процессов обработки информации и ПДн, анализа выполнения обязанностей оператором, анализа внутренних документов трансфузиологического кабинета: – определение существующей структуры и топологии сети; – установление состава, объема и местонахождения обрабатываемой информации. Формирование рекомендаций для приведения процессов обработки информации и ПДн в соответствие законодательству о защите информации и ПДн.	Лицензиат		Отчет об обследовании трансфузиологического кабинета.
16	Определение актуальных угроз и актуальных нарушителей безопасности информации			Модель угроз и модель нарушителя безопасности информации.
17	Проведение классификации сегмента ГИС ЕИБД			Акт классификации сегмента ГИС ЕИБД. Акт определения уровня защищенности персональных данных, обрабатываемых в сегменте ГИС ЕИБД. Акт классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации в сегменте ГИС ЕИБД.

№ п/п	Наименование мероприятия
18	Разработка технического задания на выполнение работ по развитию и обеспечению функционирования системы защиты персональных данных
	IV. Разработка организационно
19	Разработка политики в отношении обработки информации и персональных данных
20	Разработка положения о порядке хранения и уничтожения носителей информации
21	Разработка положения о порядке организации и проведения работ по защите информации и персональных данных
22	Регламентировать процесс резервного копирования информации
23	Разработка инструкции пользователя системы защиты информации
24	Разработка инструкция ответственного за организацию обработки информации и персональных данных
25	Разработка инструкции по антивирусной защите

Исполнитель	Срок выполнения	Документальное оформление результатов работ
		Техническое задание на выполнение работ по развитию и обеспечению функционирования системы защиты персональных данных в сегменте ГИС ЕИБД.
-распорядительных документов		
Лицензиат		Политика в отношении обработки информации и ПДн
		Положение о порядке хранения и уничтожения носителей информации
		Положение о порядке организации и проведения работ по защите информации и ПДн
		Порядок резервного копирования информации
		Инструкция пользователя системы защиты информации
		Инструкция ответственного за организацию обработки информации и персональных данных
		Инструкция по антивирусной защите

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
26	Разработка инструкции по парольной защите			Инструкция по парольной защите
27	Разработать шаблон «Согласие на обработку ПДн»			Согласие на обработку ПДн
28	Утвердить комплект организационно-распорядительных документов по защите информации	Уполномоченное лицо трансфузиологического кабинета		Приказ об утверждении комплекта документов по защите информации

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
V. Проектирование системы защиты информации				
29	Разработка технических решений на развитие и обеспечение функционирования систем защиты персональных данных сегмента ГИС ЕИБД	Лицензиат		Ведомость технического проекта. Пояснительная записка к техническому проекту. Описание комплекса технических средств. Схема организационной структуры. Схема структурная комплекса технических средств. Ведомость покупных изделий. Ведомость эксплуатационных документов. Описание технологического процесса обработки данных. Инструкция по эксплуатации комплекса технических средств. Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав системы защиты информации.
VI. Внедрение системы защиты информации в сегменте ГИС ЕИБД				
30	Закупка, монтаж и установка средств защиты информации	Лицензиат		Накладные, лицензии, сертификаты Акт приема-передачи прав

№ п/п	Наименование мероприятия	Исполнитель	Срок выполнения	Документальное оформление результатов работ
31	Установка программного обеспечения; Настройка средств защиты информации согласно техническим решениям на создание системы защиты информации сегмента ГИС ЕИБД;	Лицензиат		Акт установки средств защиты информации
32	Ввод в эксплуатацию системы защиты информации	Уполномоченное лицо трансфузиологического кабинета		Приказ о вводе системы защиты информации в эксплуатацию
VII. Проведение аттестационных испытаний трансфузиологического кабинета по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах				
33	Разработка комплекта документов, необходимых для проведения аттестации сегмента ГИС ЕИБД на соответствие требованиям действующего законодательства Российской Федерации в сфере защиты информации и персональных данных	Лицензиат		Матрица доступа к разделяемым информационным ресурсам. Технический паспорт на систему защиты информации.
34	Разработка Программы и методик аттестационных испытаний	Лицензиат		Программа и методика аттестационных испытаний
35	Проведение аттестационных испытаний	Лицензиат		Протокол проведения аттестационных испытаний Заключение по результатам аттестационных испытаний Аттестат соответствия требованиям безопасности информации

Приложение № 4
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПЛАН

проведения контроля обеспечения безопасности информации и персональных данных в трансфузиологическом кабинете в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

ИБ	– информационная безопасность
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
СрЗИ	– средство защиты информации
СКЗИ	– средство криптографической защиты информации

№ п/п	Наименование мероприятия	Периодичность выполнения	Ответственный за выполнение	Примечание
1	Проверка осведомленности и уровня подготовки работников по обеспечению защиты информации и персональных данных	Не реже одного раза в год	Ответственный за организацию обработки информации и персональных данных	Проверка осведомленности производится по наличию отметок об ознакомлении с внутренними документами организации по вопросам обработки и защиты информации. Уровень подготовки работников проверяется по наличию лиц, ознакомившихся с соответствующими инструкциями и прошедших инструктаж по эксплуатации средств защиты информации (далее – СрЗИ)
2	Проверка выполнения требований к помещениям, в которых производится обработка информации и персональных данных	Не реже одного раза в год	Ответственный за организацию обработки информации и персональных данных	При проверке помещений проводится оценка их соответствия установленным нормам и требованиям

№ п/п	Наименование мероприятия	Периодичность выполнения	Ответственный за выполнение	Примечание
3	Проверка полноты и достаточности организационно-распорядительных документов, регламентирующих обработку информации и персональных данных, актуальности их содержания требованиям по обработке и защите информации и персональных данных	Не реже одного раза в год	Ответственный за организацию обработки информации и персональных данных	Полнота и достаточность проверяется на соответствие законодательству в области защиты информации и персональных данных
4	Пересмотр Модели угроз и модели нарушителя безопасности информации, при ее обработке в сегменте ГИС ЕИБД	При изменении требований к системе защиты информации, а также состава информационной системы	Ответственный за организацию обработки информации и персональных данных	Дополнительно периодичность проведения пересмотра документа может быть определена Моделью угроз и моделью нарушителя безопасности информации, при ее обработке в сегменте ГИС ЕИБД
5	Проверка допуска персонала к информации и персональным данным	Ежеквартально или при внесении изменений в перечень лиц	Ответственный за организацию обработки информации и персональных данных	Проверяются перечни лиц, доступ которых к информации и персональным данным, обрабатываемым в информационных системах организации, необходим для выполнения служебных (трудовых) обязанностей
6	Проверка состава и структуры программно-аппаратных средств	Ежеквартально	Администратор ИБ	Состав и структура программно-аппаратных средств, включенных в реальный технологический процесс, сверяется с технической и эксплуатационной документацией
7	Контроль соблюдения условий использования и учета СрЗИ, предусмотренных эксплуатационной и технической документацией	Не реже одного раза в год	Администратор ИБ	Осуществляется контроль порядка эксплуатации применяемых СрЗИ. Допускается контроль в отношении выборочного числа СрЗИ.

№ п/п	Наименование мероприятия	Периодичность выполнения	Ответственный за выполнение	Примечание
8	Контроль порядка и своевременности блокирования учетных записей пользователей при изменении штатной структуры (увольнении, перемещении сотрудников)	Ежемесячно	Администратор ИБ	Производится проверка соответствия письменных заявок уполномоченных лиц фактическому состоянию учетных записей
9	Контроль выполнения установленных организационно-технических требований по обеспечению безопасности информации и персональных данных	Ежемесячно	Администратор ИБ	Осуществляется контроль функционирования подсистем системы защиты информации
10	Проверка выполнения установленного порядка учета, выдачи, использования и хранения носителей информации, поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Ежемесячно	Ответственный пользователь криптосредств	Проводится: – проверка выполнения пользователями Инструкции пользователя системы защиты информации сегмента ГИС ЕИБД; – проверка правильности ведения журнала учета машинных носителей информации и журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов; – выборочная проверка наличия машинных носителей информации, СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (сверка с записями в соответствующих Журналах учета)
11	Контроль действий пользователей при обработке информации и персональных данных	Ежедневно	Администратор ИБ	Может осуществляться при помощи СрЗИ, применяемых в информационной системе, и заключается в просмотре и анализе электронных журналов регистрации событий безопасности
12	Контроль системы защиты информации на аттестованном объекте	Не реже одного раза в два года		Проводится с целью проведения периодического контроля уровня защиты информации на аттестованном объекте информатизации

Приложение № 5
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПОЛИТИКА
в отношении обработки информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка информации (персональных данных) – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией (персональными данными), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),

извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность

несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
АС	– автоматизированная система
ГИС	– государственная информационная система
ЗИ	– защищаемая информация, в том числе, персональные данные, содержащаяся в базах данных
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИС	– информационная система
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
СЗИ	– система защиты информации
СрЗИ	– средство защиты информации
ЭВМ	– электронно-вычислительная машина

I. Введение

1.1. Настоящая Политика в отношении обработки информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Политика) определяет основные цели и задачи, а также общую стратегию построения системы защиты информации (далее - СЗИ) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД). Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

1.2. Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку СЗИ, с позиции комплексного применения технических и организационных мер и средств защиты информации (далее – СрЗИ).

1.3. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности в сегменте ГИС ЕИБД, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации. Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности защищаемой информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз защищаемой информации;
- координации деятельности уполномоченных лиц при проведении работ по развитию и эксплуатации сегмента ГИС ЕИБД с соблюдением требований обеспечения безопасности защищаемой информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности защищаемой информации в сегменте ГИС ЕИБД.

1.4. Политика разработана на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) № 17 от 11 февраля 2013 года «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.5. В Политике определены требования к персоналу, работающему в сегменте ГИС ЕИБД, их степень ответственности и должностные обязанности, а также должностные обязанности работников, ответственных за обеспечение безопасности защищаемой информации в сегменте ГИС ЕИБД.

II. Общие положения

2.1. Целью настоящей Политики является обеспечение безопасности защищаемой информации в сегменте ГИС ЕИБД от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации.

2.2. Безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий.

2.3. Защищаемая информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности защищаемой информации.

III. Область действия

3.1. Требования настоящей Политики распространяются на всех работников, допущенных к работе в сегменте ГИС ЕИБД (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

IV. Система защиты информации

4.1. СЗИ, строится на основании:

– Перечня обрабатываемой информации и персональных данных в сегменте ГИС ЕИБД;

– Отчета об обследовании объекта Службы крови на соответствие требованиям по защите информации и персональных данных в сегменте ГИС ЕИБД (далее – Отчет об обследовании);

– Акта классификации сегмента ГИС ЕИБД;

– Акта определения уровня защищенности персональных данных, обрабатываемых в сегменте ГИС ЕИБД;

– Модели угроз и модели нарушителя безопасности информации, при ее обработке в сегменте ГИС ЕИБД (далее – Модель угроз);

– Технического задания на выполнение работ по развитию и обеспечению функционирования системы защиты персональных данных в сегменте ГИС ЕИБД;

– Руководящих документов ФСТЭК России и ФСБ России.

4.2. На основании этих документов определяется необходимый уровень защищенности информации, обрабатываемой в сегменте ГИС ЕИБД. На основании анализа актуальных угроз безопасности защищаемой информации, описанного в Отчете об обследовании и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации.

4.3. зависимости от уровня защищенности сегмента ГИС ЕИБД и актуальных угроз, СЗИ может включать следующие подсистемы:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей персональных данных;

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и информации;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– управление конфигурацией информационной системы и системы защиты персональных данных.

4.4. В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки информации, операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими СрЗИ.

V. Основные принципы построения СЗИ

5.1. Построение СЗИ сегмента ГИС ЕИБД и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;

- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

5.6. Законность.

Данный принцип предполагает осуществление защитных мероприятий и разработку СЗИ в соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персонал сегмента ГИС ЕИБД должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

5.7. Системность.

Системный подход к построению СЗИ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации сегмента ГИС ЕИБД. При создании СЗИ должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированный доступ (далее – НСД) к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.8. Комплексность.

Комплексное использование методов и средств защиты информации предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному

злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

5.9. Непрерывность защиты информации.

Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных СрЗИ, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла сегмента ГИС ЕИБД. Сегмент ГИС ЕИБД должен находиться в защищенном состоянии на протяжении всего времени своего функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

5.10. Своевременность.

Данный принцип предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите сегмента ГИС ЕИБД и реализацию мер обеспечения безопасности информации на ранних стадиях разработки в целом, и ее СЗИ, в частности. Разработка СЗИ должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.11. Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования сегмента ГИС ЕИБД и его СЗИ с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.12. Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.13.Принцип минимизации полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к защищаемой информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

5.14. Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность сегмента ГИС ЕИБД, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за обеспечение безопасности информации и персональных данных и администратора ИБ.

5.15. Гибкость системы защиты информации.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

5.16. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

5.17. Научная обоснованность и техническая реализуемость.

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации. СЗИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.18. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и

государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация СрЗИ должна осуществляться профессионально подготовленными специалистами.

5.19. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

VI. Требования к подсистемам СЗИ

6.1. СЗИ включает в себя следующие организационные и технические меры защиты информации, реализуемые в информационных системах в рамках ее системы обеспечения информационной безопасности, в зависимости от угроз безопасности, используемых информационных технологий и структурно-функциональных характеристик автоматизированной системы:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты персональных данных.

6.2. Подсистемы СЗИ имеют различный функционал в зависимости от уровня защищенности информации, обрабатываемой в сегменте ГИС ЕИБД.

6.3. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам

доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

6.4. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

6.5. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в информационной системе программного обеспечения.

6.6. Меры по защите машинных носителей информации должны обеспечивать контроль доступа к машинным носителям информации и учет, контроль перемещения и использования.

6.7. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6.8. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.9. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

6.10. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

6.11. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

6.12. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

6.13. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам.

6.14. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

6.15. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

6.16. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечить управление изменениями конфигурации информационной системы, анализировать потенциальное воздействие планируемых изменений в конфигурации информационной системы и системы защиты персональных данных, а также определению лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.

VII. Пользователи сегмента ГИС ЕИБД

7.1. В сегменте ГИС ЕИБД можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой информации:

- администратор ИБ;

- ответственный за организацию обработки информации и персональных данных;
- ответственный пользователь криптосредств;
- пользователь.

7.2. Администратор ИБ

Администратор ИБ ответственен за функционирование СЗИ, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении сегмента ГИС ЕИБД;
- обладает полной информацией о технических средствах и конфигурации сегмента ГИС ЕИБД;
- имеет доступ ко всем техническим средствам обработки информации и данным сегмента ГИС ЕИБД;
- обладает полной информацией о сегменте ГИС ЕИБД;
- имеет полный доступ к СрЗИ и протоколирования и к части ключевых элементов сегмента ГИС ЕИБД.

Администратор ИБ уполномочен:

- реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов в соответствии с которыми пользователь получает возможность работать с элементами сегмента ГИС ЕИБД;
- осуществлять аудит СрЗИ.

7.3. Ответственный за организацию обработки информации и персональных данных

Ответственный за организацию обработки информации и персональных данных обладает следующим уровнем доступа и знаний:

- знает законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;
- знает порядок использования, обработки и хранения конфиденциальной информации, в том числе персональных данных.

Ответственный за организацию обработки информации и персональных данных уполномочен:

- осуществлять внутренний контроль соблюдения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;
- доводить до сведения работников положения законодательства Российской Федерации в части защиты информации, в том числе персональные данные ПДн;

– предоставлять необходимую информацию при проведении проверок регулирующими органами, а также проведении контрольных мероприятий по обеспечению информационной безопасности;

– организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.4. Ответственный пользователь криптосредств

Ответственный пользователь криптосредств ответственен за функционирование СКЗИ.

Ответственный пользователь криптосредств обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении сегмента ГИС ЕИБД;

– имеет частичный доступ к СрЗИ и протоколирования и к части ключевых элементов сегмента ГИС ЕИБД.

– имеет полный доступ к СКЗИ.

Ответственный пользователь криптосредств уполномочен:

– реализовывать политики безопасности в части настройки СКЗИ, позволяющие пользователю работать с элементами сегмента ГИС ЕИБД;

– осуществлять аудит СКЗИ.

7.5. Пользователь сегмента ГИС ЕИБД.

Пользователь сегмента ГИС ЕИБД осуществляет обработку защищаемой информации. Обработка информации включает: возможность просмотра защищаемой информации, ручной ввод информации в систему сегмента ГИС ЕИБД, формирование справок и отчетов по информации, полученной из сегмента ГИС ЕИБД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗИ.

Пользователь сегмента ГИС ЕИБД обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;

– располагает конфиденциальными данными, к которым имеет доступ.

VIII. Требования к персоналу по обеспечению защиты информации

8.1. Все работники, являющиеся пользователями сегмента ГИС ЕИБД, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемой информации и соблюдению режима безопасности информации.

8.2. При вступлении в должность нового работника, ответственный за организацию обработки информации и персональных данных обязан организовать его ознакомление с должностной инструкцией и необходимыми

документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования сегмента ГИС ЕИБД.

8.3. Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами сегмента ГИС ЕИБД и СЗИ.

8.4. Работники, имеющие доступ к сегменту ГИС ЕИБД, должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации).

8.5. Работники, имеющие доступ к сегменту ГИС ЕИБД, должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности информации и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

8.6. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

8.7. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе в сегменте ГИС ЕИБД, третьим лицам.

8.8. При работе с защищаемой информацией в сегменте ГИС ЕИБД работники обязаны обеспечить отсутствие возможности просмотра защищаемой информации третьими лицами с мониторов АРМ или терминалов.

8.9. При завершении работы в сегменте ГИС ЕИБД работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

8.10. Работники должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

8.11. Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы сегмента ГИС ЕИБД, могущих повлечь за собой угрозы безопасности информации, а также о выявленных ими событиях, затрагивающих безопасность информации, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности информации.

IX. Должностные обязанности пользователей сегмента ГИС ЕИБД

9.1. Должностные обязанности пользователей сегмента ГИС ЕИБД описаны в следующих документах:

- инструкция администратора ИБ;
- инструкция пользователя системы защиты информации;
- инструкция ответственного за организацию обработки информации и персональных данных;
- инструкция ответственного пользователя криптосредств.

X. Ответственность пользователей сегмента ГИС ЕИБД

10.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

10.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

10.3. При нарушениях работниками сегмента ГИС ЕИБД правил, связанных с безопасностью информации, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение № 6
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПОЛОЖЕНИЕ
о порядке хранения и уничтожения носителей информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие

обработку информации (персональных данных), а также определяющие цели обработки информации (персональных данных), состав информации (персональных данных), подлежащих обработке, действия (операции), совершаемые с информацией (персональными данными).

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИС	– информационная система
НСД	– несанкционированный доступ
ПДн	– персональные данные
ПО	– программное обеспечение
СрЗИ	– средство защиты информации
МНИ	– машинные носители информации
ГМД	– гибкие магнитные диски
НЖМД	– накопители на жестких магнитных дисках

I. Общие положения

1.1. Положение о порядке хранения и уничтожения носителей информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Положение) разработано в целях обеспечения выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

1.2. Настоящее Положение устанавливает порядок учета, хранения и уничтожения машинных и бумажных носителей информации, а также порядок учета средств защиты информации (далее – СрЗИ), эксплуатационной и технической документации к ним в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее

компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.3. Пользователи допускаются к обработке информации в сегменте ГИС ЕИБД в соответствии с Перечнем пользователей, допущенных к обработке информации и лиц, допущенных в помещение объекта Службы крови, в котором расположены технические средства сегмента ГИС ЕИБД, и Перечнем обрабатываемой информации и персональных данных в сегменте ГИС ЕИБД.

1.4. С настоящим Положением должны быть ознакомлены под роспись пользователи сегмента ГИС ЕИБД, допущенные к обработке защищаемой информации.

II. Организация учета носителей информации

2.1. Для обработки защищаемой информации в сегменте ГИС ЕИБД могут использоваться следующие машинные носители информации (далее – МНИ): гибкие магнитные диски (далее – ГМД), накопители на жестких магнитных дисках (далее – НЖМД), оптические диски, Flash-диски и другие устройства для хранения информации.

2.2. Все МНИ, на которых производится обработка защищаемой информации и ПДн сегмента ГИС ЕИБД, подлежат обязательному учету с присвоением им уникальных регистрационных (идентификационных) номеров. На МНИ должны быть зафиксированы учетные данные. Образцы фиксации указаны в Приложении 2 (П 2).

2.3. Изначально, СЗИ от НСД (DallasLock 8.0-K) блокирует использование всех МНИ на автоматизированных рабочих местах с установленной автоматизированной информационной системой трансфузиологии (далее - АИСТ).

2.4. Функции по организации работы и учету МНИ возлагаются на ответственного за организацию обработки информации и персональных данных.

2.5. Ответственный за организацию обработки информации и персональных данных в журнале учета машинных носителей информации, пример в Приложении (П 1), заносится информация о модели МНИ, его серийном номере, имени компьютера, на котором предполагается его использовать, ФИО пользователя МНИ и ФИО ответственного (согласно приведенному в приложении примеру). После заполнения всей информации, ответственное лицо обращается в Единую службу поддержки ЕИБД (по телефону: 8-800-700-76-06) и предоставляет необходимую информацию.

2.6. После предоставления всей необходимой информации Единая служба поддержки ЕИБД добавляет указанный МНИ в список разрешенных МНИ на указанном компьютере и появляется возможность работы с ним.

III. Порядок хранения носителей информации

3.1. Хранение носителей информации организует ответственный за

организацию обработки информации и персональных данных в сегменте ГИС ЕИБД.

3.2. Для хранения носителей информации используются специальные хранилища (сейфы, металлические шкафы и т.п.), исключающие возможность несанкционированного к ним доступа, подмены, хищения или уничтожения.

3.3. В сегменте ГИС ЕИБД должно быть обеспечено раздельное хранение бумажных носителей информации, обработка которых осуществляется в различных целях.

3.4. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки устройств с элементами накопления и хранения информации.

IV. Обязанности работников при обращении с носителями информации

4.1. Работник, осуществляющий работу с носителями информации, обязан:

– соблюдать режим конфиденциальности при обработке защищаемой информации, к которой он допущен;

– обеспечивать надежное хранение носителей информации;

– не передавать носители информации лицам, которые не допущены к обработке защищаемой информации;

– немедленно уведомлять непосредственного руководителя и принимать меры по предотвращению утечки защищаемой информации при выявлении фактов утраты или недостачи ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений;

– сдать носители информации в соответствии с порядком, установленным настоящим Положением, при увольнении или отстранении от исполнения обязанностей, связанных с обработкой информации.

4.2. Работнику, осуществляющему работу с носителями информации, запрещается:

– записывать на учтенные МНИ информацию, не имеющую отношения к выполняемой работе;

– принимать и передавать носители информации без соответствующего разрешения и оформления в установленном порядке;

– хранить носители информации на рабочих столах либо оставлять их без присмотра.

V. Порядок уничтожения носителей информации

5.1. Носители информации подлежат уничтожению:

– в случае достижения целей обработки информации, если иное не предусмотрено законодательством РФ;

– если они пришли в негодность, отслужили установленный срок или утратили практическое значение.

5.2. Уничтожение информации и персональных данных на носителях информации производится комиссией по классификации информационных систем, назначенной приказом, с оформлением Акта об уничтожении информации и персональных данных (П 3). Под уничтожением информации на носителях понимается физическое уничтожение носителей.

5.3. Бумажные носители информации уничтожаются путем их измельчения (например, в уничтожителе бумаги).

5.4. Уничтожение МНИ производится любым способом, исключающим возможность дальнейшего использования элемента носителя информации. Рекомендации по уничтожению МНИ приведены в Таблице 1.

Таблица 1 – Примеры способов уничтожения МНИ

Тип МНИ	Способ уничтожения (последовательность действий)
ГМД (ГМД 3,5")	уничтожение магнитного носителя в уничтожителе бумаги
Оптический носитель (CD-, DVD-диск и т.п.)	измельчение носителя любым доступным механическим способом (например, в уничтожителе бумаги при наличии в нем такой функциональной возможности)
НЖМД (HDD)	физическое дробление (значительная деформация) магнитных дисков и интегральных микросхем накопителя
Flash-диск (USB-накопитель)	физическое дробление

VI. Порядок учета СрЗИ, эксплуатационной и технической документации к ним

6.1. Для организации учета применяемых СрЗИ, эксплуатационной и технической документации к ним назначается ответственный за организацию обработки информации и персональных данных.

6.2. Все СрЗИ и документация к ним подлежат регистрации в журнале учета СрЗИ, эксплуатационной и технической документации к ним (П 4).

6.3. Программно-аппаратные СрЗИ учитываются поштучно по заводским (серийным, идентификационным) номерам и по комплектности.

6.4. Документация к СрЗИ в бумажном виде учитывается по номерам и экземплярам.

6.5. Программное обеспечение СрЗИ и документация в электронном виде учитывается по заводскому (серийному) номеру дистрибутива (МНИ) с записанным программным обеспечением и документацией.

6.6. При регистрации СрЗИ, не имеющего заводского (серийного) номера, ему присваивается учетный номер. При регистрации такого СрЗИ,

помимо заполнения граф журнала учета, на его корпус либо на МНИ с установочным комплектом СрЗИ любым доступным способом наносятся следующие реквизиты:

- учетный номер по журналу учета;
- подпись и ФИО лица, ответственного за организацию обработки информации и персональных данных.

6.7. Порядок фиксации учетных данных на МНИ с установочным комплектом СрЗИ аналогичен порядку, установленному для носителей информации (см. П.2).

6.8. Ответственное лицо должно обеспечить ведение резервной копии программного обеспечения СрЗИ, а также хранение СрЗИ и документации к ним в месте, исключающем несанкционированный доступ к ним посторонних лиц.

6.9. Все случаи получения, выдачи, установки (подключения), изъятия (отключения), уничтожения СрЗИ и документации к ним отражаются в журнале учета.

VII. Контроль учета носителей информации, СрЗИ, эксплуатационной и технической документации к ним

7.1 Лица, ответственные за учет применяемых СрЗИ, эксплуатационной и технической документации к ним, носителей информации, должны проводить периодический контроль (сверку) их наличия.

7.2 Периодичность контроля, а также лица, ответственные за организацию его проведения, предусматриваются Планом проведения контроля обеспечения безопасности информации и персональных данных.

П 1

к Положению о порядке хранения и уничтожения носителей информации

ЖУРНАЛ
учета машинных носителей информации

№	Регистрационный номер носителя информации (заполняет Тех поддержка)	Модель носителя и серийный номер	Дата регистрации \ снятия с регистрации	Имя компьютера или ФИО сотрудника для кого разрешен носитель	ФИО ответственного за носитель информации	Подпись ответственного за носитель информации
1		***USB-Флешка Transcend Ultra Speed 16Gb s/n 46554455***	***Регистрация 25.11.2020***	***Имя компьютера «ARM007» Иванов Иван Иванович***	***Иванов Иван Иванович***	
2						
3						
4						
5						
6						
7						

П 2

к Положению о порядке хранения и уничтожения носителей информации

ОБРАЗЦЫ

фиксации учетных данных на машинных носителях информации

На гибком магнитном диске

На оптическом носителе информации

На накопителе на жестком магнитном диске

На Flash-диске

П 3

к Положению о порядке хранения и уничтожения носителей информации

УТВЕРЖДАЮ

_____

_____

_____

«___» _____ 201_ г.

АКТ №___
уничтожения персональных данных

Комиссия, назначенная приказом _____
от «___» _____ 201_ г. № _____, в составе:

Председатель комиссии: _____
(фамилия и инициалы)

Члены комиссии: _____

_____
(фамилия и инициалы)

провела отбор носителей персональных данных и установила, что в связи с отсутствием законных оснований (необходимости) дальнейшей обработки персональных данных содержащаяся на них информация подлежит уничтожению:

№ п/п	Тип носителя	Рег. номер носителя	Перечень субъектов (баз данных) ПДн	Основание для уничтожения
1				
2				
3				
4				
5				

Всего подлежат уничтожению _____ носителей.
(цифрами и прописью)

Председатель комиссии

_____ _____
(личная подпись) (фамилия и инициалы)

Члены комиссии

_____ _____
(личная подпись) (фамилия и инициалы)

_____ _____
(личная подпись) (фамилия и инициалы)

Уничтоженные носители с книг и журналов учета списаны.

Лицо, ответственное за учет

_____ _____
(личная подпись) (фамилия и инициалы)

П 4

к Положению о порядке хранения и уничтожения носителей информации

ЖУРНАЛ

учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование СрЗИ	Заводской (серийный, учетный) номер СрЗИ, номер документа-ции к СрЗИ	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СрЗИ			Отметка об изъятии СрЗИ		Примечание
			От кого получены	Дата и номер сопроводительного письма	Фамилия И.О. пользователя СрЗИ	Дата, подпись	Фамилия И.О. сотрудника, производившего подключение (установку)	Дата подключения (установки), подпись	Номера аппаратных средств, в которые или к которым подключены СрЗИ	Фамилия И.О. сотрудника, производившего изъятие (отключение)	Дата, подпись	

Приложение № 7
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть

раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение

информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ЗИ	– защищаемая информация, в том числе, персональные данные, содержащаяся в базах данных
ИС	– информационная система
ПДн	– персональные данные
ПО	– программное обеспечение

I. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите информации и персональных данных в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных, обрабатываемых в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД) в соответствии с законодательством Российской Федерации.

1.2. Настоящее Положение разработано в соответствии с:

– Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

II. Получение, обработка и защита персональных данных

2.1. Порядок получения персональных данных.

2.1.1. Все персональные данные следует получать лично у субъекта персональных данных (далее – ПДн). Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

2.1.2. Оператор вправе обрабатывать персональные данные субъектов ПДн только с их письменного разрешения.

2.1.3. Письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя персональные данные, указанные в перечне ПДн, подлежащих защите в сегменте ГИС ЕИБД.

2.1.4. Работники Оператора имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

2.1.5. Работники Оператора, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2. Порядок обработки персональных данных.

Обработка персональных данных может осуществляться только в целях ведения единой базы данных по осуществлению мероприятий, связанных с обеспечением

безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов, в соответствии с Законом Российской Федерации от 09.06.1993 г. № 5142-I «О донорстве крови и ее компонентов» до истечения срока действия данного закона, далее согласно Федерального закона от 20.07.2012 № 125-ФЗ «О донорстве крови и ее компонентов».

2.2.1. При определении объема и содержания, обрабатываемых персональных данных,

Оператор должен руководствоваться Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты персональных данных.

2.2.2. При принятии решений, затрагивающих интересы субъекта ПДн, Оператор не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

2.2.3. Съемные электронные носители, на которые копируется база данных сегмента ГИС ЕИБД, для переноса ее в ноутбуки выездных бригад, должны быть промаркированы в соответствии с Положением о порядке хранения и уничтожения носителей информации и учтены в Журнале учета машинных носителей информации.

2.3. Порядок защиты персональных данных.

2.3.1. Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном федеральными законами Российской Федерации в области защиты персональных данных.

2.3.2. Оператор обязан при обработке персональных данных субъектов персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.3.3. Соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн.

2.3.4. Применять технические средства охраны и сигнализации.

2.3.5. Подписать со всеми работниками, связанными с получением, обработкой и защитой персональных данных субъектов ПДн, Обязательство о неразглашении персональных данных.

2.3.6. Привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн.

2.3.7. Запретить допуск к персональным данным субъектов ПДн работников Оператора, не включенных в Перечень лиц, допущенных к обработке персональных данных, обрабатываемых в сегменте ГИС ЕИБД.

2.3.8. Защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты

информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

2.3.9. Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях с письменного разрешения руководителя.

2.3.10. Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

2.3.11. Оператор, субъекты ПДн и их представители должны совместно вырабатывать меры защиты персональных данных субъектов ПДн.

III. Хранение персональных данных

3.1. Сведения о субъектах ПДн на бумажных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственного за организацию обработки информации и персональных данных.

3.2. Обязанности по хранению сведений о субъектах ПДн, заполнению, хранению и выдаче документов, содержащих персональные данные, в сегменте ГИС ЕИБД возлагаются на ответственного за организацию обработки информации и персональных данных.

3.3. Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы в соответствии с Положением о порядке хранения и уничтожения носителей информации и учтены в журнале учета машинных носителей информации.

3.4. В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

IV. Передача персональных данных

4.1. При передаче персональных данных субъекта ПДн Оператор должен соблюдать следующие требования:

4.1.1. Предупреждать лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы только в целях исполнения в соответствии с Законом Российской Федерации от 09.06.1993 г. № 5142-I «О донорстве крови и ее компонентов» до истечения срока действия данного закона, далее согласно Федерального закона от 20.07.2012 № 125-ФЗ «О донорстве крови и ее компонентов».

4.1.2. Осуществлять передачу персональных данных субъекта ПДн только в целях ведения единой базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием,

организацией и пропагандой донорства крови и ее компонентов в соответствии с Законом Российской Федерации от 09.06.1993 г. № 5142-I «О донорстве крови и ее компонентов» до истечения срока действия данного закона, далее согласно действующему законодательству.

4.1.3. При передаче персональных данных субъекта ПДн использовать выделенную WAN (глобальную компьютерную сеть) с применением сертифицированных средств криптографической защиты информации.

4.1.4. Передавать персональные данные субъекта ПДн представителю субъекта ПДн в порядке, установленном федеральными законами Российской Федерации.

V. Уничтожение персональных данных

5.1. При необходимости уничтожения персональных данных Оператор должен руководствоваться следующими требованиями:

5.1.1. Уничтожение персональных данных в сегменте ГИС ЕИБД осуществляется комиссией по классификации информационных систем.

5.1.2. Бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги).

5.1.3. Персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных.

5.1.4. После окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

VI. Внутренние проверки состояния защищенности

6.1. Проверка состояния защищенности сегмента ГИС ЕИБД осуществляется комиссией по классификации информационных систем.

6.2. Проверка состояния защищенности сегмента ГИС ЕИБД осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Оператором, требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

6.3. Проверка состояния защищенности сегмента ГИС ЕИБД включает в себя:

6.3.1. Определение характера циркулирующих персональных данных и установленных в сегменте ГИС ЕИБД режимов их обработки.

6.3.2. Определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты

информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники.

6.3.3. Анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия).

6.3.4. Проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации.

6.3.5. Проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств.

6.3.6. Проверка работоспособности используемых программных и программно-аппаратных средств обнаружения и предотвращения компьютерных атак.

6.3.7. Проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты.

6.3.8. Проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, регламент доступа к серверным и кроссовым помещениям.

6.3.9. Проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва).

6.3.10. Проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

6.4. Внутренняя проверка Комиссии по проведению мероприятий по защите персональных данных завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности сегмента ГИС ЕИБД.

6.5. Акт должен содержать:

6.5.1. Дата, время и место составления акта.

6.5.2. Дата и место проведения проверки.

6.5.3. Сведения о результатах проверки, в том числе о выявленных нарушениях и их характере.

6.5.4. 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.

VII. Обязанности субъекта персональных данных и Оператора

7.1. В целях обеспечения достоверности персональных данных субъект ПДн обязан:

7.1.1. Предоставлять полные и достоверные данные о себе.

7.1.2. В случае изменения своих персональных данных сообщать данную информацию Оператору.

7.2. Оператор обязан:

7.2.1. Осуществлять защиту персональных данных субъекта ПДн.

7.2.2. Ввести Журнал учета запросов (обращений) субъектов персональных данных в сегменте ГИС ЕИБД (Приложение 1).

7.2.3. Обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

VIII. Права субъекта ПДн в целях защиты персональных данных

8.1. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;

8.3. Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

8.4. Субъект персональных данных имеет право требовать исключить или исправить неверные, или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.5. Субъект персональных данных имеет право требовать об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.6. Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействии Оператора при обработке и защите его персональных данных.

IX. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

9.1. Лица, виновные в нарушении требований федеральных законов РФ, несут предусмотренную законодательством РФ ответственность.

9.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

ПРИЛОЖЕНИЕ 1
к Положению о порядке организации и проведения работ
по защите информации и персональных данных
в сегменте ГИС ЕИБД

ЖУРНАЛ

учета запросов (обращений) субъектов персональных данных

№ п/п	Дата и рег. номер запроса (обращения)	Сведения о запрашиваюшем лице (ФИО, паспортные данные)	Краткое содержание обращения	Отметка о предоставлении (отказе в предоставлении) информации	Дата и рег. номер ответа на запрос	Подпись запрашивающего лица о получении ответа (отметка об отправке письма)	Подпись ответственного лица
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							

Приложение № 8
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПОЛОЖЕНИЕ
о комиссии по классификации информационных систем

Определения

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

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ПДн	– персональные данные

I. Общие положения

1.1. Целью создания Комиссии по классификации информационных систем является выполнение требований по защите информации и персональных данных (далее - ПДн) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД), а также классификация информационных систем и ввод их в эксплуатацию.

1.2. Комиссия взаимодействует с органами, осуществляющими контроль в сфере защиты персональных данных.

II. Задачи Комиссии

2.1. Организация работы в области защиты информации и персональных данных, подготовка соответствующих предложений по решению проблем в области защиты персональных данных, возникающих в процессе обработки персональных данных, классификация информационных систем и ввод их в эксплуатацию.

III. Функции Комиссии

3.1. Рассмотрение предложений для выработки рекомендаций, направленных на улучшение действий по обработке персональных данных.

3.2. Проверка знаний, требований законодательства по защите персональных данных работниками, осуществляющими обработку персональных данных.

3.3. Информирование работников об изменениях, касающихся защиты персональных данных.

3.4. Подготовка и представление предложений по совершенствованию работ в сфере защиты информации и персональных данных.

3.5. Рассмотрение проектов локальных нормативных актов и организационно-распорядительных документов по защите персональных данных и подготовка предложений по ним.

3.6. Участие в определении уровня защищенности информационных систем персональных данных, классификации государственных информационных систем и автоматизированных систем.

3.7. Проверка готовности средств защиты информации к использованию в информационных системах.

3.8. Участие во внедрении средств защиты информации.

3.9. Ввод в эксплуатацию систем защиты информации.

3.10. Уничтожение конфиденциальной информации и персональных данных.

IV. Права Комиссии

4.1. Получать полную информацию об обработке персональных данных.

4.2. Заслушивать на заседаниях Комиссии сообщения работников, ответственных за обработку персональных данных о выполнении ими обязанностей по соблюдению защиты персональных данных и соблюдению гарантий прав субъектов персональных данных (доноров).

4.3. Участвовать в подготовке локальных нормативных актов и организационно-распорядительных документов, находящихся в компетенции Комиссии.

4.4. Содействовать разрешению споров, связанных с нарушением законодательства в области защиты персональных данных.

Приложение № 9
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПОРЯДОК
резервного копирования информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации

(персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
ИС	– информационная система
ОС	– операционная система
ПО	– программное обеспечение
СУБД	– система управления базами данных

I. Общие положения

1.1. Настоящий порядок резервного копирования информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Порядок) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных (защищаемой информации и персональных данных), хранящихся в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД), а также к резервированию аппаратных средств.

1.2. Настоящий Порядок разработан с целью:

— определения категории информации, подлежащей обязательному резервному копированию;

— определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

— определения порядка восстановления информации в случае возникновения такой необходимости;

— упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности сегмента ГИС ЕИБД в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

— персональная информация пользователей (личные каталоги) и групповая информация на файловых серверах;

— информация, обрабатываемая пользователями в сегменте ГИС ЕИБД, а также информация, необходимая для восстановления работоспособности сегмента ГИС ЕИБД, в т.ч. систем управления базами данных (далее - СУБД) общего пользования и справочно-информационные системы общего использования;

— рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения сегмента ГИС ЕИБД, СУБД, серверов и рабочих станций;

— информация, необходимая для восстановления серверов и систем управления базами данных сегмента ГИС ЕИБД, локальной вычислительной сети, системы электронного документооборота;

— регистрационная информация системы информационной безопасности сегмента ГИС ЕИБД;

— другая информация сегмента ГИС ЕИБД, являющаяся по мнению пользователей и администратора безопасности критичной для работоспособности сегмента ГИС ЕИБД.

1.5. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.6. Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники, указанные в Перечне пользователей, допущенных к обработке информации и лиц, допущенных в помещение сегмента ГИС ЕИБД. Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на

основании Заявки. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности (далее – ИБ), произошедших в процессе резервного копирования, сообщается администратору ИБ.

II. Общие требования к резервному копированию

2.1. В Регламенте резервного копирования описываются действия при выполнении следующих мероприятий:

— резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

— контроль резервного копирования:

— хранение резервных копий;

— полное или частичное восстановление данных.

2.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

— это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

— имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:

— обеспечивает выполнение функций, перечисленных в п. 2.1;

— средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. Требования к программному обеспечению систем резервного копирования:

— лицензионное системное программное обеспечение и программное обеспечение резервного копирования;

— программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.5. Сопровождение системы резервного копирования возлагается на уполномоченных работников, которые обязаны следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

2.6. Предварительный учет магнитных носителей архивных копий производится в отдельном журнале учета магнитных носителей для архивного копирования, который находится у администратора ИБ. Все магнитные

носители с архивными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.7. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора ИБ.

2.8. Доступ к носителям архивных копий имеют только уполномоченные работники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.9. Магнитные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета магнитных носителей архивных копий. Передача магнитных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

2.10. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

III. Ответственность за состояние резервного копирования

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на уполномоченных работников, осуществляющих резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора ИБ.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается администратору ИБ.

IV. Периодичность резервного копирования

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4.3. Информация и персональные данные, содержащаяся в постоянно изменяемых базах данных сегмента ГИС ЕИБД, сохраняется в соответствии со следующим графиком:

— ежемесячно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;

— ежеквартально проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

— ежегодно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

Резервное копирование информации проводится уполномоченным лицом Федерального государственного бюджетного учреждения здравоохранения «Центр крови Федерального медико-биологического агентства».

V. Ротация носителей резервной копии

5.1. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации сегмента ГИС ЕИБД в случае отказа любого из устройств резервного копирования.

5.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным работником. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

VI. Восстановление информации из резервных копий

6.1. В случае необходимости восстановление данных из резервных копий производится ответственным работником.

6.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

6.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Приложение № 10
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

СОГЛАСИЕ ПАЦИЕНТА (ДОНОРА)
на обработку персональных данных, включая биометрических персональные данные

Я,

_____,
(фамилия, имя, отчество полностью)

паспорт серии _____, номер _____, выдан _____.

_____

____проживающий (ая) по адресу:

_____

_____

____

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152 - ФЗ «О персональных данных», предоставляю _____ (далее – Оператор) расположенному по адресу: _____, свое согласие на обработку моих персональных данных, включающих: фамилию, имя, отчество; место и дату рождения; регистрацию по месту жительства; адрес проживания (фактический); телефонный номер (домашний, рабочий, мобильный); адрес электронной почты; личную фотографию; паспортные данные (серия, номер паспорта, кем и когда выдан); информацию о трудовой деятельности (место работы или учебное заведение, должность), группу крови, резус-принадлежность, информацию об исследованных антигенах и о наличии иммунных антител; состав и биохимические показатели периферийной крови; информацию о состоянии здоровья (сведения о заболеваниях и отводах от донорства: СПИД, наличие ВИЧ-инфекции, сифилис, вирусные гепатиты, туберкулез, болезни крови), информацию о перенесенных инфекционных заболеваниях, нахождении в контакте с инфекционными больными, пребывании на территориях, на которых существует угроза возникновения и (или) распространения массовых инфекционных заболеваний или эпидемий, об употреблении наркотических средств, психотропных веществ, о работе с вредными и (или) опасными условиями труда, а также вакцинациях и хирургических вмешательствах, выполненных в течение года до даты сдачи крови и (или) ее компонентов; информация о предыдущих донациях; информация о награждении нагрудными знаками "Почетный донор СССР" и "Почетный донор России"; биометрические персональные данные (это физиологические, биологические характеристики человека, позволяющие идентифицировать его личность).

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, передавать в необходимом объеме в Федеральное государственное бюджетное учреждение здравоохранения «Центр крови Федерального медико-биологического агентства» (ФГБУЗ Центр крови ФМБА России) на основании: Федерального закона № 125-ФЗ от 20.07.2012 «О донорстве крови и ее компонентов»; Трудового кодекса Российской Федерации, статьи 121, 139, 165, 186; приказа Минздрава РФ от 28.10.2020 г. № 1166н «Об утверждении порядка прохождения донорами медицинского обследования и перечня медицинских противопоказаний (временных и постоянных) для сдачи крови и (или) ее компонентов и

ОБРАЗЕЦ

сроков отвода, которому подлежит лицо при наличии временных медицинских показаний, от донорства крови и (или) ее компонентов».

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва.

Подпись субъекта персональных данных _____

Дата составления согласия _____

ОБРАЗЕЦ

Приложение № 11
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 197

ИНСТРУКЦИЯ
по антивирусной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

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

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
ПДн	– персональные данные
СЗИ	– система защиты информации
СрЗИ	-- средство защиты информации
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю России

I. Общие положения

1.1. Настоящая Инструкция по антивирусной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее - Инструкция) предназначена для администратора ИБ, ответственного за организацию обработки информации и персональных данных, и пользователей сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.2. Инструкция устанавливает требования и ответственность администраторов и пользователей при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3. Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в сегменте ГИС ЕИБД.

II. Требования по обеспечению антивирусной защиты

2.1. Требования к порядку организации антивирусной защиты.

2.1.1. Для организации антивирусной защиты сегмента ГИС ЕИБД допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2. Приобретение и установка (обновление) антивирусных программных средств осуществляется в установленном порядке. Не реже чем два раза в месяц Администратор ИБ должен производить обновление антивирусных баз, получая их из официальных источников. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за организацию обработки информации и персональных данных в сегменте ГИС ЕИБД с привлечением (при необходимости) администратора ИБ и/или специалистов лицензированной организации.

2.1.3. Должностные лица не должны допускать использования в сегменте ГИС ЕИБД программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.2. Требования к порядку проведения антивирусного контроля.

2.2.1. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором ИБ на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ – администратором ИБ;
- на других серверах и АРМ не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

2.2.2. При загрузке компьютера должен проводиться антивирусный контроль в автоматическом режиме. Порядок и периодичность расширенного антивирусного контроля и других необходимых антивирусных проверок определяется администратором ИБ на этапе планирования мероприятий установленным порядком (не реже одного раза в месяц и при необходимости, в случае появления подозрений в заражении вирусной программой).

2.2.3. Обязательному дополнительному антивирусному контролю подлежит любая информация на съемных машинных носителях информации, поступающая для обработки в сегменте ГИС ЕИБД. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель информации).

2.2.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с администратором ИБ должен провести внеочередной антивирусный контроль своей рабочей станции для определения ими факта наличия или отсутствия компьютерного вируса.

2.2.5. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора ИБ, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске администратору ИБ для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору ИБ, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

III. Ответственность при организации антивирусной защиты

3.1. Ответственность за организацию антивирусной защиты и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на администратора ИБ.

3.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на ответственного за организацию обработки информации и персональных данных и пользователей сегмента ГИС ЕИБД.

Приложение № 12
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
по парольной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

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

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности сегмента ГИС ЕИБД
АРМ	– автоматизированное рабочее место
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность

I. Общие положения

1.1. Данная Инструкция по парольной защите в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее - Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови

и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

II. Требования по организации парольной защиты

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в сегменте ГИС ЕИБД и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности (далее – администратор ИБ), содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями сегмента ГИС ЕИБД самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 12 символов для привилегированных учетных записей (административных) и не менее 8 символов для учетных записей пользователей ИС;
- алфавит пароля - не менее 70 символов букв английского и(или) русского алфавита верхнего и нижнего регистра, цифр и специальных символов;
- количество последовательных попыток введения неверного пароля должно быть строго ограничено. После 5 (пяти) неуспешных попыток введения пароля должна выполняться временная блокировка учетной записи пользователя не менее чем на 15 минут;
- в числе символов пароля обязательно должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы (S,r,0-9,@, #,%,*, $, и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 2-х позициях;
- личный пароль пользователь ИС не имеет права сообщать никому.

2.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора ИБ. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

2.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

2.5. Блокировка программно-технических средств ГИС ЕИБД ФГБУЗ Центр крови ФМБА России или учетной записи пользователя в случае достижения

установленного максимального количества неуспешных попыток аутентификации должна составлять от 3 до 15 минут

2.6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора ИБ и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой в сегменте ГИС ЕИБД.

2.8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 2.6 или п. 2.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.9. Хранение значений паролей на бумажном носителе допускается только в опечатанном печатью конверте в сейфе у Администратора ИБ.

2.10. При вводе пароля пользователю сегмента ГИС ЕИБД, необходимо исключить (затруднить) возможность его компрометации, а именно: не произносить пароль вслух; исключить возможность его подсматривания посторонними лицами, исключить (затруднить) фото/видеосъемку техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.). Вводимые символы пароля должны отображаться условными знаками «*», «•» или иными знаками.

2.11. Временные пароли, заданные при модернизации системы защиты информации сегмента ГИС ЕИБД работниками сторонних организаций, рекомендуется изменить при первом входе в систему.

2.12. Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

III. Правила использования пароля

3.1. Пароль должен быть известен только его владельцу. Запрещается сообщать пароль кому бы то ни было, в том числе администраторам систем и другим пользователям.

3.2. Работники обязаны обеспечить конфиденциальность своих паролей.

3.3. При покидании рабочего места более чем на 5 минут пользователь обязан заблокировать свой компьютер.

3.4. В случае компрометации (факт ознакомления с паролем лица, не являющегося его владельцем) пароля или подозрении на компрометацию пользователь обязан уведомить об этом Администратора ИБ и незамедлительно

сменить свой пароль.

IV. Требования к конфиденциальности паролей

4.1. Запрещено хранить пароли в открытом или общедоступном виде.

4.2. Запрещается разглашение паролей после прекращения их действия.

4.3. Запрещается использовать чужие идентификаторы и пароли, а также осуществлять их подбор.

V. Выдача/изменение паролей пользователей

5.1. Пароли функциональных пользователей могут выдаваться/изменяться:

- при принятии нового работника;
- по истечении срока действия пароля;
- в процессе восстановления доступа;
- при изменении пароля пользователем;
- при компрометации пароля;
- другие случаи, требующие выдачи/изменения пароля.

5.2. Изменение паролей функциональных пользователей может осуществляться в двух режимах:

- плановое изменение пароля;
- внеплановое изменение пароля.

5.3. Плановое изменение паролей в сегменте ГИС ЕИБД должно проводиться Администратором ИБ в соответствии с требованиями эксплуатационной и организационно - распорядительной документации на сегмента ГИС ЕИБД, нормативных правовых, правовых актах, регламентирующих эксплуатацию сегмента ГИС ЕИБД, но:

- не реже 1 раза в 360 дней для учетных записей пользователей;
- не реже 1 раза в 180 дней для привилегированных учетных записей.

5.4. Внеплановое изменение паролей учетных записей пользователей в сегменте ГИС ЕИБД может проводиться по инициативе Администратора ИБ после обнаружения фактов попыток несанкционированного доступа, компрометации или возникновения подозрения на компрометацию пароля либо других нештатных ситуаций, в случае прекращения полномочий (увольнение, перевод на другую должность) привилегированных пользователей сегмента ГИС ЕИБД и других случаях, требующих изменения паролей.

5.5. Для привилегированных учетных записей внеплановое изменение паролей может также производиться перед значимыми мероприятиями, для организации (проведения) которых планируется задействовать функционал сегмента ГИС ЕИБД.

5.6. Во всех случаях выдачи/изменения пароля, за исключением случаев истечения срока действия пароля и изменения пароля пользователем, функциональному пользователю назначается временный пароль. Временный пароль передается функциональному пользователю в соответствии с требованиями

настоящей Политики. После чего функциональным пользователем при первом входе в сегмент ГИС ЕИБД временный пароль должен быть изменен в соответствии с требованиями раздела 3 настоящей Политики.

5.7. По истечении срока действия пароля функциональный пользователь сегмента ГИС ЕИБД обязан произвести изменение пароля в соответствии с требованиями настоящей Политики.

5.8. Порядок выдачи/изменения паролей публичных пользователей, системных (технологических) учетных записей определяется Администратором ИБ с учетом требований настоящей Политики эксплуатационной и организационно-распорядительной документации сегмента ГИС ЕИБД или в нормативных, правовых актах, регламентирующих эксплуатацию сегмента ГИС ЕИБД.

5.9. Порядок выдачи/изменения паролей учетных записей суперпользователей (root, Administrator) определяется Администратором с учетом требований настоящей Политики эксплуатационной и организационно-распорядительной документации сегмента ГИС ЕИБД или в нормативных правовых актах, регламентирующих эксплуатацию сегмента ГИС ЕИБД.

VI. Контроль

6.1 Администратор ИБ на постоянной основе обеспечивает проведение контроля действий пользователей сегмента ГИС ЕИБД при работе с паролями, а также обеспечивает контроль за актуальностью учетных записей пользователей и их прав доступа в сегмент ГИС ЕИБД.

6.2 Администратор ИБ на постоянной основе обеспечивает проведение анализа журналов событий доступа привилегированных учетных записей, системных (технологических) учетных записей, учетных записей суперпользователей (root, Administrator) на предмет попыток нелегитимного доступа, и инициирует процедуру изменения пароля в случае подозрения на его компрометацию.

6.3 Администратор ИБ обеспечивает проведение периодического контроля соблюдения требований, установленных настоящей Инструкцией.

VII. Ответственность за организацию парольной защиты

7.1. Ответственность за организацию парольной защиты в сегменте ГИС ЕИБД и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на администратора ИБ.

7.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на ответственного за организацию обработки информации и персональных данных и пользователей сегмента ГИС ЕИБД.

7.3. Периодический контроль за выполнением всех требований настоящей Инструкции и состоянием антивирусной защиты осуществляется администратором ИБ.

Приложение № 13
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
о порядке обращения с носителями информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.
Персональные данные – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных).

Обозначения и сокращения

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
МНИ	– машинные носители информации
ПДн	– персональные данные

I. Особенности учета носителей, содержащих защищаемую информацию

1.1. Съемные машинные носители информации (далее - МНИ) (дискеты, съемные накопители информации большой емкости,

магнитооптические диски и т.д.), предназначенные для обработки защищаемой информации, учитываются по журналу учета МНИ работником, ответственным за организацию обработки информации и персональных данных в сегменте ГИС ЕИБД.

1.2. На съемных МНИ любым доступным способом в удобном для просмотра месте проставляются следующие учетные реквизиты: учетный номер и дата выдачи, пометка "Для служебного пользования", подпись работника, ответственного за организацию обработки информации и персональных данных в сегменте ГИС ЕИБД.

1.3. Учтенные МНИ передаются работникам под расписку в журнале учета МНИ.

1.4. МНИ, пришедшие в негодность, неисправные или потерявшие практическую ценность, уничтожаются по акту.

1.5. Порядок обращения с МНИ идентичен порядку хранения и уничтожения носителей информации (Положение о порядке хранения и уничтожения носителей информации).

II. Организация работ при обработке защищаемой информации на средствах вычислительной техники

2.1. Работники, осуществляющие обработку защищаемой информации на средствах вычислительной техники, несут ответственность за соблюдение порядка подготовки и обработки документов, содержащих такую информацию, с помощью средств вычислительной техники.

2.2. Обеспечение защиты информации при ее обработке на средствах вычислительной техники осуществляется в соответствии с требованиями настоящей Инструкции, приказов и распоряжений уполномоченного лица по вопросам защиты информации.

III. Эксплуатация хранилищ с носителями информации

3.1. Носители информации должны храниться в защищаемых хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

IV. Ответственность

4.1. Пользователи сегмента ГИС ЕИБД несут персональную ответственность за сохранность полученных носителей информации, за соблюдение положений настоящей Инструкции.

4.2. Ответственный за организацию обработки информации и персональных данных в сегменте ГИС ЕИБД несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки защищаемой информации с носителей информации настоящей Инструкции.

Приложение № 14
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
пользователя системы защиты информации сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных);

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

Обозначения и сокращения

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
НСД	– несанкционированный доступ
ПДн	– персональные данные
СЗИ	– система защиты информации
СрЗИ	– средство защиты информации
ФСБ России	– Федеральная служба безопасности России
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю России

I. Общие положения

1.1. Инструкция пользователя системы защиты информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации, обрабатываемой с использованием средств автоматизации.

II. Обязанности пользователя

2.1. Пользователь сегмента ГИС ЕИБД обязан:

2.1.1. Хранить в тайне информацию, ставшую ему известной во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать ответственного за организацию обработки информации и персональных данных, администратора ИБ.

2.1.2. При определении защищаемой информации, подлежащей защите, использовать документ «Перечень обрабатываемой информации и ПДн».

2.1.3. Знать и выполнять правила работы со средствами защиты информации (далее – СрЗИ), используемыми на персональных компьютерах в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных СрЗИ.

2.1.4. Хранить в тайне свой пароль доступа в сегменте ГИС ЕИБД, а также информацию о системе защиты, установленной в сегменте ГИС ЕИБД.

2.1.5. Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски, флешки и т.д.).

2.1.6. Сообщать о необходимости обновления антивирусных баз администратору ИБ.

2.1.7. Немедленно ставить в известность администратора ИБ:

- в случае утери носителя с конфиденциальной информацией и/или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа (далее - НСД);

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств.

2.1.8. В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных СрЗИ ставить в известность администратора ИБ.

2.2. В случае увольнения пользователь обязан вернуть все документы и материалы, относящиеся к деятельности организации. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности сегмента ГИС ЕИБД, полученные в течение срока работы.

2.3. Уборка помещений должна производиться под контролем пользователя, имеющего доступ в помещение и постоянно в нем работающего.

2.3.1. Вынос технических средств, на которых проводилась обработка защищаемой информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с ответственным за организацию обработки информации и персональных данных запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.3.2. АРМ, используемые для работы с защищаемой информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора.

2.4. Пользователю категорически запрещается:

– передавать кому бы то ни было, устно или письменно, защищаемую информацию;

– использовать защищаемую информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

– выполнять работы с документами, содержащими защищаемую информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения ответственного за организацию обработки информации и персональных данных;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие защищаемую информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими защищаемую информацию;

– использовать компоненты программного и аппаратного обеспечения сегмента ГИС ЕИБД в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию технических средств сегмента ГИС ЕИБД в части установки программных и аппаратных средств;

- осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора ИБ.

2.5. Принимать меры по реагированию в случае возникновения внештатных ситуации и аварийных ситуаций с целью ликвидации их последствий в пределах, возложенных на него функций.

2.6. Оперативно докладывать администратору ИБ о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.7. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов сегмента ГИС ЕИБД.

2.8. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

III. Права пользователя

3.1. Пользователь имеет право:

3.1.1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

IV. Ответственность пользователя

4.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации. За разглашение защищаемой информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

4.2. За разглашение защищаемой информации, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Приложение № 15
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
ответственного за организацию обработки информации и персональных данных

Определения

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации.

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

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных);

Обозначения и сокращения

АРМ	– автоматизированное рабочее место
НСД	– несанкционированный доступ
ОСК	– объект службы крови
ПДн	– персональные данные
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

I. Общие положения

1.1. Инструкция ответственного за организацию обработки информации и персональных данных определяет функции, права и обязанности ответственного за организацию обработки информации и персональных данных по вопросам обеспечения информационной безопасности при подготовке и исполнении документов на автоматизированных рабочих местах (далее – АРМ) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.2. Ответственный за организацию обработки информации и персональных данных назначается из числа работников объекта Службы крови (далее – ОСК) и обеспечивает безопасность информации и персональных данных (далее – ПДн), обрабатываемых, передаваемых и хранимых в сегменте ГИС ЕИБД.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4. Ответственному за организацию обработки информации и персональных данных предоставляются права доступа к любым средствам защиты информации на АРМ в сегменте ГИС ЕИБД по согласованию с уполномоченным лицом в Федеральном государственном бюджетном учреждении здравоохранения «Центр крови Федерального медико-биологического агентства» (за исключением информации, закрытой с использованием средств криптозащиты).

II. Основные функции ответственного за организацию обработки информации и персональных данных

2.1. Контроль выполнения требований действующего законодательства в сфере обеспечения безопасности ПДн.

2.2. Планирование мероприятий по организации обеспечения безопасности ПДн.

2.3. Организация мероприятий, направленных на предотвращение несанкционированного доступа (далее – НСД) к ПДн или передача их лицам, не имеющим права доступа к такой информации.

2.4. Организация постоянного контроля за обеспечением уровня (в случае государственных информационных систем - класса) защищенности ПДн.

2.5. Проведение периодического контроля эффективности мер защиты ПДн.

2.6. Рассмотрение предложений по устранению недостатков и предупреждению нарушений в системе защиты ПДн, осуществление контроля за устранением нарушений.

III. Обязанности ответственного за организацию обработки информации и персональных данных

3.1. Ответственный за организацию обработки информации и персональных данных обязан:

3.2. Осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

3.3. Доводить до работников положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

3.4. Осуществлять планирование и проведение организационных мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн;

3.5. Знать, соблюдать и обеспечивать соблюдение пользователями порядка и правил уничтожения носителей ПДн, входить в состав комиссии по уничтожению носителей ПДн;

3.6. Проводить регулярный инструктаж пользователей по правилам работы с ПДн;

3.7. Совместно с администратором информационной безопасности проводить периодический контроль эффективности мер защиты ПДн.

IV. Права ответственного за организацию обработки информации и персональных данных

4.1. Ответственный за организацию обработки информации и персональных данных имеет право:

4.1.1. Требовать от пользователей и обслуживающего персонала соблюдения установленных правил обработки ПДн;

4.1.2. Участвовать в анализе инцидентов, касающихся функционирования средств защиты информации и расследования фактов НСД к ПДн;

4.1.3. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

V. Ответственность

5.1. Ответственный за организацию обработки информации и персональных данных несет ответственность за:

5.1.1. ненадлежащее выполнение своих обязанностей;

5.1.2. разглашение состава и содержания комплекса организационно-технических мероприятий по защите ПДн субъектам, не принимающим участие в обработке;

5.1.3. разглашение ПДн, ставших известными ему в ходе выполнения функциональных (должностных) обязанностей.

Приложение № 16
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
администратора информационной безопасности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации.

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

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

Обозначения и сокращения

АРМ	– автоматизированное рабочее место
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИС	– информационная система
НСД	– несанкционированный доступ
СЗИ	– система защиты информации
СрЗИ	– средство защиты информации

I. Общие положения

1.1. Инструкция администратора информационной безопасности определяет функции, права и обязанности администратора информационной

безопасности (далее – администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов на автоматизированных рабочих местах (далее – АРМ) в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.2. Администратор ИБ назначается из числа работников объекта Службы крови и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4. Администратору ИБ предоставляются права доступа к любым средствам защиты информации на АРМ в сегменте ГИС ЕИБД по согласованию с уполномоченным лицом в Федеральном государственном бюджетном учреждении здравоохранения «Центр крови Федерального медико-биологического агентства» (за исключением информации, закрытой с использованием средств криптозащиты).

II. Обязанности администратора ИБ

2.1. Администратор ИБ обязан:

2.1.1. Знать перечень установленных АРМ в сегменте ГИС ЕИБД и перечень задач, решаемых с их использованием.

2.1.2. Осуществлять учет и периодический контроль за составом и полномочиями пользователей АРМ сегмента ГИС ЕИБД.

2.1.3. Осуществлять оперативный контроль за работой пользователей АРМ сегмента ГИС ЕИБД, анализировать содержимое системных журналов всех АРМ сегмента ГИС ЕИБД и адекватно реагировать на возникающие нештатные ситуации.

2.1.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на АРМ средств защиты информации от несанкционированного доступа (далее – СрЗИ от НСД).

2.1.5. Присутствовать при внесении изменений в конфигурацию (модификацию) АРМ и серверов.

2.1.6. Периодически проверять состояние используемых СрЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.7. Докладывать руководству об имевших место попытках НСД к информации и техническим средствам АРМ.

2.1.8. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СрЗИ от НСД, установленных на АРМ.

2.1.9. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.1.10. Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.1.11. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.1.12. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов сегмента ГИС ЕИБД.

2.1.13. Предпринимаемые меры по возможности должны согласовываться с вышестоящим руководством.

2.1.14. Выполнять обязанности ответственного за выявление инцидентов и реагирование на них, в рамках своих полномочий (П 1).

2.1.15. Объективно и основательно проводить разбирательство каждого Инцидента.

2.1.16. Определять первоочередные меры, направленные на локализацию Инцидента и минимизацию негативных последствий.

2.1.17. Фиксировать в журнале учета инцидентов (П 2) и карточке данных «Инцидент ИБ» (П 4) всю исходную информацию об Инциденте и результаты его расследования.

2.1.18. Представлять отчеты и рекомендации по проведенным разбирательствам.

2.1.19. Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента, и на его основе разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов и минимизации возможности их повторения в будущем.

2.1.20. Производить планирование и принятие мер по предотвращению повторного возникновения Инцидентов (П 3).

2.1.21. Составлять заключения по фактам несоблюдения условий хранения носителей защищаемой информации, использования средств защиты информации, приводящим к снижению уровня защищенности информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

III. Права администратора ИБ

3.1. Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов сегмента ГИС ЕИБД.

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ГИС ЕИБД при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. Вносить свои предложения по совершенствованию мер защиты в сегменте ГИС ЕИБД.

3.1.4. По согласованию с непосредственным руководителем требовать предоставлений письменных объяснений по обстоятельствам Инцидента у нарушителя ИБ.

3.1.5. Запрашивать и получать от руководителей и сотрудников, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента.

3.1.6. Инициировать на основании заявок отключение от сегмента ГИС ЕИБД пользователей, нарушивших правила или требования ИБ, на период проведений расследования Инцидента в случае, если имеется существенный риск того, что продолжение работы пользователя может повлечь значительное увеличение ущерба или новые Инциденты.

3.1.7. Инициировать процедуры привлечения нарушителя ИБ к дисциплинарной или материальной ответственности согласно внутренним нормативным документам.

IV. Ответственность администратора ИБ

4.1. На Администратора ИБ возлагается персональная ответственность за СрЗИ, средства вычислительной техники, информационно-вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним приказом уполномоченного лица и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

4.2. Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений, составляющих коммерческую тайну, и сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение № 1

к Инструкции администратора информационной безопасности

ПОЛОЖЕНИЕ
по выявлению инцидентов информационной безопасности и реагирования на них в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

1. Общие положения

1.1 Положение разработано в соответствии с нормативно-правовыми документами:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2 Обнаружение, идентификация и регистрация Инцидентов проводится администратором ИБ.

1.3 Под Инцидентом понимается любое нарушение требований по обеспечению информационной безопасности (далее – ИБ), включая следующий перечень:

- неавторизованный доступ к информационным ресурсам сегмента ГИС ЕИБД;
- несанкционированное удаление или модификация данных в сегменте ГИС ЕИБД;
- несанкционированное изменение прав доступа пользователя сегмента ГИС ЕИБД;
- распространение компьютерных вирусов, внедрение в сегмент ГИС ЕИБД «троянских коней» и иного вредоносного программного обеспечения;
- осуществление сетевых атак на сегмент ГИС ЕИБД;
- хищение или разглашение защищаемой информации;
- преднамеренный вывод из строя либо разрушение технических средств;
- хищение технических средств;
- нелегальное проникновение в помещения сегмента ГИС ЕИБД;
- другие инциденты.

2. Обнаружение Инцидента

2.1. Основными источниками информации об Инцидентах являются:

- факты, выявленные руководителями структурных подразделений, администратором ИБ, а также другими пользователями сегмента ГИС ЕИБД.
- результаты работы средств мониторинга ИБ (средств анализа защищенности), результаты проверок и аудита (внутреннего или внешнего);
- другие источники информации.

2.2. Пользователь сегмента ГИС ЕИБД может выявить признаки наличия Инцидента путем анализа текущей ситуации на предмет ее соответствия требованиям утвержденных в организационно-распорядительных документах организации. Выявленные несоответствий дают основания предполагать факт возникновения Инцидента. Любые сведения об Инциденте должны быть незамедлительно переданы администратору ИБ

3. Анализ Инцидента

3.1. Администратор ИБ после получения информации о предполагаемом Инциденте незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа полученных данных администратор ИБ проводит проверку наличия нарушений (признаков Инцидента). После подтверждения факта наличия Инцидента, администратор ИБ вносит его в журнал учета инцидентов и заводит на Инцидент карточку «Инцидент ИБ».

3.2. По усмотрению администратора ИБ единичный Инцидент, не приведший к негативным последствиям, фиксируется в карточке данных «Инцидент ИБ» с присвоением статуса «Разбирательство не требуется».

3.4. В случае наличия признаков Инцидента в полученной информации, администратор ИБ определяет предварительную степень важности Инцидента и принимает решение о необходимости проведения разбирательства, информирует непосредственного руководителя и инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте, администратор ИБ по согласованию с непосредственным руководителем определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

4. Разбирательство Инцидента

4.1 Цели и этапы разбирательства Инцидента:

4.1.1. Целями разбирательства Инцидентов являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения ИБ, предотвращение и минимизацию подобных нарушений в будущем;
- обеспечение безопасности защищаемой информации;

- предотвращение несанкционированного доступа к защищаемой информации и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство Инцидента, состоит из следующих этапов:

- подтверждение/опровержение факта возникновения Инцидента;
- подтверждение/корректировка уровня значимости Инцидента;
- уточнение дополнительных обстоятельств (деталей) Инцидента;
- получение (сбор) доказательств возникновения Инцидента, обеспечение их сохранности и целостности;
- минимизация последствий Инцидента;
- разработка мероприятий по обнаружению и/или предупреждению инцидентов.

4.2 Порядок проведения разбирательства Инцидента:

4.2.1. В процессе проведения разбирательства Инцидента обязательными для установления являются:

- дата и время совершения Инцидента;
- ФИО, должность и подразделение Нарушителя;
- уровень критичности Инцидента;
- обстоятельства и мотивы совершения Инцидента;
- информационные ресурсы, затронутые Инцидентом;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению Инцидента.

4.2.2. При Инциденте, затрагивающем не более одного структурного подразделения, администратор ИБ информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При Инциденте, затрагивающим более одного структурного подразделения, администратор ИБ информирует руководителей соответствующих структурных подразделений.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя, информация об отключении прав доступа администратором ИБ направляется руководителю предполагаемого нарушителя.

4.2.5. Администратор ИБ в процессе проведения расследования Инцидента при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по Инциденту администратор ИБ проводит анализ полученных данных и оценку негативных последствий от реализации Инцидента. В ходе данной оценки учитываются:

- прямой финансовый ущерб;
- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба.

4.2.7. С целью минимизации последствий Инцидента возможно временное отключение прав доступа пользователя к сегменту ГИС ЕИБД на время проведения расследования. Подобное отключение инициируется администратором ИБ с обязательным согласованием с руководителем сегмента ГИС ЕИБД.

5. Оформление результатов проведенного разбирательства

5.1 Собранная в процессе разбирательства Инцидента информация фиксируется в картотеке данных «Инцидент ИБ» и учитывается при подготовке итогового заключения по Инциденту.

5.2 Администратор ИБ формирует итоговое заключение по расследованию Инцидента и согласовывает со всеми участниками разбирательства.

5.3 Итоговое заключение по Инциденту Администратор ИБ направляет непосредственному руководителю.

5.4 Администратор ИБ фиксирует завершение разбирательства в карточке «Инцидент ИБ» и присваивает инциденту статус «Разбирательство завершено».

6. Планирование и принятие мер по предотвращению повторного возникновения Инцидентов

6.1 По завершению разбирательства Инцидента, Администратор ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю для решения вопроса о целесообразности привлечения нарушителя к дисциплинарной ответственности.

6.2 На основании полученных результатов разбирательства Администратор ИБ организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем.

6.3. Планирование и принятие мер по предотвращению повторного возникновения Инцидентов основывается на:

- планомерной деятельности по повышению уровня осознания ИБ пользователями сегмента ГИС ЕИБД;
- проведении мероприятий по обучению пользователей сегмента ГИС ЕИБД правилам и способам работы со средствами защиты информации;
- доведении до пользователей сегмента ГИС ЕИБД норм законодательства и организационно-распорядительных документов, устанавливающих ответственность за нарушение требований ИБ;
- своевременной модернизации системы обеспечения ИБ, с учетом возникновения новых угроз ИБ;
- своевременном обновлении программного обеспечения, средств защиты информации.

6.4. В работе с персоналом основной упор должен делаться на

поощрение за надлежащие выполнение требований ИБ, проявление личной инициативы в укреплении системы ИБ.

6.5 Результатом планирования мероприятий по предотвращению повторного возникновения Инцидентов является «План мероприятий по предотвращению повторного возникновения инцидентов» (далее – План). План должен включать перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий выявленных Инцидентов и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

П 2

к Инструкции администратора информационной безопасности

ЖУРНАЛ
учета инцидентов информационной безопасности
в сегменте федеральной государственной информационной системы
«Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

№	Дата и время выявления инцидента	ФИО сотрудника, обнаружившего инцидент	Описание инцидента	ФИО ответственного за выявление инцидентов (Администратора ИБ)	Номер в карточке «Инцидент ИБ»	Результат исследования инцидента	Подпись ответственного за выявление инцидентов информационной безопасности и реагирования на них
1							
2							
3							
4							
5							
6							
7							
8							

П 3

к Инструкции администратора информационной безопасности

ПЛАН
мероприятий по предотвращению повторного возникновения инцидентов в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

№	Наименование работ	Наименование мероприятия	Сроки выполнения	Ответственный	Документальное оформление результатов работ
1.	Повышение квалификации персонала. Проверка знаний пользователями информационной системы норм законодательства в области информационной безопасности	Повышение квалификации администратора информационной безопасности	Ежегодно	Ответственный за организацию обработки информации и персональных данных.	– Свидетельство о повышении квалификации (сертификат). – Журнал учета проведения инструктажа пользователей информационной системы.
		Повышение квалификации ответственного пользователя криптосредств			
		Повышение квалификации ответственного за организацию обработки информации и персональных данных			
		Повышение квалификации ответственного за выявление инцидентов и реагирование на них			
		Повышение квалификации пользователей информационной системы			
2.	Проверка обновлений программного обеспечения и средств защиты информации	Проверка обновления прикладного программного обеспечения	Ежеквартально	Администратор информационной безопасности. Ответственный пользователь криптосредств	– Журнал обновлений программного обеспечения и средств защиты информации.
		Проверка обновления операционных систем			
		Проверка обновления средств защиты информации (включая средства защиты информации от несанкционированного доступа, средства защиты информации от вредоносного кода, системы обнаружения и предотвращения вторжений, средства анализа защищенности)			
3.	Анализ защищенности информационной системы	Проверка информационной системы на наличие уязвимостей (выявление уязвимостей)	Ежеквартально	Администратор информационной безопасности.	– Отчет по результатам анализа защищенности информационной системы.
		Анализ защищенности информационной системы и оперативное устранение выявленных уязвимостей			

№	Наименование работ	Наименование мероприятия	Сроки выполнения	Ответственный	Документальное оформление результатов работ
		Контроль соблюдения пользователями информационной системы требований информационной безопасности			
4.	Актуализация организационно-распорядительных документов в области информационной безопасности	Актуализация перечня лиц, ответственных за обеспечение информационной безопасности. Актуализация приказов о назначении ответственных лиц.	Ежеквартально	Ответственный за организацию обработки информации и персональных данных. Администратор информационной безопасности.	– Приказы о назначении ответственных лиц. – Перечни (списки) лиц, допущенных к работе в информационной системе. – Перечни (списки) лиц, допущенных в помещения информационной системы. – Пакет организационно-распорядительной документации. – Модель угроз и нарушителя информационной безопасности информационной системы.
		Актуализация организационно-распорядительной документации, описывающей систему защиты информации информационной системы.			
		Пересмотр актуальных угроз информационной безопасности в информационной системе			

П 4

к Инструкции администратора информационной безопасности

Карточка данных об инциденте

Дата события

Номер события[1]:

(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

Информация о сообщающем лице

Фамилия _____ Адрес _____

Организация _____ _____

Телефон _____ Электронная почта _____

_____

Описание события ИБ

Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на бизнес
- Любые идентифицированные уязвимости

Детали события ИБ

Дата и время возникновения события

Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? *(отметить квадрат)* Да ☐ Нет ☐

Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

[1] (Номера событий назначаются руководителем)

Дата инцидента
Номер инцидента[2]:

(Если требуется) соответствующие идентификационные номера событий и (или) инцидентов:

Информация о сотруднике группы обеспечения эксплуатации

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Информация о сотруднике

Фамилия _____ Адрес _____
Телефон _____ Электронная почта _____

Описание инцидента ИБ

Дальнейшее описание инцидента:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на бизнес
- Любые идентифицированные уязвимости

Детали инцидента ИБ

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? *(отметить квадрат)* Да ☐ Нет ☐

Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится

[2] (Номера инцидентов назначаются руководителем)

Тип инцидента ИБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже) **Действительный** ☐ **Попытка** ☐ **Подозрение** ☐

(Один из) **Намеренная** ☐ *(указать типы угрозы)*

Хищение (TH)	☐	Хакерство/Логическое проникновение (HA)	☐
Мошенничество (FR)	☐	Неправильное использование ресурсов (MI)	☐
Саботаж/физический ущерб (SA)	☐	Другой ущерб (OD)	☐
Вредоносная программа (MC)	☐		

Определить:

(Один из) **Случайная** ☐ *(указать типы угрозы)*

Отказ аппаратуры (HF)	☐	Другие природные события (NE)	☐
Отказ ПО (SF)	☐	*Определить:*	
Отказ связи (CF)	☐	Потеря существенных сервисов (LE)	☐
Пожар (HE)	☐	Недостаточное кадровое обеспечение (SS)	☐
Наводнение (FL)	☐	Другие случаи (OA)	☐

Определить:

(Один из) **Ошибка** ☐ *(указать типы угрозы)*

Операционная ошибка (OE)	☐	Ошибка пользователя (UE)	☐
Ошибка аппаратной поддержки (HE)	☐	Ошибка конструкции (DE)	☐
Ошибка поддержки ПО (SE)	☐	Другие случаи (включая истинные заблуждения) (OA)	☐

Определить:

Неизвестно ☐

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)

Определить:

Пораженные активы

Пораженные активы (если есть) *(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)*

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента на бизнес

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 1÷10, используя сокращения (указатели категорий): (FD) – финансовые потери/разрушение бизнес-операций, (CE) – коммерческие и экономические интересы, (PI) – информация, содержащая персональные данные, (LR) – правовые и нормативные обязательства (это необходимо сличить с английским оригиналом), (MO) – менеджмент и бизнес-операции, (LG) – потеря престижа Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»

		Значимость	Указатели	Стоимость
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	☐			
Нарушение целостности *(т. е., несанкционированная модификация)*	☐			
Нарушение доступности *(т. е., недоступность)*	☐			
Нарушение неотказуемости	☐			
Уничтожение	☐			

Полные стоимости восстановления после инцидента

(Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 1÷10 для «значимости» и в деньгах для «стоимости»)	Значимость	Указатели	Стоимость

Разрешение инцидента

Дата начала расследования инцидента _____

Фамилия лица (лиц), проводившего (их) расследование инцидента _____

Дата окончания инцидента _____

Дата окончания воздействия _____

Дата завершения расследования инцидента _____

Ссылка и место хранения отчета о расследовании _____

Причастные лица

(Один из)

Лицо (PE) ☐

Организованная группа (GR) ☐

Легально учрежденная организация/учреждение (OI) ☐

Случайность (AC) ☐

Нет виновного (NP) ☐
Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐

Политика/Терроризм (PT) ☐

Развлечение/хакерство (PH) ☐

Реванш (RE) ☐

Другие мотивы (OM) ☐

Определить:

Действия, <u>предпринятые</u> для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)

Действия, запланированные для разрешения инцидента

(например, см. выше)

Прочие действия

(например, по-прежнему требуется проведение расследования для другого персонала)

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный ☐ **Незначительный** ☐

(Укажите любые другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации).

Руководитель ИБ	☐	Руководитель ГРИИБ	☐
Местный руководитель (уточнить, какого подразделения)	☐	Руководитель информационных систем	☐
Автор отчета	☐	Руководитель автора отчета	☐
Полиция	☐	Другие лица	☐

(например, справочная служба, отдела кадров, менеджмента, внутреннего аудита, регулятивного органа)

Определить:

Привлеченные лица

Инициатор		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Роль	_____	Роль	_____	Роль	_____
Дата	_____	Дата	_____	Дата	_____

Аналитик		Аналитик		Аналитик	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Роль	_____	Роль	_____	Роль	_____
Дата	_____	Дата	_____	Дата	_____

Приложение № 17
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ЖУРНАЛ №____
учета машинных носителей информации
в сегменте федеральной государственной информационной системы
«Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

№	Регистрационный номер носителя информации (заполняет Тех поддержка)	Модель носителя и серийный номер	Дата регистрации \ снятия с регистрации	Имя компьютера или ФИО сотрудника для кого разрешен носитель	ФИО ответственного за носитель информации	Подпись ответственного за носитель информации
1						
2						
3						
4						
5						
6						
7						

Приложение № 18
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПЕРЕЧЕНЬ
лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы
«Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

№ п/п	Ф.И.О	Должность	Исключен из перечня на основании
1	Валеев Рустэм Фанилевич	И.о. начальника ОИКТ	
2	Болдырева Татьяна Евгеньевна	Врач-трансфузиолог	
3	Гатауллин Артур Ильдарович	Врач-хирург	

Приложение № 19
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
по обращению с сертифицированными средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов», и криптоключам к ним

Определения

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Обозначения и сокращения

АРМ	– автоматизированное рабочее место
ГИС	– государственная информационная система
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
КЗ	– контролируемая зона
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина

СКЗИ	– средство криптографической защиты информации

I. Общие положения

1.1. Инструкция по обращению с сертифицированными средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов», и криптоключам к ним (далее – Инструкция) регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации.

1.2. Инструкция по обращению с сертифицированными средствами криптографической защиты информации (СКЗИ), предназначенными для защиты информации, обрабатываемой в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД), и криптоключам к ним разработана в соответствии со следующими документами:

1.2.1. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Утверждена приказом ФАПСИ от 13.06.2001 № 152;

1.2.2. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 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»;

1.2.3. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». Утверждено приказом ФСБ России от 09.02.2005 № 66;

1.2.4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

1.3. Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.4. К криптосредствам (шифровальным, криптографическим средствам) относятся:

1.4.1. Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.4.2. Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.4.3. Средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

1.4.4. Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.4.5. Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.4.6. Ключевые документы (независимо от вида носителя ключевой информации).

1.5. Для обеспечения безопасности информации при ее обработке в сегменте ГИС ЕИБД должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.6. Класс криптографической защиты информации, циркулирующей в сегменте ГИС ЕИБД, обеспечиваемый СКЗИ, определяется в соответствии с Моделью угроз и нарушителя и Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 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».

II. Организационная структура

2.1 Безопасность обработки защищаемой информации в сегменте ГИС ЕИБД области с использованием криптосредств организует и обеспечивает ответственный пользователь криптосредств.

III. Обязанности пользователей

3.1. Пользователи криптосредств допускаются к работе с ними только после ознакомления под подпись с настоящей Инструкцией, Типовыми требованиями, другими документами, регламентирующими организацию и обеспечение безопасности информации при их обработке в сегменте ГИС ЕИБД.

3.2. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3. Пользователи криптосредств обязаны:

3.3.1. Не нарушать конфиденциальность закрытых ключей.

3.3.2. Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.3.3. Не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер.

3.3.4. Не допускать записи на ключевой документ посторонней информации.

3.3.5. Не допускать установки ключевых документов в другие ПЭВМ.

3.3.6. Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

3.3.7. Не нарушать конфиденциальность защищаемой информации.

3.3.8. Точно соблюдать требования к обеспечению безопасности информации, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

3.3.9. Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

3.3.10. Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

3.3.11. Своевременно выявлять и сообщать ответственному пользователю криптосредств и ответственному за организацию обработки информации и персональных данных о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним, защищаемой информации.

3.3.12. Немедленно уведомлять ответственного пользователя криптосредств и ответственного за обработку информации и персональных данных и принимать меры по предупреждению нарушения конфиденциальности защищаемой информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности информации.

IV. Опечатывание аппаратных средств

4.1. Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

V. Организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы

5.1. Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность защищаемой информации, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

5.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

5.3. Перечисленные в настоящей Инструкции требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

5.4. Режимные помещения выделяются с учетом размеров контролируемых зон. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие 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 в режимные помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

5.5. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается ответственным за организацию обработки информации и персональных данных в сегменте ГИС ЕИБД.

5.6. Двери режимных помещений должны закрываться на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

5.7. Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

VI. Порядок доступа к хранилищам

6.1. Пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

6.2. Металлические хранилища должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

6.3. Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

6.4. При необходимости доступа к содержимому хранилища ответственный пользователь криптосредств проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

6.5. По окончании работы ответственный пользователь криптосредств закрывает и опечатывает хранилище, за которое он ответственен.

6.6. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за данные хранилища.

6.7. Порядок предоставления сотрудникам ключей для доступа к хранилищам:

6.7.1. Рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, под подпись в соответствующем журнале ответственным пользователем криптосредств.

6.7.2. Запасные экземпляры ключей от хранилищ хранятся в сейфе (хранилище) ответственного пользователя криптосредств.

6.7.3. Запасные экземпляры ключей от сейфа ответственного пользователя криптосредств передаются в опечатанном пенале под подпись в соответствующем журнале.

6.7.4. Ключи от хранилища не должны предоставляться сотрудникам, не ответственным за данные хранилища.

6.7.5. Ключи от механических замков хранилищ должны быть пронумерованы, учтены в соответствующем журнале.

6.7.6. При увольнении сотрудника, либо при назначении другого лица ответственным за хранилище данного сотрудника, сотрудник обязан сдать имеющиеся у него ключи от механического замка хранилища ответственному пользователю криптосредств.

6.7.7. Сотрудникам запрещено передавать кому-либо ключи от хранилищ кроме как в случаях, предусмотренных настоящей Инструкцией.

6.8. Действия при несанкционированном проникновении или утрате ключей от хранилища:

6.8.1. При утрате ключа от хранилища замок данного хранилища 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. Об утрате

ключа сотрудник должен немедленно оповестить ответственного пользователя криптосредств. Порядок хранения документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь криптосредств.

6.8.2. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств. Ответственный пользователь криптосредств должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств, составить акт и принять, при необходимости, меры к локализации последствий.

VII. Контроль безопасности криптосредств

7.1. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного пользователя криптосредств в пределах его полномочий.

VIII. Ответственность за нарушение требований

8.1. Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

Приложение № 20
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ИНСТРУКЦИЯ
ответственного пользователя криптосредств в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Обозначения и сокращения

АРМ	– автоматизированное рабочее место
Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
ОСК	– объект службы крови
ПДн	– персональные данные
КЗ	– контролируемая зона
ПО	– программное обеспечение
СКЗИ	– средство криптографической защиты информации

I. Общие положения

1.1. Инструкция ответственного пользователя криптосредств определяет функции, права и обязанности ответственного пользователя криптосредств, а также регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки и передаче в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД).

1.2. Ответственный пользователь криптосредств назначается из числа работников объекта Службы крови (далее – ОСК) и обеспечивает правильность использования и нормальное функционирование средств криптографической защиты информации (далее – СКЗИ).

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4. Ответственный пользователь криптосредств обладает правами доступа к любым СКЗИ (включая СКЗИ на АРМ) по согласованию с уполномоченным лицом в Федеральном государственном бюджетном учреждении здравоохранения «Центр крови Федерального медико-биологического агентства» (за исключением информации, закрытой с использованием средств криптозащиты).

II. Обязанности

2.1. Ответственный пользователь криптосредств обязан:

2.1.1. Осуществлять учет криптосредств, и документации к ним.

2.1.2. Осуществлять контроль за соблюдением условий использования криптосредств.

2.1.3. Надежно хранить документацию к криптосредствам.

2.1.4. Обеспечивать конфиденциальность информации о криптосредствах.

2.1.5. Хранить ключевые документы к криптосредствам в закрытом металлическом шкафу.

III. Учет ключевых документов

3.1. Ключевые документы подлежат учету.

3.2. Все экземпляры ключевых документов выдаются пользователям криптосредств под подпись в соответствующем журнале учета.

IV. Уничтожение ключевых документов

4.1. Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.2. Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

V. Техническое обслуживание криптосредств

5.1. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, а также смена криптоключей Ответственным не осуществляется. Для технического обслуживания криптосредств необходимо обратиться в техническую поддержку Федерального государственного бюджетного учреждения здравоохранения «Центр крови Федерального медико-биологического агентства» по телефону: 8(800)700-76-06, или по электронной почте: sd@bloodfmba.ru.

VI. Ответственность за нарушение требований

6.1. Ответственный пользователь криптосредств несет персональную ответственность за сохранность полученных криптосредств и документации к ним, ключевых документов, а также за соблюдение положений настоящей Инструкции.

Приложение № 21
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ЖУРНАЛ №____
поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 22
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

РЕГЛАМЕНТ
управления (администрирования) системой защиты информации сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Определения

В настоящем документе используются следующие термины и их определения:

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств (далее – ТС) и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при её обработке в автоматизированной системе.

Блокирование информации – временное прекращение обработки информации.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Канал связи - совокупность технических устройств, обеспечивающих передачу сообщений любого вида от отправителя к получателю, осуществляемую с помощью электрических сигналов.

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и исключена возможность хищения ТС обработки защищаемой информации и/или осуществления несанкционированного доступа к ним.

Конфиденциальность защищаемой информации – обязательное для соблюдения оператором или иным получившим доступ к защищаемой информации лицом требование не допускать её распространения без наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

Носитель информации – физическое лицо или материальный объект, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Сети общего пользования – информационно-телекоммуникационные сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Перечень принятых сокращений

Сегмент ГИС ЕИБД	– сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
ИБ	– информационная безопасность
ПО	– программное обеспечение
ПСЗИ	– подсистема защиты информации
СрЗИ	– средство защиты информации
СКЗИ	– средство криптографической защиты информации

I. Общие положения

1.1. Область применения

Регламент управления (администрирования) системой защиты информации (далее – Регламент) сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмент ГИС ЕИБД) распространяется на администраторов информационной безопасности (далее – ИБ) и администраторов ГИС. Регламент обязателен к применению всеми работниками, выполняющими административную роль в сегменте ГИС ЕИБД.

На основании Регламента могут разрабатываться дополнительные инструкции, детализующие и/или уточняющие его положения для конкретных средств защиты информации (далее – СрЗИ), используемых в сегменте ГИС ЕИБД.

1.2. Общие сведения

Основными целями деятельности по управлению (администрированию) системой защиты информации сегмента ГИС ЕИБД является:

– создание условий для осуществления своевременного выявления и оперативного реагирования на инциденты ИБ;

– создание условий для корректного функционирования сегмента ГИС ЕИБД;

– разграничения ответственности администраторов, участвующих в управлении системы защиты информации (далее – СЗИ) сегмента ГИС ЕИБД;

– предотвращение и/или снижение негативного влияния инцидентов ИБ на выполнение технологических процессов сегмента ГИС ЕИБД;

– предотвращение и/или снижение повторения инцидентов ИБ в сегменте ГИС ЕИБД.

Основными задачами, с помощью которых обеспечивается выполнение указанных целей, являются:

– корректная настройка СрЗИ сегмента ГИС ЕИБД;

– разграничение полномочий и ответственности администраторов и лиц, обеспечивающих функционирование сегмента ГИС ЕИБД;

– регламентация размещения средств вычислительной техники (далее – СВТ) и настроек СрЗИ сегмента ГИС ЕИБД;

Регламентом определены роли, связанные с процессом управления (администрирования) сегмента ГИС ЕИБД, а также процедуры защиты информации, включающие в себя:

– проведение обновлений и контроль обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, описан порядок распределения ролей и ответственности;

– ведение журналов по учету, выдаче, и запрету использования не учтенных съемных машинных носителей информации;

– ведение журналов по учету и хранению машинных носителей информации;

– процедуры связанные с изменением конфигурации сегмента ГИС ЕИБД.

II. Определение ролей процесса управления (администрирования) системы защиты информации

2.1. В целях соответствия принципу предоставления минимальных полномочий (ролей) достаточных для выполнения служебных обязанностей, не допускающих дублирования или пересечения ролей, назначаются действующие на постоянной основе администраторы.

Выделяются следующие роли:

Администратор ГИС – обеспечивает настройку и штатное функционирование компонентов. В обязанности администратора ГИС входит:

– установка и настройка СВТ в ГИС;

– установка и настройка программного обеспечения в СВТ;

– поддержание штатного функционирования СВТ;

– обновление программного и системного обеспечения в СВТ;

– установка и настройка периферийного оборудования в ГИС;

– поддержание штатного функционирования периферийного оборудования;

– внесение изменений в конфигурацию ГИС, а также их документирование;

– проведение тестовых испытаний обновлений компонентов ГИС на тестовом стенде перед применением настроек;

– учет СВТ и компонентов ГИС;

Администратор ИБ – обеспечивает настройку и штатное функционирование компонентов сегмента ГИС ЕИБД, отвечает за формирование требований к настройкам СрЗИ и соответствие применяемых мер и технологий требованиям регуляторов в области защиты информации.

В обязанности администратора ИБ входят:

– настройка антивирусной защиты и поддержание ее штатного функционирования;

– настройка защиты каналов связи и поддержание ее штатного функционирования;

– настройка межсетевого экранирования и поддержание ее штатного функционирования;

– генерация ключевой информации необходимой для функционирования защиты каналов связи;

– настройка разграничения доступа к объектам ГИС;

– настройка журналов регистрации событий СЗИ ГИС;

– предварительное тестирование планируемых изменений в конфигурации СЗИ ГИС;

– внесение изменений в конфигурацию СЗИ ГИС, а также документирование внесенных изменений;

– резервирование и восстановление конфигурации СЗИ ГИС;

– проведение тестовых испытаний настроек СЗИ ГИС на тестовом стенде перед применением настроек;

– формирование требований к мерам обеспечения защиты информации в ГИС, в том числе при взаимодействии с внешними системами;

– учет компонентов СЗИ ГИС;

– выявление и реагирование на инциденты ИБ;

– мониторинг журналов регистрации событий безопасности;

– периодический контроль выполнения требований по обеспечению безопасности информации в ГИС;

– обработка заявок на предоставления доступа к защищаемым объектам ГИС;

– учет носителей ключевой информации;

– учет изменений в программно-аппаратный состав СЗИ ГИС;

– проведения анализа защищенности ГИС;

– выдача и учет машинных (в том числе съемных) носителей информации, используемых в ГИС;

– уничтожение машинных (в том числе съемных) носителей информации, используемых в ГИС.

III. Основные правила управления (администрирования) подсистемы защиты информации

3.1. Уровни доступа

Уровни доступа к документам и сведениям конфиденциального характера сегмента ГИС ЕИБД должны отвечать разделению функциональных обязанностей субъекта доступа и соответствовать выполняемым задачам.

В общем случае выделяются следующие уровни доступа:

– административный доступ с высокими привилегиями на заведение/блокировку и изменение прав доступа администраторов с меньшими привилегиями (в том числе администраторов из числа подрядных организаций), выполнение контролирующих функций;

– административный доступ подрядных организаций к сегменту ГИС ЕИБД, предназначенный для администрирования ГИС, выполнения настроек и технических работ в ГИС.

Права администратора не предоставляют возможности выполнения производственных работ в сегменте ГИС ЕИБД.

Для работы в сегменте ГИС ЕИБД каждому субъекту доступа создается своя учетная запись, обладающая определенным в заявке набором ролей и прав доступа.

Доступ администраторов к средам разработки и тестирования сегмента ГИС ЕИБД предоставляется на основании выполняемых ими функциональных

обязанностей путем создания отдельных индивидуальных учетных записей в ОС, СУБД и средах разработки.

3.2. Правила идентификации и аутентификации

При доступе к сегменту ГИС ЕИБД должны осуществляться идентификация и аутентификация субъектов доступа с использованием учетной записи и пароля или криптографических методов аутентификации. Учетные записи администраторов ГИС должны быть персонализированы.

Любой доступ, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации, должен требовать идентификацию и аутентификацию субъекта доступа.

Аутентификация осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств, а в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.

Вводимые пароли должны маскироваться.

В сегменте ГИС ЕИБД должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Все групповые учетные записи должны иметь оформленное разрешение на использование общих учетных записей и одного ответственного за использование учетной записи для каждой учетной записи подобного рода.

В сегменте ГИС ЕИБД должна обеспечиваться многофакторная (двухфакторная) аутентификация администраторов при удаленном доступе в сегменте ГИС ЕИБД с использованием сети связи общего пользования, в том числе сети Интернет, а также администраторов при локальном доступе в ГИС.

3.3. Правила идентификации и аутентификации устройств

Администратором ИБ должен быть определен перечень типов устройств, используемых в сегменте ГИС ЕИБД и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Всем устройствам в сегменте ГИС ЕИБД должны быть присвоены уникальные идентификаторы, однозначно связанным с ними.

Идентификация устройств в сегменте ГИС ЕИБД обеспечивается следующими способами:

– по логическим именам (имя устройства и (или) ID);

– по логическим (например, IP-адрес) и (или) по физическим адресам (например, MAC-адрес) устройства;

– по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в сегменте ГИС ЕИБД обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

3.4. Управление идентификаторами и учетными записями

Для сегмента ГИС ЕИБД должен быть назначен администратор, ответственный за создание, присвоение и уничтожение идентификаторов пользователей и устройств, а также ответственный за хранение, выдачу,

инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Учетные записи администраторов (пользователей), которые прекратили работу в сегменте ГИС ЕИБД вследствие увольнения или прекращения срока действия государственного контракта, должны быть отключены и заблокированы на следующий день после увольнения (прекращения срока действия государственного контракта), их права на доступ в сегменте ГИС ЕИБД должны быть аннулированы.

Учетные записи пользователей при неиспользовании должны блокироваться через 90 дней.

3.5. Правила разграничения доступа

Организация доступа к сегменту ГИС ЕИБД осуществляется на основании заявки. Заявка служит основанием для выполнения действий по предоставлению субъекту доступа прав доступа к сегменту ГИС ЕИБД администратором ИБ.

Права доступа администраторов к сегменту ГИС ЕИБД определяются их должностными обязанностями в соответствии с производственной необходимостью. Права субъектов доступа на доступ к сегменту ГИС ЕИБД должны предоставляться исходя из принципа минимальной достаточности прав для выполнения должностных обязанностей (включая обязанности по замещению отсутствующих администраторов или пользователей).

Администраторы должны придерживаться принципов разделения полномочий и областей ответственности при работе в сегменте ГИС ЕИБД и не должны пытаться обойти установленные механизмы разграничения доступа. Администратор ИБ выявляет и пресекает случаи нарушения разделения полномочий и выполнения несанкционированных действий, а также случаи передачи администраторами своих факторов аутентификации (паролей, устройств e-Token и т. д.).

Средства управления доступом сегмента ГИС ЕИБД должны быть защищены от модификации, пути обхода механизмов контроля доступа должны пресекаться. Администратор из числа работников подрядных организаций не должен иметь возможность самостоятельно изменять свои права доступа.

Правила разграничения доступа реализуются в рамках подсистемы управления доступом на основе установленных списков доступа или матриц доступа и обеспечивают управление доступом субъектов доступа (групп субъектов) и запускаемых при входе в систему от их имени процессов к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, а также иным объектам доступа.

В случае отсутствия явно указанных правил предоставления доступа субъекту доступа к объекту доступа подсистема управления доступом должна запретить доступ.

Подсистема управления доступом должна предоставлять субъекту доступа возможность запуска только ограниченного набора прикладных задач.

При длительном (более пятнадцати минут) временном отсутствии администратора на рабочем месте сессия должна автоматически блокироваться и требовать повторной аутентификации администратора перед возобновлением

работы. Аналогично должен блокироваться доступ к терминалам серверов и сетевого оборудования. Блокирование сеанса доступа субъекта доступа в сегменте ГИС ЕИБД должно обеспечивать временное приостановление работы субъекта (без выхода из ГИС). Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Механизм управления доступом должен контролировать количество одновременно запущенных сессий работы с сегментом ГИС ЕИБД и иметь возможность их ограничения.

Механизм управления информационными потоками обеспечивает разрешенный маршрут прохождения информации между устройствами, при взаимодействии с сетью Интернет, ведомственной транспортной сетью (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками.

Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из сегмента ГИС ЕИБД. и (или) входящие в сегменте ГИС ЕИБД.

Изменение и отмена прав доступа субъекта доступа к объектам доступа производятся администратором ИБ при изменении служебных обязанностей или задач субъекта.

Изменение и отмена прав доступа субъектов доступа к объектам доступа производятся на основании заявки с обязательным указанием полного набора параметров прав доступа субъекта после их изменения.

3.6. Управление информационными потоками

В сегменте ГИС ЕИБД должно осуществляться управление информационными потоками при передаче информации между устройствами.

При управлении информационными потоками должны выполняться следующие требования:

– разрешение передачи информации в сегменте ГИС ЕИБД только по утвержденному маршруту;

– изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

Управление информационными потоками должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, а также между сегментом ГИС ЕИБД и сетью общего пользования на основе правил управления информационными потоками, включающих в себя контроль конфигурации сегмента ГИС ЕИБД, источника и получателя передаваемой информации, структуры передаваемой информации,

характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

Управление информационными потоками должно блокировать передачу защищаемой информации через сеть общего пользования (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционированно исходящие из сегмента ГИС ЕИБД и (или) входящие в сегменте ГИС ЕИБД.

3.7. Контроль использования прав доступа и учетных записей

Инвентаризация прав субъектов доступа на доступ к сегменту ГИС ЕИБД должна осуществляться Администратором ИБ на регулярной основе не реже чем один раз в год.

На ежеквартальной основе Администратором ИБ проводит анализ журналов аудита с целью контроля действий администраторов, формирует отчет о выявленных случаях нарушения настоящих правил и контролирует правильность и своевременность устранения выявленных нарушений.

Проверка соответствия прав администраторов на доступ к документам и сведениям конфиденциального характера сегмента ГИС ЕИБД их должностным обязанностям должна осуществляться каждый раз при утверждении заявки на предоставление или изменение прав доступа в сегменте ГИС ЕИБД.

Учетные записи администраторов, которые прекратили работу с сегментом ГИС ЕИБД вследствие увольнения или прекращения срока действия договора, должны быть отключены и заблокированы на следующий день после увольнения (прекращения срока действия договора), их права на доступ к сегменту ГИС ЕИБД должны быть аннулированы.

В сегменте ГИС ЕИБД должны регистрироваться все случаи создания учетных записей субъектов доступа, назначения или изменения прав доступа администраторов, случаи успешной и неуспешной регистрации администраторов в сегменте ГИС ЕИБД. В дальнейшем эти сведения должны обрабатываться и анализироваться для выявления случаев несанкционированного доступа к сегменту ГИС ЕИБД и документам и сведениям конфиденциального характера в сегменте ГИС ЕИБД.

3.8. Пересмотр прав доступа администраторов

Пересмотр прав доступа администраторов с высокими привилегиями на доступ к информационному ресурсу должен осуществляться администратором ИБ на регулярной основе не реже чем один раз в шесть месяцев.

Выявленные избыточные права доступа субъектов доступа к сегменту ГИС ЕИБД должны быть отозваны незамедлительно.

3.9. Управление блокированием сеансов доступа

В сегменте ГИС ЕИБД должно быть установлено ограничение числа параллельных сеансов доступа для каждой учетной записи, основанное на идентификаторах пользователей и (или) принадлежности к определенной роли.

Значение числа параллельных сеансов доступа может быть задано как для сегмента ГИС ЕИБД в целом, для групп пользователей, отдельных пользователей или их комбинаций.

3.10. Поддержка и сохранение атрибутов безопасности

В сегменте ГИС ЕИБД должна обеспечиваться поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности информации в процессе ее хранения и обработки.

Атрибуты безопасности представляют собой свойства объектов и (или) субъектов доступа, которые используются для контроля доступа субъектов к объектам доступа и управления информационными потоками.

3.11. Действия пользователей, разрешенные до прохождения ими процедур идентификации и аутентификации

Администратором ИБ должен быть установлен перечень действий субъектов доступа, разрешенных до прохождения ими процедур идентификации и аутентификации. Действия, не включенные в данный перечень, должны быть технически недоступны до прохождения процедур идентификации и аутентификации.

Системному администратору и администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования сегмента ГИС ЕИБД в случае сбоев в работе или выхода из строя отдельных технических средств (устройств).

3.12. Управление антивирусной защитой

Должны обеспечиваться возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макровирусов, объектов ActiveX, апплетов языка Java и т. п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

Обязательным является обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.

Должна обеспечиваться возможность автоматического распространения обновлений антивирусных баз на все компоненты сегмента ГИС ЕИБД.

Должно обеспечиваться соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.

Должны обеспечиваться надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы (по возможности в русскоязычной среде).

Должно обеспечиваться наличие документации, необходимой для практического применения и освоения антивирусного ПО.

В сегменте ГИС ЕИБД должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору ИБ;

В сегменте ГИС ЕИБД должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий ПО средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах сегмента ГИС ЕИБД (серверах, автоматизированных рабочих местах).

В штатном режиме работы системы антивирусной защиты администратор ИБ, отвечающий за ежедневное сопровождение антивирусной защиты, выполняет следующие действия:

– установка средств антивирусной защиты на все объекты антивирусной защиты;

– контроль наличия связи между сервером администрирования и защищаемыми объектами;

– необходимое обновление версий средств антивирусной защиты на объектах антивирусной защиты;

– контроль выполнения задач постоянной защиты;

– настройка автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;

– контроль актуальности версий антивирусных баз и модулей сканирования ПО сервера администрирования;

– непрерывный мониторинг информационного обмена в средствах защиты с целью обнаружения проявлений программно-математических воздействий;

– обработка сведений, поступающих от средств антивирусной защиты;

– формирование сводных отчетов о работе средств антивирусной защиты, инцидентах и пр.;

– формирование отчетов о работе средств антивирусной защиты в сегменте ГИС ЕИБД.

Процесс управления системой антивирусной защиты включает в себя следующие действия администратора ИБ, отвечающего за ежедневное сопровождение антивирусной защиты:

– внесение изменений в политику антивирусной защиты;

– управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;

– мониторинг событий, информация о которых поступает от средств антивирусной защиты с объектов защиты.

В обязанности администратора ИБ, отвечающего за ежедневное сопровождение антивирусной защиты, входит проведение следующих мероприятий, обеспечивающих возможность анализа результатов работы средств системы антивирусной защиты:

– разработка отчетов о работе средств антивирусной защиты;

– разработка сводных отчетов о работе средств антивирусной защиты, инцидентах и т. п. за месяц.

В отчетах о состоянии системы антивирусной защиты отражается следующая информация:

– количество обнаруженных вредоносных программ за данный период;

– список наиболее активных обнаруженных вредоносных программ;

– список объектов, где наблюдается наибольшая частота обнаружения вредоносных программ;

– список зараженных объектов.

В случае заражения серверов сегмента ГИС ЕИБД вредоносными программами, администратор ИБ выполняет следующие действия:

– обновление антивирусных баз сервера администрирования и всех объектов антивирусной защиты;

– проверка состояния всех объектов антивирусной защиты, наличия зараженных серверов в случае обнаружения пораженных узлов;

– оперативные меры по предотвращению распространения заражения вредоносными программами и при необходимости отключение от сети зараженного сервера;

– проведение действий, направленных на устранение вредоносной программы на всех пораженных узлах сегмента ГИС ЕИБД;

– по завершении мероприятий по устранению последствий заражения – восстановление работоспособности узла.

Все или часть вышеперечисленных мероприятий могут быть делегированы администратору сегмента ГИС ЕИБД, отвечающему за ежедневное сопровождение антивирусной защиты.

При появлении сообщения средств защиты от вредоносных программ о наличии вредоносных программ и (или) при возникновении подозрения на наличие вредоносных программ на компонентах сегмента ГИС ЕИБД, а также подключенных машинных носителях информации и сетевых папках (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.) пользователь сегмента ГИС ЕИБД должен незамедлительно уведомить администратора ИБ.

Администратор ИБ совместно с администратором ГИС должен инициировать внеочередную проверку с использованием средств защиты от вредоносных программ, установленных на соответствующем компоненте сегмента ГИС ЕИБД.

При обнаружении вредоносных программ в результате проверки и (или) при наличии подозрений о них администратор ГИС незамедлительно уведомляет администратора ИБ для определения им факта наличия или отсутствия вредоносных программ и возможного нарушения функционирования компонентов ГИС.

В случае обнаружения средствами защиты от вредоносных программ зараженных файлов администратору ИБ совместно с администратором ГИС необходимо выполнить следующие действия:

– приостановление работы компонента сегмента ГИС ЕИБД и изолирование его от локальной вычислительной сети (при наличии такой возможности);

– незамедлительное оповещение о факте обнаружения вредоносного ПО владельца зараженных файлов, а также смежных подразделений, использующих данные файлы в работе;

– анализ необходимости дальнейшего их использования (совместно с владельцем зараженных файлов);

– «лечение» или уничтожение зараженных файлов;

– внеплановая проверка всех компонентов сегмента ГИС ЕИБД, которые могли быть подвержены деструктивному воздействию со стороны обнаруженного вредоносного ПО;

– по факту обнаружения зараженных файлов, составление служебной записки на имя руководителя с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных мероприятий по нейтрализации угрозы;

– принятие мер по предотвращению подобного инцидента безопасности.

Уничтожение вредоносных программ выполняется администратором ИБ, отвечающим за ежедневное сопровождение антивирусной защиты.

Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путем уничтожения программы на жестком диске либо на ином носителе. После уничтожения зараженной программы необходимо восстановить программу, используя ее резервную копию.

Если вредоносная программа поразила файлы, то она уничтожается либо путем стирания этих файлов, либо путем использования специального режима «лечения» в антивирусном ПО. Использование режима «лечения» не дает полной гарантии восстановления файла, поэтому после «лечения» необходима проверка восстановления данного файла. Режим «лечения» используется лишь в тех случаях, когда отсутствует резервная копия зараженной программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

В любом случае, после уничтожения вредоносных программ и восстановления зараженных программ и файлов с данными еще раз выполняется проверка наличия вредоносных программ с использованием антивирусной программы с установленными последними обновлениями. Перед повторной проверкой производится перезагрузка сервера через выключение и последующее его включение. Отсутствие вредоносных программ при повторной проверке свидетельствует об их уничтожении.

3.13. Управлению системой обнаружения и предотвращения вторжений

В штатном режиме работы системы обнаружения и предотвращения вторжений администратор ИБ, отвечающий за ежедневное сопровождение системы обнаружения и предотвращения вторжений, выполняет следующие действия:

– установка и настройка системы обнаружения и предотвращения вторжений;

– контроль актуальности версий баз сигнатур системы обнаружения и предотвращения вторжений;

– непрерывный мониторинг информационного обмена в средствах защиты сегмента ГИС ЕИБД с целью выявления программно-математических воздействий;

– обработка сведений, поступающих от системы обнаружения и предотвращения вторжений;

– формирование сводных отчетов о работе системы обнаружения и предотвращения вторжений, инцидентах и пр.;

– обработка отчетов о состоянии логических сетей;

– формирование отчетов о работе системы обнаружения и предотвращения вторжений логической сети.

Процесс управления системой обнаружения и предотвращения вторжений включает в себя следующие действия администратора ИБ, отвечающего за ежедневное сопровождение системы обнаружения и предотвращения вторжений:

– управление системой обнаружения и предотвращения вторжений;

– мониторинг событий, информация о которых поступает от средств системы обнаружения и предотвращения вторжений;

– оперативное реагирование на сигналы (сообщения) системы обнаружения и предотвращения вторжений, свидетельствующие об обнаружении компьютерной атаки;

– выработка решений по дальнейшей обработке выявленных компьютерных атак.

В обязанности администратора ИБ, отвечающего за ежедневное сопровождение системы обнаружения и предотвращения вторжений, входит проведение следующих мероприятий, обеспечивающих возможность анализа результатов работы системы обнаружения и предотвращения вторжений:

– разработка отчетов о работе системы обнаружения и предотвращения вторжений;

– разработка сводных отчетов о работе системы обнаружения и предотвращения вторжений, инцидентах и т. п. за месяц.

В отчетах о состоянии системы обнаружения и предотвращения вторжений должна отражаться следующая информация:

– количество обнаруженных угроз безопасности информации, относящихся к вторжениям, за данный период;

– наиболее распространенные векторы атак;

– объекты, где наблюдается наибольшая частота обнаружения вторжений.

Вся информация, связанная с компьютерными атаками на сегменте ГИС ЕИБД и использованием системы обнаружения и предотвращения вторжений, заносится в единую базу (хранилище данных) компьютерных атак. Данный процесс происходит в два этапа:

– события ИБ, связанные с компьютерными атаками, регистрируются администратором ПСЗИ, после чего происходят их анализ и направление информации об этих событиях администратору ИБ;

– по завершении обработки инцидента ИБ (закрытии инцидента ИБ), связанного с компьютерной атакой, составляется отчет о компьютерной атаке, содержащий описание типа компьютерной атаки и элементов сегмента ГИС ЕИБД, подвергшихся компьютерной атаке, а также описание уязвимостей

элементов сегмента ГИС ЕИБД, использованных для реализации компьютерной атаки, и другая информация, содержащаяся в журналах регистрации событий ИБ.

Процесс выявления и реагирования на инциденты ИБ описан в документе «Регламент выявления инцидентов сегменте ГИС ЕИБД».

Администратор ИБ должен обеспечить регулярный процесс резервного копирования конфигурации системы обнаружения и предотвращения вторжений с учетом следующих обязательных условий:

– перед внесением каких-либо изменений необходимо убедиться в наличии резервной копии текущей конфигурации системы обнаружения и предотвращения вторжений;

– резервное копирование должно осуществляться после каждого внесения изменений в конфигурацию системы обнаружения и предотвращения вторжений;

– резервное копирование должно осуществляться с использованием безопасных протоколов (например, SSHv2 или SCP);

– доступ к серверам/каталогам с резервными копиями конфигураций системы обнаружения и предотвращения вторжений должны иметь только администратор ИБ;

– вложенность резервных копий системы обнаружения и предотвращения вторжений должна быть не менее 2 конфигураций.

Любые изменения в конфигурации системы обнаружения и предотвращения вторжений, в том числе отключение определенных сигнатур базы решающих правил, должны согласовываться с Администратором ИБ.

Обновление версии средств обнаружения и предотвращения вторжений должно осуществляться только после прохождения процедуры тестирования обновлений.

3.14. Управление доверенной загрузкой

Доверенная загрузка должна обеспечивать следующее:

– блокирование попыток несанкционированной загрузки нештатной ОС (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной ОС;

– контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

3.15. Управление машинными носителями информации

К машинным носителям информации в сегменте ГИС ЕИБД относятся машинные носители информации, стационарно устанавливаемые в корпус средств вычислительной техники, систем хранения данных (накопители на жестких дисках), а также съемные машинные носители информации.

Доступ к машинным носителям информации сегмента ГИС ЕИБД предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

Доступ к машинным носителям информации осуществляется на основании должным образом заверенной заявки.

В заявке указываются:

– тип и объем носителя;

– ФИО и должность работника, в ведении которого находится машинный носитель информации;

– цели использования носителя;

– права (чтение/запись) и срок доступа;

– подпись непосредственного руководителя или вышестоящего руководителя подразделения работника.

Все машинные носители информации должны в обязательном порядке регистрироваться и учитываться.

Учет и выдача машинных носителей информации производятся в журнале учета машинных носителей информации администратором ИБ.

На каждом машинном носителе информации проставляется его регистрационный номер.

Ответственные лица по работе с машинными носителями из числа эксплуатационного персонала получают учтенный машинный носитель для выполнения работ на конкретный срок. При получении и сдаче машинных носителей делается соответствующая отметка в журнале учета машинных носителей информации.

Использование съемных носителей информации (USB-flash диски, внешние HDD, flash-карты, магнитные и оптические диски, а также мобильные устройства, обладающие внутренним хранилищем данных и подключаемые по портам ввода/вывода (USB и др.) запрещено.

В сегменте ГИС ЕИБД должен обеспечиваться контроль подключения машинных носителей информации. Контроль подключения машинных носителей информации предусматривает:

– определение типов носителей информации, подключение которых к сегменту ГИС ЕИБД разрешено;

– определение лиц из числа эксплуатационного персонала, которым предоставлены полномочия по подключению носителей к сегменту ГИС ЕИБД;

– запрет подключения носителей информации, подключение которых к сегменту ГИС ЕИБД не разрешено;

– регистрацию действий ответственных лиц по работе с машинными носителями из числа эксплуатационного персонала и событий по подключению к сегменту ГИС ЕИБД носителей.

В сегменте ГИС ЕИБД должен осуществляться контроль ввода (вывода) информации на машинные носители информации. Контроль ввода (вывода) информации на машинные носители информации предусматривает:

– определение типов носителей информации, ввод (вывод) информации на которые подлежит контролю;

– определение лиц из числа эксплуатационного персонала, которым предоставлены полномочия по вводу (выводу) информации на машинные носители;

– запрет действий по вводу (выводу) информации для лиц из числа эксплуатационного персонала, не имеющих полномочий на ввод (вывод)

информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации;

– регистрацию действий лиц из числа эксплуатационного персонала и событий по вводу (выводу) информации на машинные носители информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между лицами из числа эксплуатационного персонала, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на машинных носителях информации.

Уничтожение защищаемой информации на машинных носителях либо самого носителя осуществляется согласно акту уничтожения машинных носителей информации гарантированным способом, исключающим или существенно затрудняющим ее восстановление на носителе.

При уничтожении информации должна обеспечиваться регистрация событий. Администратор ИБ должен выполнять контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации.

В случае если гарантированное уничтожение информации на машинном носителе невозможно, носитель должен быть утилизирован. Машинные носители должны утилизироваться с использованием средств, осуществляющих размагничивание носителя информации либо его физическое разрушение, не позволяющее впоследствии восстановить хранившуюся на нем информацию.

Для сегменте ГИС ЕИБД должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

– перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

– очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

В сегменте ГИС ЕИБД должен обеспечиваться контроль перемещения используемых в сегменте ГИС ЕИБД машинных носителей информации за пределы контролируемой зоны. Передача машинных носителей информации должна осуществляться только по согласованию с руководителем структурного подразделения и администратора ИБ.

Порядок перемещения (вноса и выноса) машинных носителей за пределы контролируемой зоны регламентирован в документе, устанавливающем пропускной и внутриобъектовый режимы.

При контроле перемещения машинных носителей информации осуществляются:

– определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;

– предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);

– учет всех перемещаемых машинных носителей информации;

– при передаче машинных носителей информации – исключение физического повреждения при доставке правильным способом упаковки;

– в случае передачи съемных носителей за пределы контролируемой зоны – обязательная передача носителей лично в руки адресата;

– периодическая проверка наличия машинных носителей информации.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в сегменте ГИС ЕИБД предусматривает:

– определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

– физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

– защиту машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.

Работники, получившие машинные носители информации, несут персональную ответственность за их сохранность и предотвращение несанкционированного доступа к записанной на них защищаемой информации.

Лица из числа эксплуатационного персонала сегмента ГИС ЕИБД, использующие для выполнения своих служебных обязанностей машинные носители информации, при эксплуатации машинных носителей информации должны соблюдать следующие правила:

– в нерабочее время хранить носители в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

– немедленно оповещать администратора ИБ о фактах утери носителей либо ключей от хранилища, в которых хранятся носители.

Лицам из числа эксплуатационного персонала сегмента ГИС ЕИБД, использующим для выполнения своих служебных обязанностей машинные носители, при эксплуатации носителей, содержащих информацию конфиденциального характера, запрещается:

– оставлять машинные носители без присмотра в открытом доступе;

– перемещать носители за пределы контролируемой зоны сегмента ГИС ЕИБД без согласования с непосредственным руководителем работника и работника подразделения ИБ;

– передавать машинные носители посторонним лицам, в том числе своим родственниками и коллегам по работе;

– хранить на машинных носителях информацию, предназначенную для личного использования;

– выносить машинные носители информации в целях, не связанных с выполнением должностных обязанностей;

– передавать машинные носители информации в сторонние организации без отметки в журнале.

Приложение № 23
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

РЕГЛАМЕНТ

управления конфигурацией комплекса средств обеспечения информационной безопасности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Перечень терминов и сокращений

Сокращение/ термин	Определение
Администраторы	ИТ-специалисты разных сфер деятельности, обеспечивающие функционирование программно-технических средств сегмента ГИС ЕИБД
Сегмент ГИС ЕИБД	сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
Информационная безопасность	Обеспечение конфиденциальности, целостности и доступности информации
Информация	Сведения, данные, в том числе документы, файлы, графики и базы данных, учетные и информационные программы, хранящиеся как на бумажных, так и на электронных носителях
Координатор изменений	Лицо, ответственное за координацию всего процесса управления изменениями, а также за принятие решений о целесообразности изменений, выдачу санкций на проведение изменения и последующую оценку результатов проведенных изменений
КСЗИ	Комплекс средств защиты информации
ППО	Прикладное программное обеспечение

Сокращение/ термин	Определение
Риск	Сочетание вероятности события и его последствий

I.Общие положения

1.1. Область применения

Требования настоящего Регламента распространяются на все подразделения и должностные лица, ответственные за обеспечение информационной безопасности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмента ГИС ЕИБД).

1.2. Общие положения

Процесс управления изменениями комплекса средств защиты информации (далее – КСЗИ) сегмента ГИС ЕИБД выполняется для поддержания конфигурации КСЗИ сегмента ГИС ЕИБД (структуры КСЗИ, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на КСЗИ сегмента ГИС ЕИБД.

Управление изменениями КСЗИ направлено на уменьшение вероятности возникновения различных инцидентов информационной безопасности при внесении изменений в компоненты инфраструктуры КСЗИ сегмента ГИС ЕИБД.

Процесс управления изменениями имеет следующие цели:

- удостовериться в необходимости и оправданности вносимых изменений;
- минимизировать риски непрерывности оказания государственной услуги, доступности сервисов и безопасности информации при проведении изменений;
- обеспечить оптимальное использование ресурсов при проведении изменений;
- обеспечить документирование изменений и действий по их подготовке и проведению;
- обеспечить получение обратной связи от заинтересованных сторон по итогам проведения изменения.

II.Процесс управления изменениями

Процесс управления изменениями включает в себя следующие шаги:

1) Формирование и подача заявки на изменения. В рамках данного шага инициатор изменения идентифицирует необходимость проведения изменения, последствия отказа от изменения и критерии успеха проведения изменения и

подает заявку на проведение изменения. Заявка оформляется при необходимости проведения следующих работ:

– перезагрузка прикладного программного обеспечения (далее – ППО);

– перезагрузка аппаратного программного обеспечения;

– системные изменения;

– инфраструктурные изменения;

– архитектурные изменения;

– прикладные изменения (включая установку хот-фиксов, патчей, версий, релизов ППО).

2) Прием, регистрация и классификация заявки на изменения. В рамках данного шага Координатор изменений выполняет первичную оценку заявки, регистрирует заявку и классифицирует ее по степени срочности проведения изменения и по степени потенциального влияния, оказываемого изменением, а также определяет Исполнителя изменения. Для нестандартных и аварийных изменений Координатор изменений назначает период времени после проведения изменений, по прошествии которого должна быть проведена оценка изменения. Координатор изменений имеет право отказать в приеме заявки, если считает ее недостаточно обоснованной или некорректно заполненной. В том случае, если предлагаемое изменение является стандартным, осуществляется переход к этапу подготовки изменения.

3) Идентификация и оценка рисков, связанных с изменением. В рамках данного шага Координатор изменений идентифицирует возможные негативные последствия проведения изменения и оценивает вероятность их наступления, а также степень влияния на оказание услуги. Для оценки рисков, связанных с реализацией изменения, Координатор изменений привлекает Куратора ППО, затрагиваемого изменением.

4) Планирование изменения и мер по снижению связанных с ним рисков. В рамках данного шага Исполнитель изменения производит изыскание технических возможностей реализации изменения, разрабатывает меры по снижению идентифицированных ранее рисков, а также идентифицирует необходимые для подготовки и проведения изменения ресурсы и составляет план работ. Координатор изменений утверждает разработанные Исполнителем изменения документы.

5) Принятие решения о целесообразности изменения и согласование изменения. В рамках данного шага Координатор изменений на основе информации, полученной на предыдущих этапах, принимает решение о целесообразности изменения. В случае целесообразности реализации изменения Координатор изменения направляет заявку на изменение на согласование в Комитет по изменениям. В случае отрицательного результата согласования Координатор изменений направляет Исполнителю изменений мотивированный отказ.

6) Подготовка изменения. В рамках данного шага Исполнитель изменения осуществляет подготовительные работы для проведения изменения, предусмотренные на этапе планирования изменения.

7) Выдача санкции на проведения изменения. В рамках данного шага Координатор изменений на основе информации, полученной в ходе подготовки

изменения, санкционирует проведение изменения и определяет время его проведения. В случае отказа в санкции на проведение изменения осуществляется повторное планирование работ по подготовке и проведению изменения с учетом вновь выявленных недостатков и рисков, после чего происходит повторное рассмотрение изменения на предмет его целесообразности.

8) Проведение изменения. В рамках данного шага Исполнитель изменения осуществляет и координирует работы по проведению изменения, а также определяет успешность реализации изменения на основе принятых ранее критериев. В случае неуспешного проведения осуществляется повторное планирование работ по подготовке и проведению изменения с учетом вновь выявленных недостатков и рисков, после чего происходит повторное рассмотрение изменения на предмет его целесообразности. При проведении изменения могут быть идентифицированы новые потребности в других изменениях, на основании которых могут быть сформированы новые заявки на изменения.

9) Оценка изменения. В рамках данного шага заинтересованные стороны оценивают результаты проведенного изменения.

На диаграмме приложения (Приложение 1) представлена последовательность действий процесса управления изменениями и взаимосвязи между ними.

III. Роли и ответственность участников

Определены следующие роли в рамках процедуры управления изменениями:

1) Инициатор изменения – лицо, идентифицирующее необходимость в изменении и заинтересованное в его проведении.

2) Координатор изменений – лицо, ответственное за координацию всего процесса управления изменениями, а также за принятие решений о целесообразности изменений, выдачу санкций на проведение изменения и последующую оценку результатов проведенных изменений.

3) Исполнитель изменения – лицо, ответственное за подготовку изменения, включая идентификацию необходимых ресурсов, разработку мер по снижению рисков, планирование работ во времени, проектирование, тестирование и реализацию изменения.

4) Администраторы сегмента ГИС ЕИБД – лица, ответственные за поддержание работоспособности и конфигурацию компонентов информационных систем и сервисов, затрагиваемых изменением.

5) Куратор ППО – лицо, ответственное за эксплуатацию ППО, затрагиваемого изменением.

6) Комитет по изменениям. В Комитет по изменениям входят:

- работники отдела эксплуатации ППО;
- работники отдела технической эксплуатации;

– работники отдела вычислительной и сетевой инфраструктуры общесистемного программного обеспечения;

– при необходимости – работники ИТ-подразделения и отдела режима секретности и безопасности информации.

В таблице ниже (Таблица 1) приведено распределение ролей и ответственности участников процесса управления изменениями на различных его этапах.

В матрице ролей и ответственности при выполнении процедуры управления изменениями приняты следующие условные обозначения:

R – Responsible (Исполнитель). Должностное лицо, непосредственно выполняющее действие.

A – Accountable (Ответственный). Должностное лицо, ответственное за достижение результата действия.

C – Consulted (Консультант, Эксперт). Должностное лицо, чья консультация и (или) экспертное мнение необходимы для выполнения действия.

I – Informed (Информируемый). Должностное лицо, которое ставится в известность о результате выполнения действия.

Таблица 1 – Матрица ролей и ответственности при выполнении процедуры управления изменениями

Наименование процедуры	**Координатор изменений**	**Инициатор изменения**	**Исполнитель изменения**	**Администраторы и разработчики компонентов информационной системы**	**Комитет по изменениям**	**Куратор ППО**
Формирование и подача заявки на изменение	I	AR	–	–	–	–
Прием, регистрация и классификация заявки на изменение	AR	I	I	C	–	C
Идентификация и оценка рисков, связанных с изменением	AR	I	I	C	–	C
Планирование изменения и мер по снижению связанных с ним рисков	A	C	R	–	–	–
Принятие решения о целесообразности проведения изменения и согласование изменения	AR	C	I	–	R	–
Подготовка изменения	I	C	AR	–	–	–
Выдача санкции на проведение	AR	C	I	C	–	C

Наименование процедуры	Координатор изменений	Инициатор изменения	Исполнитель изменения	Администраторы и разработчики компонентов информационной системы	Комитет по изменениям	Куратор ППО
изменения						
Проведение изменения	I	I	AR	–	I	–
Оценка проведенного изменения	AR	R	I	C	–	C

IV. Детальное описание этапов выполнения процедуры управления изменениями

4.1. Формирование и подача заявки на изменение

Подача заявки на изменение осуществляется Инициатором изменения.

Заявка должна включать в себя следующую информацию:

- цели изменения;
- описание изменения;
- последствия отказа от проведения изменения.

Заявка передается Координатору изменений на рассмотрение.

Форма Заявки приведена в приложении (Приложение 2).

4.2. Прием, регистрация и классификация заявки на изменение

В рамках данного этапа Координатор изменений выполняет первичную оценку заявки, регистрирует заявку и классифицирует ее по степени срочности проведения изменения и по степени потенциального влияния, оказываемого изменением, а также определяет Исполнителя изменения.

На основании классификации заявки (для нестандартных и аварийных изменений) Координатор изменений устанавливает период времени после проведения изменения, по прошествии которого должна быть проведена оценка изменения.

4.3. Прием и регистрация заявки на изменение

При получении заявки на проведение изменения Координатор изменений осуществляет первичную оценку корректности заполнения и обоснованности заявки, привлекая Куратора ППО и владельца сервиса.

Инициатору изменения может быть отказано в приеме заявки в следующих случаях:

- заявка некорректно заполнена;
- заявка недостаточно обоснована;
- владелец сервиса отказал в согласовании изменений.

При приеме заявки Координатор изменений присваивает ей номер и регистрирует ее в журнале изменений.

Записи в журнале изменений должны включать в себя следующую информацию:

- номер заявки;
- дата подачи заявки;
- краткое описание изменения;
- дата закрытия заявки;

– классификация заявки;

– конечный результат обработки заявки (применено/признано нецелесообразным).

Форма Журнала изменений приведена в приложении (Приложение 3).

4.4. Классификация заявки на изменение по приоритету рассмотрения

На основании представленной в заявке информации о необходимости проведения изменения и последствиях отказа от него Координатор изменений присваивает заявке приоритет и делает соответствующую отметку в Заявке и в Журнале изменений.

Определены следующие классы приоритета рассмотрения заявок на изменения:

– Аварийное изменение. Изменение срочно необходимо для восстановления работоспособности критичных сервисов. Изменения данного типа проводятся вне рамок процедуры, описываемой в данном документе. Заявка носит уведомительный характер и подается уже после проведения изменения.

– Срочное изменение. Изменение необходимо провести как можно скорее, так как оно необходимо для устранения известных проблем, серьезно влияющих на качество сервиса.

– Плановое изменение. Изменение может быть отложено до наиболее удобного для его проведения момента.

4.5. Классификация заявки на изменение по степени оказываемого изменением влияния

Координатор изменений определяет компоненты информационной инфраструктуры, затрагиваемые изменениями, и, на основании консультаций с Куратором ППО, администраторами и разработчиками информационных систем, классифицирует заявку по степени оказываемого изменением влияния.

Координатор изменений делает соответствующие отметки в Заявке и в Журнале изменений.

По степени оказываемого влияния определены следующие категории изменений:

– Стандартное изменение. Изменение, проводимое регулярно и для которого заранее определены необходимые ресурсы, риски, и меры по их снижению.

– Незначительное изменение. Небольшое изменение, для которого отсутствует стандартная процедура и которое требует предварительной оценки рисков и необходимых ресурсов, а также планирования работ. Необходимые для проведения изменения трудозатраты не превышают десяти человеко-часов. Необходимые для проведения изменения финансовые затраты не превышают десяти тыс. рублей.

– Значительное изменение. Масштабное изменение, которое требует предварительного проектирования. Необходимые для проведения изменения трудозатраты превышают десять человеко-часов. Необходимые для проведения изменения финансовые затраты превышают десять тыс. рублей.

4.6. Назначение Исполнителя изменения

На основе имеющейся информации о характере изменения и затрагиваемых им компонентах Координатор изменений определяет и назначает Исполнителя изменения.

Для стандартных изменений Исполнитель должен быть заранее определен соответствующей процедурой.

Координатор изменений вносит ФИО и должность Исполнителя изменений в Заявку и в Журнал изменений.

4.7. Идентификация и оценка рисков, связанных с изменением

На основе имеющейся информации о характере изменения и затрагиваемых им компонентах Координатор изменений идентифицирует возможные негативные последствия проведения изменения, а также его влияние на работу пользователей сервисов, привлекая для этого Куратора ППО, администраторов сегмента ГИС ЕИБД.

На основании накопленного опыта эксплуатации сегмента ГИС ЕИБД и информации, доступной во внешних источниках, Координатор изменений экспертным методом оценивает риски наступления негативных последствий изменения по следующим параметрам:

– вероятность наступления последствия (высокая/средняя/низкая);

– степень влияния последствия на оказание государственной услуги (высокая/средняя/низкая).

С учетом требований аттестата соответствия сегмента ГИС ЕИБД, информации о характере изменения и затрагиваемых им компонентах Координатор изменений и Управление режима секретности и безопасности информации определяют необходимость уведомления органа по аттестации, повторной аттестации или проведения дополнительных аттестационных испытаний сегмента ГИС ЕИБД по требованиям безопасности информации.

По итогам выполнения данного этапа Координатор изменений составляет Протокол оценки рисков и передает его вместе с копией Заявки на доработку Исполнителю изменения.

Форма Протокола приведена в приложении (Приложение 4).

4.8. Планирование изменения и мер по снижению связанных с ним рисков

В рамках данного этапа Исполнитель изменения выполняет следующие действия:

а) изыскание технических возможностей проведения изменения;

б) разработка мер, направленных на снижение рисков проведения изменения:

1) тестирование изменения;

2) подготовка процедур восстановления системы;

3) выбор периода времени для проведения изменения, когда затрагиваемые сервисы наименее востребованы;

4) предупреждение пользователей затрагиваемых сервисов о времени проведения изменения и возможных негативных последствиях;

в) оценка ресурсов, необходимых для подготовки и проведения изменения;

г) составление плана работ по подготовке и проведению изменения;

д) разработка проектной документации по изменению (требуется для изменений, классифицированных как «значительные»).

В случае возникновения необходимости привлечения для выполнения работ сторонних экспертов (сторонних организаций, производителей отдельных компонентов сегмента ГИС ЕИБД) Исполнитель изменения планирует ресурсы, требуемые ему для реализации изменений.

По итогам выполнения данного этапа Исполнитель изменения формирует и передает Координатору изменений на утверждение следующие документы:

– «Заключение о наличии технической возможности проведения изменения и описание необходимых для этого ресурсов»;

– «План проведения изменения» (в случае положительного заключения о наличии технической возможности проведения изменения);

– «Критерии успешности изменения»;

– проектная документация (для изменений, классифицированных как «значительные»).

Координатор изменений имеет право вернуть подготовленные документы Исполнителю изменений на доработку в случае, если считает информацию в них исчерпывающей.

4.9. Принятие решения о целесообразности проведения изменения и согласование изменения

В рамках данного этапа Координатор изменений рассматривает документы, подготовленные Исполнителем изменения на предыдущем этапе.

Координатор изменения принимает решение о целесообразности изменения, учитывая следующие факторы:

– оправданность рисков, связанных с проведением изменения, и достаточность разработанных мер по их снижению;

– экономическая целесообразность проведения изменения.

Решение об установке программного обеспечения и его компонентов должно основываться на принципе установки только необходимого и достаточного программного обеспечения.

В случае целесообразности реализации изменения Координатор изменения направляет заявку на изменение на согласование в Комитет по изменениям, отслеживает ход согласования, контролирует сроки ответов.

Все представители Комитета по изменениям должны предоставить ответ «Согласовано» или «Не согласовано» с указанием причины.

По итогам выполнения данного этапа Координатор изменений делает соответствующую пометку в Заявке на проведение изменения. Если изменение признано Координатором изменения нецелесообразным, заявка закрывается, о чем делается соответствующая пометка в Журнале изменений. Если изменение признано Координатором изменения целесообразным и согласовано всеми участниками Комитета по изменениям, осуществляется подготовка изменения в соответствии с разделом 4.10.

4.10. Подготовка изменения

В рамках данного этапа Исполнитель изменения отвечает за выполнение подготовительных действий, предусмотренных Планом проведения изменения.

Такие действия должны включать в себя:

– тестирование изменения;

– подготовку процедур восстановления системы до изначального состояния (создание резервных копий и т. п.)

По итогам выполнения данного этапа Исполнитель изменения составляет Отчет о подготовке изменения, содержащий описание результатов проведенных действий, и передает его Координатору изменений.

4.11.Выдача санкции на проведение изменения

В рамках данного этапа Координатор изменений на основе результатов подготовки изменения выдает санкцию на проведение изменения и назначает время его проведения.

Для назначения времени проведения изменения Координатор изменений консультируется с Инициатором изменения, Куратором ППО и администраторами сегмента ГИС ЕИБД.

Координатор изменений может отказать в санкции на проведение изменения в том случае, если результаты подготовки изменения являются неудовлетворительными.

При отказе в санкции на проведение изменения осуществляется возврат к этапу планирования изменения и мер по снижению связанных с ним рисков.

По итогам выполнения данного этапа Координатор изменений делает соответствующую пометку в заявке на проведение изменения.

4.12. Проведение изменения

В рамках данного этапа Исполнитель изменения проводит работы по реализации изменения, предусмотренные Планом проведения изменения.

Исполнитель изменения оценивает успешность проведенного изменения в соответствии с ранее определенными критериями успеха изменения.

В случае неуспешного проведения изменения производится восстановление системы до изначального состояния в соответствии с ранее подготовленными процедурами восстановления системы и осуществляется возврат к этапу планирования изменения и мер по снижению связанных с ним рисков.

При проведении изменения могут быть идентифицированы потребности в других изменениях, на основании чего должны быть сформированы новые заявки на проведение изменений.

По итогам выполнения данного этапа Исполнитель изменения составляет Отчет о проведении изменения и передает его Координатору изменений. Координатор направляет Отчет о проведении изменения участниками Комитета по изменениям для ознакомления.

4.13. Оценка проведенного изменения

По результатам внесенных изменений в КСЗИ сегмента ГИС ЕИБД Координатор изменений производит оценку необходимости уведомления органа по аттестации, повторной аттестации сегмента ГИС ЕИБД или проведении дополнительных аттестационных испытаний сегмента ГИС ЕИБД.

В том случае, если проведенное изменение являлось нестандартным или аварийным, то по прошествии ранее определенного Координатором изменений периода времени должна быть проведена оценка изменения.

Координатор изменений отвечает за проведение оценки изменения и привлекает к ее проведению Инициатора изменения, Куратора ППО, администраторов сегмента ГИС ЕИБД.

По итогам выполнения данного этапа вовлеченные стороны в свободной форме составляют служебные записки, где дают свою оценку влияния проведенного изменения на их деятельность.

Координатор изменений информирует Комитет по изменениям о результатах оценки проведенного изменения.

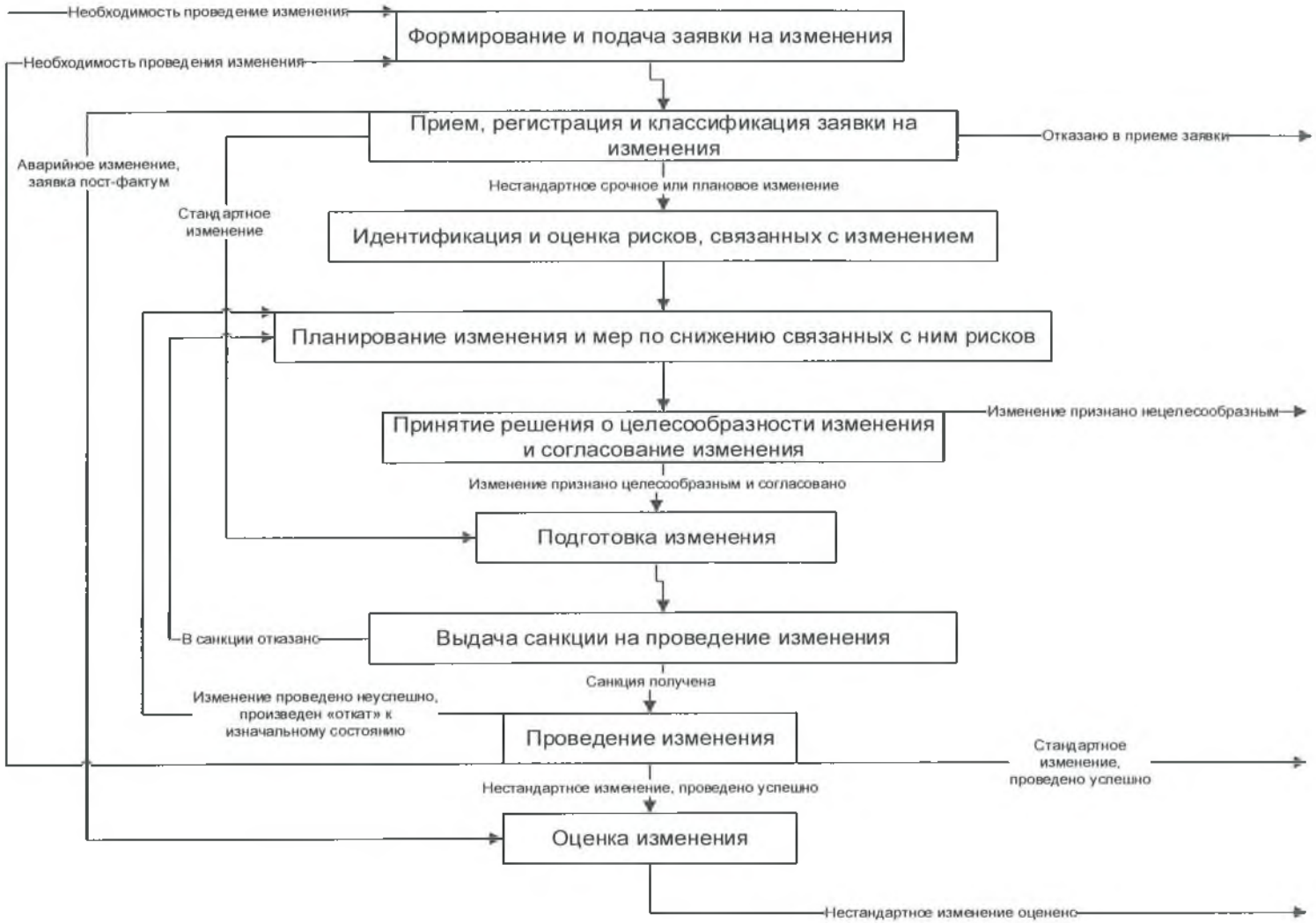
V.Актуализация

Настоящий Регламент действует весь срок до своей отмены.

Периодическая проверка актуальности настоящего Регламента проводится с интервалом не реже одного раза в год.

Решение об изменении настоящего Регламента принимает руководитель организации на основании результатов применения настоящего Регламента, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних проверок.

Приложение 1. (обязательное) Диаграмма процесса управления изменениями



Приложение 2. (обязательное) Форма заявки на изменение

ЗАЯВКА №___[1] **на проведение изменения в сегмента ГИС ЕИБД** Дата подачи заявки: *чч.мм.гггг*	
Цель изменения:	*Описание целей проведения работ*
Описание предлагаемого изменения:	*Описание предлагаемого изменения (или ссылка на документ, описывающий изменение)*
Последствия отказа от изменения:	*Описание рисков и возможных негативных последствий отказа от изменения (или ссылка на соответствующий документ)*
Классификация по приоритету:	*(аварийное/срочное/плановое)*
Классификация по степени влияния:	*(стандартное/незначительное/значительное)*
Результат оценки рисков:	*Ссылка на протокол оценки рисков, связанных с изменением*
Заключение о наличии технической возможности:	*Заключение о наличии технической возможности для проведения изменения и описание необходимых ресурсов (программных, аппаратных, человеческих)*
План внесения изменений:	*Ссылка на техническое задание/инструкцию/ детальный план с указанием реквизитов (наименование документа, номер, дата)*
План восстановления:	*Ссылка на инструкцию/детальный план с указанием реквизитов (наименование документа, номер, дата)*
План тестирования:	*Ссылка на план тестирования с указанием его реквизитов (наименование документа, номер, дата)*
Критерии успешности:	*Описание критериев успешности изменений*
Результаты подготовки изменения:	*Описание результатов подготовительных работ, в том числе тестирования изменения и подготовки восстановительных процедур*
Результаты проведения изменения:	*Отчеты о результатах проведения изменения*
Результаты оценки изменения:	*Ссылки на служебные записки, содержащие оценку результатов изменения заинтересованными сторонами*
Заинтересованные лица	
Инициатор изменения:	*ФИО, должность*
Координатор изменения:	*ФИО, должность*
Члены Комитета по изменениям:	*ФИО, должность*
Исполнитель изменения:	*ФИО, должность*
Администраторы информационной системы, затрагиваемых изменением:	*ФИО, должность* *ФИО, должность*
Куратор ППО:	*ФИО, должность*
Принятые решения	
Решение	Подписи заинтересованных лиц
	ФИО, должность, подпись, дата

[1] Номер Заявки присваивается Координатором изменений.

Приложение 3. (обязательное) Форма журнала изменений

№ заявки	Дата подачи	Дата закрытия	Краткое описание	Классификация	Результат

Приложение 4. (обязательное) Форма протокола оценки рисков, связанных с изменением

№ п/п	Описание возможных негативных последствий	Вероятность наступления	Оценка влияние на деятельность организации	Необходимость аттестации (переаттестации)

Координатор изменений: _____ (ФИО, подпись)

Лист регистрации изменений

Номер версии документа	Дата изменения	Автор изменения	Краткое описание изменения

Приложение № 24
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

РЕГЛАМЕНТ
контроля за обеспечением уровня защищенности сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Перечень принятых сокращений

ИБ	–	информационная безопасность
ГИС	–	государственная информационная система
ПО	–	программное обеспечение
САЗ	–	средство анализа защищенности
СЗИ	–	система защиты информации
СрЗИ	–	средство защиты информации

I. Общие положения

1.1. Область применения

Регламент контроля за обеспечением уровня защищенности информации сегмента федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегмента ГИС ЕИБД) определяет порядок организации и проведения работ по контролю за обеспечением уровня защищенности информации (далее – контроль защищенности), содержащейся в сегменте ГИС ЕИБД.

Ответственными за организацию и проведение работ по контролю за обеспечением уровня защищенности информации является администратор информационной безопасности (далее – ИБ), являющийся ответственным за эксплуатацию средств анализа защищенности.

1.2. Общие сведения

Плановые мероприятия по контролю защищенности должны проводиться не реже одного раза в год.

Внеплановые мероприятия по контролю защищенности должны

проводиться по факту возникновения инцидента ИБ или по указанию руководителя структурного подразделения, ответственного за обеспечение безопасности информации в сегменте ГИС ЕИБД.

К мероприятиям по контролю защищенности относятся:

- контроль актуальности внутренних организационно-распорядительных документов;
- контроль выполнения работ по выявлению, анализу и устранению уязвимостей;
- контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- контроль состава технических средств, программного обеспечения и средств защиты информации.

При обнаружении нарушений требований по обеспечению соответствующего уровня защищенности информации администратор ИБ принимает меры по их устранению.

II. Контроль (анализ) защищенности информации с учетом особенностей функционирования сегмента ГИС ЕИБД

2.1. Контрольные мероприятия (проверки) должны проводиться на плановой основе, а также, при необходимости внепланово.

Решение о необходимости проведения внеплановых контрольных мероприятий принимает руководитель структурного подразделения, ответственного за обеспечение безопасности информации в сегменте ГИС ЕИБД.

Контроль за событиями безопасности и действиями администратора ГИС должен осуществляться на постоянной основе.

Контрольные мероприятия (проверки) организуются администратором ИБ.

Плановые проверки проводятся не реже одного раза в месяц и включают в себя:

- контроль (анализ) защищенности информации, содержащейся в сегменте ГИС ЕИБД;
- проверку ведения эталонных копий средств защиты;
- анализ изменения угроз безопасности информации в сегменте ГИС ЕИБД, возникающих в ходе их эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в сегменте ГИС ЕИБД.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений необходимо предпринять действия, направленные на устранение возможности использования выявленных уязвимостей.

2.2. Контроль актуальности внутренних организационно-распорядительных документов

Администратор ИБ осуществляет сбор и анализ действующих на момент проведения мероприятий по контролю защищенности внутренних нормативных и организационно-распорядительных документов, регулирующих вопросы обеспечения информационной безопасности и защиты информации в сегменте ГИС ЕИБД (далее – документы ИБ).

Контроль актуальности документов ИБ осуществляется на постоянной основе.

Актуальность документов ИБ проверяется в том числе в части:

- описания и инструкций;
- состава и структуры анализируемых документов;
- состава защищаемой информации (информационных активов);
- описания технологических и бизнес-процессов, а также информационных потоков защищаемой информации;
- распределения ролей и назначенных ответственных лиц.

По итогам проведенных контрольных мероприятий администратор ИБ составляет отчет с описанием выявленных нарушений.

При выявлении несоответствий в документах по защите информации администратором ИБ составляется план мероприятий по их доработке.

2.3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

Ответственным за установку обновлений программного обеспечения является администратор ИБ. Он должен проверять наличие обновлений программного обеспечения на постоянной основе (не реже одного раза в месяц).

При наличии обновлений программного администратором ИБ принимается решение о целесообразности установки данных обновлений в соответствии с утвержденным планом мероприятий по устранению уязвимостей.

Администратором ИБ могут применяться специальные программные или технические средства.

2.4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

Ответственным за проведение контроля соответствия реализованных настроек и конфигурации средств защиты информации является администратор ИБ.

Работы по контролю соответствия реализованных настроек и конфигурации средств защиты информации производятся на периодической основе (не реже одного раза в месяц).

Администратор ИБ выполняет работы по контролю соответствия реализованных настроек и конфигурации средств защиты информации, которые входят в состав СЗИ сегмента ГИС ЕИБД, на предмет соответствия эксплуатационной документации.

Контроль работоспособности осуществляется посредством проведения тестов и проверок средств защиты информации, предусмотренных

эксплуатационной документацией на эти средства и на СЗИ сегмента ГИС ЕИБД.

По результатам проведения контрольных мероприятий и анализа результатов администратор ИБ составляет отчет, содержащий сведения о выявленных нарушениях.

При выявлении ошибок в работе или несоответствия параметров установленным значениям, администратор ИБ составляет план мероприятий по устранению выявленных недостатков.

2.5. Контроль состава технических средств, программного обеспечения и средств защиты информации

Ответственным за проведение контроля состава технических средств, программного обеспечения и средств защиты информации является администратор ИБ.

Контроль состава технических средств, программного обеспечения и средств защиты информации осуществляется путем проведения инвентаризации.

Работы по инвентаризации проводятся на периодической основе (не реже одного раза в полгода).

При проведении инвентаризации могут применяться специальные программные или технические средства.

По результатам проведения контрольных мероприятий и анализа результатов администратор ИБ составляется отчет, содержащий сведения о выявленных нарушениях.

При выявлении нарушений администратор ИБ составляет план мероприятий по их устранению.

III. Анализ и оценка функционирования сегмента ГИС ЕИБД и ее СЗИ

3.1. В ходе контроля защищенности осуществляется анализ и оценка функционирования сегмента ГИС ЕИБД и ее СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ сегмента ГИС ЕИБД.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации сегмента ГИС ЕИБД.

При выявлении (поиске), анализе и устранении уязвимостей должно проводиться выявление (поиск) уязвимостей, связанных с ошибками кода в программном обеспечении, правильностью установки и настройки СрЗИ, технических средств и программного обеспечения.

Для выявления (поиска) уязвимостей должны использоваться средства анализа (контроля) защищенности (сканеры безопасности), имеющие стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правила описания уязвимостей, проверочных списков, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Доступ к функциям выявления (поиска) уязвимостей должен предоставляться только администратору ИБ.

Перечень сканируемых уязвимостей в сегменте ГИС ЕИБД должен уточняться с установленной периодичностью, а также после появления информации о новых уязвимостях.

В качестве источников информации об уязвимостях должны использоваться опубликованные данные разработчиков программного обеспечения, технических средств, а также другие базы данных уязвимостей.

IV. Принятие решения о необходимости доработки (модернизации) СЗИ сегмента ГИС ЕИБД

4.1. Решение о необходимости доработки (модернизации) СЗИ сегмента ГИС ЕИБД принимается по результатам контроля за обеспечением уровня защищенности информации в сегменте ГИС ЕИБД.

Решение о необходимости доработки (модернизации) СЗИ сегмента ГИС ЕИБД принимается в том числе, в следующих случаях:

- выявления угроз безопасности информации, нейтрализация которых невозможна применяемыми мерами защиты информации в составе СЗИ сегмента ГИС ЕИБД;
- применения новых информационных технологий в сегменте ГИС ЕИБД;
- внесения изменения в состав и структуру сегмента ГИС ЕИБД;
- изменения требований законодательства.

Приложение № 25
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ПРАВИЛА И ПРОЦЕДУРЫ
анализа угроз безопасности информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

Перечень терминов и сокращений

Термин/сокращение	Определение
Сегмент ГИС ЕИБД	сегмент федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»
Информация	Сведения, данные, в том числе документы, файлы, графики и базы данных, учетные и информационные программы, хранящиеся как на бумажных, так и на электронных носителях
УБИ	Угроза безопасности информации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

I. Общие положения

Настоящий документ определяет правила и процедуры анализа угроз безопасности информации в сегменте федеральной государственной информационной системы «Единая информационная база по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов» (далее – сегменте ГИС ЕИБД).

Под угрозами безопасности информации при ее обработке в сегменте ГИС ЕИБД понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности информации при ее обработке в сегменте ГИС ЕИБД могут быть связаны как с непреднамеренными действиями работников, осуществляющих обслуживание и поддержку сегменте ГИС ЕИБД, так и со специально осуществляемыми

неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от пользователей и эксплуатирующего персонала, осуществляющих обслуживание и поддержку сегмента ГИС ЕИБД, в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности информации.

Систематизированный перечень угроз безопасности информации при ее обработке в сегменте ГИС ЕИБД содержится в Модели угроз безопасности информации. Указанные угрозы могут исходить от различных источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости, характерные для сегмента ГИС ЕИБД, реализуя тем самым угрозы информационной безопасности.

Перечень угроз разработан на основании положений модели вероятного нарушителя безопасности, состава информации, обрабатываемой в сегменте ГИС ЕИБД, требуемых характеристик ее безопасности с учетом положений нормативно-методических документов ФСТЭК России.

II. Источники угроз безопасности информации

В ходе оценки угроз безопасности информации определяются возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей, – актуальные нарушители.

Техногенные источники угроз (физические явления, материальные объекты) не рассматриваются в сегменте ГИС ЕИБД, соответственно угрозы безопасности информации, связанные с техногенными источниками, не включаются и не рассматриваются в модели угроз сегменте ГИС ЕИБД.

Характеристика нарушителей и рассмотрение целей реализации угроз безопасности информации нарушителями безопасности информации приведено в таблице (Таблица 1).

Таблица 1 Возможные цели реализации угроз безопасности информации нарушителями

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Возможные цели реализации угроз безопасности информации **отсутствуют**
2	Террористические, экстремистские группировки	Внешний	Возможные цели реализации угроз безопасности информации **отсутствуют**
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды.
4	Отдельные физические	Внешний	Получение финансовой или иной

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
	лица (хакеры)		материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
5	Конкурирующие организации	Внешний	У Оператора сегменте ГИС ЕИБД **отсутствуют** конкурирующие организации
6	Разработчики программных, программно-аппаратных средств	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Возможные цели реализации угроз безопасности информации **отсутствуют**
8	Поставщики вычислительных услуг, услуг связи	Внутренний	Возможные цели реализации угроз безопасности информации **отсутствуют**
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия.
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
13	Бывшие работники (пользователи)	Внешний	Возможные цели реализации угроз безопасности информации

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
			отсутствуют

III. Угрозы безопасности информации

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России, в котором приведен обобщенный перечень основных угроз безопасности информации, потенциально опасных для сегмента ГИС ЕИБД. При моделировании рассмотрены угрозы УБИ.001 – УБИ.222, дальнейший список угроз строился с учётом структурно-функциональных характеристик информационной системы, включающих структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иных характеристик информационной системы, применяемых информационных технологий и особенностей ее функционирования.

При определении возможных угроз безопасности информации для сегмента ГИС ЕИБД из банка данных угроз безопасности информации необходимо исключить угрозы:

- нехарактерные для сегмента ГИС ЕИБД, связанные с особенностями ее функционирования и информационными технологиями, которые в ней не используются;
- реализуемые нарушителями с высокими возможностями (высоким потенциалом);
- для которых не могут быть определены способы реализации;
- для которых не могут быть определены негативные последствия от реализации угрозы.

IV. Оценка актуальности угроз безопасности информации

Оценка актуальности угроз безопасности информации проводится в соответствии с документом «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021 г.). Для определения актуальности угроз безопасности информации рассматривается перечень возможных угроз безопасности информации и анализируется наличие сценариев их реализации.

V. Описание последствий от нарушения свойств безопасности информации

Нарушение конфиденциальности информации, обрабатываемой в

сегменте ГИС ЕИБД, может привести к утечке информации (персональные данные, информация ограниченного распространения).

Нарушение целостности информации, обрабатываемой в сегменте ГИС ЕИБД, может привести к нарушению деятельности информационного обеспечения процессов деятельности Федеральной антимонопольной службы по контролю и аудиту в сфере закупок.

Нарушение доступности информации, обрабатываемой в сегменте ГИС ЕИБД может привести к нарушению деятельности информационного обеспечения процессов деятельности Федеральной антимонопольной службы по контролю и аудиту в сфере закупок.

Возможные негативные последствия от реализации (возникновения) угроз безопасности информации приведены в таблице (

Таблица 2).

Таблица 2. Виды рисков (ущерба) и возможные негативные последствия от реализации угроз безопасности информации

№ п/п	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Финансовый, иной материальный ущерб физическому лицу.
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Недополучение ожидаемой (прогнозируемой) прибыли. Потеря клиентов, поставщиков. Невозможность заключения договоров, соглашений.
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия).

VI. Заключение

Определенный перечень актуальных угроз дает возможность сформулировать требования по защите информации, осуществить выбор программных и технических средств защиты, а также организационных мер, которые должны быть использованы при эксплуатации и модернизации сегмента ГИС ЕИБД.

По результатам определения угроз безопасности информации сегмента ГИС ЕИБД корректировка структурно-функциональных характеристик сегмента ГИС ЕИБД, направленных на блокирование (нейтрализацию) отдельных угроз безопасности информации, не требуется.

Выявленные актуальные угрозы безопасности информации должны быть предотвращены с помощью проведения соответствующих мероприятий по технической и организационной защите информации.

Меры защиты информации, обеспечивающие блокирование (нейтрализацию) выявленных актуальных угрозы безопасности информации, приведены в документации технического проекта на сегменте ГИС ЕИБД.

В случае изменения состава программных или технических средств, входящих в состав сегмента ГИС ЕИБД, функционального назначения сегмента ГИС ЕИБД, осуществления мероприятий по защите информации Модель угроз должна быть пересмотрена.

VII. Актуализация

Периодическая проверка актуальности настоящего документа проводится с интервалом не реже одного раза в год, обновление документа проводится по мере необходимости.

Решение об изменении настоящего документа принимает должностное лицо, ответственное за выполнение мероприятий по обеспечению защиты информации и Руководитель оператора сегменте ГИС ЕИБД на основании результатов применения настоящего документа, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних проверок.

Приложение № 26
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2024 № 191

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей в трансфузиологическом кабинете

I. Общие положения

1.1. Настоящие Правила рассмотрения трансфузиологическим кабинетом (далее – ТК) запросов субъектов персональных данных или их представителей (далее – Правила) определяют порядок учета, рассмотрения и реагирования ТК (далее – Оператор) на запросы субъектов персональных данных или их представителей, действующих на основании нотариально заверенной доверенности либо в других случаях, предусмотренных действующим законодательством (далее – Представители).

1.2. Правила обязательны для исполнения всеми работниками Оператора, организующими процедуры учета и обработки обращений субъектов и их Представителей или непосредственно участвующие в процедурах учета и обработки обращений субъектов и их Представителей.

II. Взаимодействие Оператора с субъектами персональных данных

2.1. Ответственным работником Оператора за рассмотрение запросов субъектов персональных данных или их Представителей назначается ответственный за организацию обработки персональных данных в ТК или другое должностное лицо, назначаемое для рассмотрения запроса Оператором (далее – Ответственное лицо).

2.2. Субъекты, персональные данные которых обрабатываются Оператором, имеют право:

1) получать доступ к своим персональным данным.

2) требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

3) получать от Оператора информацию, содержащую:

– подтверждение факта обработки персональных данных Оператором;

– правовые основания обработки персональных данных Оператором;

– цели и применяемые Оператором способы обработки персональных данных;

– наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07. 2006 г. № 152-ФЗ «О персональных данных»;

– информацию об осуществленной, осуществляемой или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

4) возражать Оператору относительно принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении своих персональных данных или иным образом затрагивающих их права и законные интересы;

5) отозвать согласие на обработку персональных данных Оператором;

6) обжаловать в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействие Оператора при обработке и защите его персональных данных;

2.3. Субъекты, персональные данные которых обрабатываются Оператором, обязаны предоставлять Оператору достоверные сведения о себе и своевременно информировать об изменении своих персональных данных. Оператор имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Оператора документами.

2.4. Согласие на обработку персональных данных Оператором дается субъектом персональных данных или его Представителем в любой

позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

2.5. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07. 2006 г. № 152-ФЗ «О персональных данных».

2.6. Запросы субъекта или его Представителя, поступающие Оператору, фиксируются Ответственным лицом в Журнале учета обращений субъектов персональных данных и их представителей (утвержденный Приказом руководителя ТК).

2.7. При поступлении запроса в письменной форме субъекта или его Представителя о предоставлении сведений, указанных в подпункте 2.2.3 пункта 2.2 настоящих Правил, Ответственное лицо направляет ответ в письменной форме на запрос субъекта персональных данных или его Представителя в течение тридцати дней с даты получения запроса субъекта персональных данных или его Представителя.

В случае требования предоставления иных, непредусмотренных законодательством сведений, Ответственное лицо составляет мотивированный отказ в письменной форме, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07. 2006 г. № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его Представителя либо с даты получения запроса субъекта персональных данных или его Представителя.

2.8. Ответственное лицо обязано обеспечить текущее хранение нижеуказанных документов в течение трех лет, а по истечении указанного срока – передать документы на архивное хранение:

– запросы субъекта персональных данных или его Представителя;

– копии документов, являющихся основанием для уточнения или отказа в уточнении обрабатываемых персональных данных;

– копии документов, являющихся основанием для прекращения неправомерной обработки персональных данных или отказа в прекращении обработки персональных данных;

– копии документов, являющихся основанием для отказа в прекращении обработки персональных данных;

– уведомления субъекта персональных данных или его Представителя об уточнении или об отказе уточнения обрабатываемых персональных данных;

– уведомления субъекта персональных данных или его Представителя о прекращении неправомерной обработки персональных данных или отказе в прекращении обработки персональных данных;

– уведомления субъекта персональных данных или его Представителя о прекращении обработки персональных данных или отказе в прекращении обработки персональных данных;

– иные документы и копии иных документов, непосредственно связанные с выполнением Оператором своих обязанностей по рассмотрению запросов субъекта персональных данных или его Представителя.

III. Обработка запросов об уточнении неполных, устаревших, неточных персональных данных

3.1. В случае запроса субъекта персональных данных или его Представителя об уточнении Оператором (или лицом, действующим по поручению Оператора) обработки неполных, устаревших, неточных персональных данных Ответственное лицо обязано:

– зафиксировать наличие запроса субъекта персональных данных или его Представителя об уточнении обработки неполных, устаревших, неточных персональных данных в Журнале учета обращений субъектов персональных данных и их представителей (утвержденный Приказом руководителя ТК);

– осуществить блокирование указанных персональных данных с момента получения запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

– осуществить проверку фактов, изложенных в запросе, и подтверждающих факты документов, предоставляемых субъектом персональных данных или его Представителем.

3.2. В случае подтверждения фактов, изложенных в запросе, Ответственное лицо обязано:

– произвести или обеспечить уточнение указанных персональных данных на основании представленных сведений в течение семи рабочих дней со дня представления таких сведений;

– осуществить снятие блокирования указанных персональных данных;

– в письменной форме уведомить субъекта персональных данных или его Представителя об устранении допущенных нарушений.

3.3. В случае не подтверждения фактов, изложенных в запросе, Ответственное лицо обязано:

– осуществить снятие блокирования указанных персональных данных;

– уведомить в письменной форме субъекта персональных данных или его Представителя об отказе в уточнении персональных данных.

IV. Обработка запросов о прекращении неправомерной обработки персональных данных

4.1. В случае запроса субъекта персональных данных или его Представителя о прекращении неправомерной обработки Оператором (или лицом, действующим по поручению Оператора) персональных данных Ответственное лицо обязано:

– зафиксировать запрос субъекта персональных данных или его Представителя о прекращении неправомерной обработки персональных данных в Журнале учета обращений субъектов персональных данных и их представителей (утвержденный Приказом руководителя ТК);

– осуществить блокирование указанных персональных данных с момента получения запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц;

– осуществить проверку фактов, изложенных в запросе, и подтверждающих факты документов, предоставляемых субъектом персональных данных или его Представителем.

4.2. В случае подтверждения факта неправомерной обработки персональных данных Ответственное лицо обязано:

– прекратить или обеспечить прекращение неправомерной обработки персональных данных в срок, не превышающий трех рабочих дней с даты выявления неправомерной обработки персональных данных;

– уничтожить такие персональные данные или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, если обеспечить правомерность обработки персональных данных невозможно;

– уведомить в письменной форме субъекта персональных данных или его Представителя о прекращении неправомерной обработки персональных данных;

4.3. В случае не подтверждения факта неправомерной обработки персональных данных Ответственное лицо обязано:

– осуществить снятие блокирования указанных персональных данных;

– уведомить в письменной форме субъекта персональных данных или его Представителя об отказе в прекращении обработки персональных данных в срок, не превышающий тридцати дней с даты поступления запроса субъекта

персональных данных или его Представителя о прекращении неправомерной обработки персональных данных.

V. Обработка отзывов согласий на обработку персональных данных

5.1. В случае отзыва субъектом персональных данных или его Представителем согласия на обработку его персональных данных Оператором Ответственное лицо обязано зафиксировать наличие отзыва субъектом персональных данных или его Представителем согласия на обработку его персональных данных в Журнале учета обращений субъектов персональных данных или их представителей (утвержденный Приказом руководителя ТК).

5.2. Если обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, Ответственное лицо обязано:

- уведомить субъекта о последствиях отзыва им согласия;
- уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом;
- уведомить в письменной форме субъекта персональных данных или его Представителя о прекращении обработки персональных данных.

5.3. Если обработка персональных данных осуществляется при выполнении условий, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Ответственное лицо обязано в письменной форме (содержащей ссылку на положения части 2 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа) уведомить субъекта персональных данных или его Представителя об отказе в прекращении обработки персональных данных.

VI. Предоставление персональных данных субъектов их Представителям, членам их семей и родственникам

6.1. Представителю субъекта персональные данные передаются в порядке, установленном действующим законодательством.

6.2. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого

субъекта, за исключением случаев, когда передача персональных данных субъекта без его согласия допускается действующим законодательством РФ.

VII. Порядок обработки запросов субъектов персональных данных или их представителей

Порядок обработки запросов субъектов персональных данных или их представителей приведен в таблице:

№	Запрос	Действия	Срок	Ответ
1. Запрос субъекта персональных данных (далее – ПДн)				
1.1.	Обработка ПДн	Подтверждение обработки ПДн	30 дней (согласно ч.1 ст.20 закона № 152-ФЗ)	Подтверждение обработки ПДн
		Отказ подтверждения обработки ПДн	30 дней (согласно ч.2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе подтверждения обработки ПДн
1.2.	Ознакомление с ПДн	Предоставление информации по ПДн	30 дней (согласно ч. 1 ст. 20 закона № 152-ФЗ)	1. Подтверждение обработки ПДн, а также правовые основания и цели такой обработки
				2. Способы обработки ПДн
				3. Сведения о лицах, которые имеют доступ к ПДн
				4. Перечень обрабатываемых ПДн и источник их получения
				5. Сроки обработки ПДн, в том числе сроки их хранения
				6. Информация об осуществленной или о предполагаемой трансграничной передаче
		Отказ предоставления информации по ПДн	30 дней (согласно ч. 2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе предоставления информации по ПДн
1.3.	Уточнение ПДн	Изменение ПДн	7 рабочих дней с даты предоставления уточняющих сведений (согласно ч. 3 ст. 20 закона № 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения ПДн	30 дней (согласно ч. 2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе предоставления изменения ПДн
1.4.	Уничтожение ПДн	Уничтожение ПДн	7 рабочих дней с даты предоставления сведений о незаконном	Уведомление об уничтожении

№	Запрос	Действия	Срок	Ответ
			получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно ч. 3 ст. 20 закона № 152-ФЗ)	
		Отказ уничтожение ПДн	30 дней (согласно ч. 2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе уничтожения ПДн
1.5.	Отзыв согласия на обработку ПДн	Прекращение обработки и уничтожение ПДн	30 дней (согласно ч. 5 ст. 21 закона № 152-ФЗ)	Уведомление о прекращении обработки и уничтожении ПДн
		Отказ прекращения обработки и уничтожения ПДн	30 дней (согласно ч. 2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе прекращения обработки и уничтожения ПДн
1.6.	Недостоверность ПДн субъекта	Блокировка ПДн	С момента обращения субъекта ПДн о недостоверности или с момента получения запроса на период проверки (согласно ч. 1 ст. 21 закона № 152-ФЗ)	Уведомление о блокировке ПДн
		Изменение ПДн	7 рабочих дней с даты предоставления уточненных сведений (согласно ч. 2 ст. 21 закона № 152-ФЗ)	Уведомление о внесенных изменениях ПДн
		Снятие блокировки ПДн	После внесения изменений	
		Отказ изменения ПДн	30 дней (согласно ч. 2 ст. 20 закона № 152-ФЗ)	Уведомление об отказе изменения ПДн
1.7.	Неправомерность действий с ПДн субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно ч. 3 ст. 21 закона № 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно ч. 3 ст. 21 закона № 152-ФЗ)	Уведомление об уничтожении ПДн

№	Запрос	Действия	Срок	Ответ
1.8.	Достижение целей обработки ПДн	Прекращение обработки ПДн, Уничтожение ПДн	30 дней (согласно ч. 4 ст. 21 закона № 152-ФЗ)	Уведомление об уничтожении ПДн

Приложение № 27
к приказу ФГБОУ ВО БГМУ
Минздрава России
от 08.12.2021 № 191

ЖУРНАЛ №____
учета обращений субъектов персональных данных или их представителей о выполнении их законных прав, при обработке их персональных данных

Начат «____» _____20____г.
Окончен «____» _____20____г.

№ п.п.	Фамилия И.О. обратившегося лица	Документы, подтверждающие полномочия обратившегося лица*	Сведения об обращении		Действие по обращению	Сведения о принятом решении		Подпись исполнителя	Примечание
			Дата	Предмет		Дата	Основание		
1	2	3	4	5	6	7	8	9	10