ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0296759800C0B293A84B02717194FF8892
Владелец: СОКОЛЕНКО ЮЛИЯ АЛЕКСАНДРОВНА
Действителен: с 15.04.2025 до 15.07.2026

ПРИЛОЖЕНИЕ №12
УТВЕРЖДЕНО
Приказом
МКУ ДО «ЦППМ и СП»
От 05.08.2025 № 138
«О вводе в действие комплекта организационно-
распорядительной документации
по организации обработки и защиты персональных данных»
Директор
Соколенко Юлия Александровна

_____
(подпись, печать)

«___» _____ 2025 г.

ИНСТРУКЦИЯ

по управлению событиями информационной безопасности информационных систем персональных данных в МКУ ДО «ЦППМ и СП»

1. Общие положения

1.1. Настоящая Инструкция по управлению событиями информационной безопасности информационных систем персональных данных в МКУ ДО «ЦППМ и СП» (далее – Инструкция) определяет в МКУ ДО «ЦППМ и СП» перечень событий информационной безопасности, подлежащих регистрации и сроки их хранения, состав и содержание информации о событиях безопасности, подлежащих регистрации, порядок сбора, записи и хранения информации о событиях информационной безопасности в течение определенного времени хранения, а также порядок защиты информации о событиях информационной безопасности информационных систем персональных данных (далее – информационные системы) в МКУ ДО «ЦППМ и СП».

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные
Событие ИБ	Событие информационной безопасности

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Событие информационной безопасности	Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение	ГОСТ Р ИСО МЭК 27001

Термин	Определение	Источник
	политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью	

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

приказ 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».

1.4. Администратор безопасности информационных систем и системный администратор информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах под подпись. Обязанность по организации ознакомления вышеуказанных работников с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Перечень событий информационной безопасности, подлежащих регистрации, и сроки их хранения

2.1. К регистрируемым события ИБ относятся события:

– события ИБ, имеющие отношение к возможности реализации угроз безопасности ПДн, обрабатываемых в информационных системах, описанных в Моделях угроз безопасности информации для информационных систем;

– события ИБ, регистрируемые в журналах операционных систем технических средств информационных систем и средств защиты информации;

– организационно-технические события информационной безопасности в инфраструктуре информационных систем.

2.2. Автоматически определяемые события ИБ регистрируются автоматически в электронных журналах сообщений программных средств информационных систем и средств защиты информации и хранятся в течение времени не менее 1 месяца со дня регистрации события ИБ.

2.3. События ИБ, не определяемые автоматически регистрируются журналах событий информационной безопасности информационных систем по форме Приложения №1 к настоящей Инструкции. На каждую информационную систему заводится отдельный журнал.

Ведение и надежное хранение журналов событий информационной безопасности информационных систем осуществляет администратор безопасности.

Срок хранения завершенных журналов событий информационной безопасности информационных систем персональных данных определяется утвержденной номенклатурой МКУ ДО «ЦППМ и СП».

Уничтожение журналов событий информационной безопасности информационных систем по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в МКУ ДО «ЦППМ и СП».

2.4. Перечень событий безопасности, не определяемых автоматически и которые необходимо регистрировать при их возникновении, приведен в Перечне регистрируемых событий информационной безопасности персональных данных информационных систем (Приложение №2 к настоящей Инструкции).

3. Состав и содержание информации о событиях информационной безопасности, подлежащих регистрации

3.1. Состав и содержание информации по каждому событию ИБ, должны идентифицировать тип события, источник события ИБ, дату, время и результат события, а также пользователя информационных систем, связанного с данным событием.

4. Порядок сбора, записи и хранения событий информационной безопасности

4.1. Настройку электронных журналов регистрации событий ИБ в программном обеспечении информационных систем и средств защиты информации осуществляет системный администратор информационных систем и администратор безопасности каждый в своей части. Настройка осуществляется в соответствии с эксплуатационной документацией на программно–технические средства информационных систем.

4.2. Системные администраторы информационных систем и администратор безопасности должны с периодичностью не реже 1 раза в неделю просматривать журналы регистрации событий безопасности информационных систем.

4.3. Настройки электронных журналов регистрации событий ИБ должны обеспечивать запись в память технических средств информационных систем и средств защиты информации информацию о поступающих событиях безопасности без переполнения памяти в течение 1 месяца с момента регистрации события ИБ.

4.4. Информация о событиях безопасности в информационных системах, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности при ее обнаружении в журнале событий информационной безопасности.

4.5. В случае обнаружения установления факта и/или компьютерного инцидента неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, администратор безопасности обязан немедленно сообщить о таком факте ответственному за организацию обработки персональных данных в МКУ ДО «ЦППМ и СП», который принимает меры в

соответствии с Инструкцией о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в МКУ ДО «ЦППМ и СП».

5. Защита информации о событиях информационной безопасности

5.1. Права доступа к файлам отчетов электронных журналов безопасности и настройкам журналов установлены администратору безопасности и системным администраторам информационных систем, в части касающейся в соответствии с Матрицей доступа.

5.2. Доступ к электронным журналам безопасности информационных систем пользователям информационных систем запрещен.

5.3. Ответственность за сохранность журнала событий информационной безопасности информационных систем по форме Приложения №1 к настоящей Инструкции и за конфиденциальность заносимой в него информации несет администратор безопасности.

6. Ответственность

6.1. Работники МКУ ДО «ЦППМ и СП» несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ №1
к Инструкции по управлению событиями информационной безопасности
информационных систем персональных данных
в МКУ ДО «ЦППМ и СП»

ЖУРНАЛ
событий информационной безопасности
информационной системы персональных данных
МКУ ДО «ЦППМ и СП»

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№	Код события (в соответствии с перечнем регистрируемых событий ИБ)	Место события ИБ	Участники события ИБ, источник события ИЬ	Дата и время события ИБ	ФИО пользователя	Результат события ИБ	Подпись администратора безопасности
1	2	3	4	5	6	7	8
1	*006*	*АРМ №1*	*[И.О. Фамилия ответственного за организацию обработки ПДн] [И.О. Фамилия администратора безопасности] И.И. Иванов*	*обнаружено 01.01.2021, 11:45*	*Петров Сергей Геннадьевич*	*Пользователь заблокирован*	*_____ [И.О. Фамилия администратора безопасности]*

Лист _____

Правила
по формированию и ведению
журналов событий информационной безопасности
информационных систем персональных данных МКУ ДО «ЦППМ и СП»

1. **Формирование журнала**

Журнал ведется на бумажных носителях (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителем МКУ ДО «ЦППМ и СП» с указанием количества прошитых и пронумерованных листов в журнале.

2. **Ведение журнала**

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – код события из перечня регистрируемых событий;
- Графа 3 – указывается название рабочего места пользователя;
- Графа 4 – указываются участники события и источник события ИБ;
- Графа 5 – дата и время события ИБ;
- Графа 6 – Ф.И.О. пользователя;
- Графа 7 – результат события ИБ;
- Графа 8 – подпись администратора безопасности.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

ПРИЛОЖЕНИЕ №1
к Инструкции по управлению событиями информационной безопасности
информационных систем персональных данных
в МКУ ДО «ЦППМ и СП»

Перечень
регистрируемых событий информационной безопасности
информационных систем персональных данных МКУ ДО «ЦППМ и СП»

№ группы	Группа	Код события	Событие
1	Идентификация и аутентификация пользователей и устройств	001	Устаревший пароль (не соблюдены требования к срокам обновления пароля)
		002	Скомпрометированный пароль (пароль пользователя известен другому лицу)
		003	Утеря пароля (блокировка входа после неверного 3-х кратного входа)
		004	Пользователь не внесен в журнал выдачи первичных паролей
		005	Нет отметки в журнале выдачи первичных паролей отметки о блокировании доступа уволенному сотруднику.
		006	Пароль пользователя не соответствует требованиям
		007	Бездействие пользователя более установленного времени (блокировка доступа по истечению установленного интервала)
		008	Утеря аппаратного средства аутентификации.
		009	Порча аппаратного средства аутентификации
		010	
2	Машинные носители информации	011	Отсутствует учетный номер на МНИ и запись в журнале учета
		012	Превышение срока пользования учтенным МНИ
		013	Запись на учтенный МНИ иной информации вместе с ПДн
		014	Несанкционированный вынос МНИ из зоны обработки ПДн
		015	Несанкционированная передача МНИ другому пользователю
		016	Хранение МНИ на рабочем столе пользователя
		017	МНИ, оставленный без присмотра
		018	

		019	
		020	
3	Вирусы	021	Вирусная атака (заражение)
		022	Истек срок лицензии на антивирусное ПО и ПО не обновлено
		023	Сбои (нарушения в работе) антивирусного ПО
		024	
		025	
4	Контролируемая зона	026	Вынос учтенного оборудования информационных систем за границы контролируемой зоны
		027	Внутри контролируемой зоны неучтенные МНИ или неучтенные технические средства чтения и записи информации.
		028	Экран монитора виден со стороны двери или окон в контролируемом помещении
		029	В помещении контролируемой зоны отсутствуют сотрудник, помещение не заперто.
		030	В помещении контролируемой зоны без сопровождения присутствует сотрудник, не имеющий допуска к обработке ПДн.
		031	
		032	
		033	
		034	
		035	
5	СКЗИ	036	Компрометация СКЗИ (ключевая информация известна другому пользователю)
		037	Утеря СКЗИ или ключевой информации.
		038	Информация в журнале учета СКЗИ неактуальна (не обновлена)
		039	Нахождение инсталлирующих носителей, ЭД и ТД на СКЗИ в неположенном месте
		040	Действующие и резервные ключевые документы хранятся нераздельно
		041	Отсутствие или нарушение опломбирования оборудования с СКЗИ
		042	
		043	
		044	
		045	