Федеральное государственное бюджетное профессиональное образовательное учреждение «Электростальский медицинский колледж
Федерального медико-биологического агентства»

УТВЕРЖДАЮ
Директор ФГБПОУ
ЭМК ФМБА России
_____Н.Н. Шарапина

Перечень событий безопасности, подлежащих регистрации в информационных системах персональных данных

№ п/п	Наименование события безопасности	Состав и содержание информации о событии безопасности	Программное средство	Срок хранения информации о событии безопасности	Периодичность аудита (просмотра, анализа) результатов регистрации событий безопасности
1	**2**	**3**	**4**	**5**	**6**
1.	вход (выход), а также попытки входа субъектов доступа в операционную систему	тип события, дата и время входа (выхода), источник события, результат попытки (успешно или неуспешно), субъект доступа (пользователь или процесс), идентификатор, предъявленный при попытке доступа	Операционная система (далее – ОС), средство защиты информации от несанкциониро-ванного доступа (далее – СЗИ от НСД)	30 дней	Не реже 1 раза в неделю
2.	загрузка (останов) операционной системы	тип события, дата и время загрузки (останова) операционной системы, источник события, результат попытки (успешно или	ОС, СЗИ от НСД	30 дней	Не реже 1 раза в неделю

№ п/п	Наименование события безопасности	Состав и содержание информации о событии безопасности	Программное средство	Срок хранения информации о событии безопасности	Периодичность аудита (просмотра, анализа) результатов регистрации событий безопасности
1	2	3	4	5	6
		неуспешно), субъект доступа (пользователь или процесс), идентификатор, предъявленный при попытке доступа			
3.	подключение машинных носителей информации	тип события, дата и время подключения машинного носителя информации, логическое имя (номер) подключаемого машинного носителя информации, результат попытки, субъект доступа (пользователь или процесс)	СЗИ от НСД	30 дней	Не реже 1 раза в неделю
4.	вывод информации на носители информации	тип события, дата и время вывода информации на носитель информации, логическое имя (номер) машинного носителя информации, результат попытки, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации	СЗИ от НСД	30 дней	Не реже 1 раза в неделю
5.	запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	тип события, дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)	СЗИ от НСД	30 дней	Не реже 1 раза в неделю
6.	попытка доступа программных средств к защищаемым объектам доступа (каталогам, файлам)	тип события, дата и время попытки доступа к защищаемому объекту, результат попытки (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип)	ОС, СЗИ от НСД	30 дней	Не реже 1 раза в неделю

№ п/п	Наименование события безопасности	Состав и содержание информации о событии безопасности	Программное средство	Срок хранения информации о событии безопасности	Периодичность аудита (просмотра, анализа) результатов регистрации событий безопасности
1	2	3	4	5	6
7.	попытка удаленного доступа	тип события, дата и время попытки удаленного доступа, результата попытки (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе	ОС	30 дней	Не реже 1 раза в неделю
8.	о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов)	тип события, дата и время обнаружения, имя компьютера, IP адрес, учетная запись, тип ошибки, описание ошибки	Средство антивирусной защиты	30 дней	Не реже 1 раза в день
9.	обнаружение вредоносных компьютерных программ (вирусов)	тип события, дата и время обнаружение, имя компьютера, имя учетной записи, путь к файлу, действие, обнаруженный объект, IP адрес	Средство антивирусной защиты	30 дней	Не реже 1 раза в день
10.	сведения о сетевых атаках	имя компьютера на которого осуществлена атака, IP адрес сетевого устройства, на которого осуществлена атака, дата и время атаки, IP адрес атакующего, протокол и номер порта, на которого осуществлена атака	Средство обнаружения вторжений	30 дней	Не реже 1 раза в день