П-151/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Инструкция
по управлению событиями информационной безопасности

1. Введение

1.1. Настоящая инструкция определяет для информационной системы (далее ИС) «ФИС ГИА и ФИС ФРДО»:

1.1.1. Перечень событий информационной безопасности (далее событий ИБ), подлежащих регистрации и сроки их хранения.

1.1.2. Состав и содержание информации о событиях безопасности, подлежащих регистрации.

1.1.3. Порядок сбора, записи и хранения информации о событиях безопасности в течение определенного времени хранения.

1.1.4. Порядок защиты информации о событиях безопасности.

2. Регистрация событий ИБ

2.1. В регистрируемые события ИБ должны быть включены события ИБ, имеющие отношение к возможности реализации угроз безопасности информации, обрабатываемой в ИС, описанных в модели угроз безопасности информации для ИС.

2.2. К регистрируемым событиям ИБ относятся события безопасности, регистрируемые в журналах операционных систем технических средств ИС и средств защиты информации (далее – СЗИ), а также организационно-технические события информационной безопасности в инфраструктуре ИС.

2.3. Автоматически определяемые события ИБ регистрируются автоматически в электронных журналах сообщений программных средств ИС и средств защиты информации (СЗИ).

2.4. События ИБ, не определяемые автоматически регистрируются в журнале событий безопасности по форме ПРИЛОЖЕНИЯ №1.

2.5. Перечень событий безопасности, не определяемых автоматически и которые необходимо регистрировать при их возникновении, приведен в перечне регистрируемых событий ИБ (ПРИЛОЖЕНИЕ №2).

3. Порядок сбора, записи и хранения событий ИБ

3.1. Настройку журналов регистрации событий ИБ в программном обеспечении ИС и СЗИ осуществляет системный администратор ИС на основании предоставленных полномочий и администратор безопасности каждый в своей части. Настройка

осуществляется в соответствии с эксплуатационной документацией на программно – технические средства ИС.

3.2. Системные администраторы ИС и администратор безопасности должны с периодичностью не реже 1 раза в неделю просматривать журналы регистрации событий безопасности ИС.

3.3. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца с момента регистрации события.

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

4. Защита информации о событиях ИБ

4.1. Права доступа к файлам отчетов электронных журналов безопасности и настройкам журналов установлены администратору безопасности и системным администраторам ИС.

4.2. Доступ к электронным журналам безопасности должен быть блокирован при пользовательском уровне доступа к ИС.

4.3. Ответственность за сохранность журнала событий безопасности по форме ПРИЛОЖЕНИЯ №1 и за конфиденциальность заносимой в него информации несет администратор безопасности.

5. Заключительные положения

5.1. Администратор безопасности и системные администраторы ИС должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

5.2. Администратор безопасности и системные администраторы ИС должны быть ознакомлены с настоящей инструкцией до начала работы с ИС под роспись.

5.3. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

6. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

6.1. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6.2. Приказ ФСТЭК России от 23.03.2017 года № 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

6.3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Разработчик:
заместителя директора по общим вопросам

_____/ Ю.Ю. Алексеев /

П-151/2019

ПРИЛОЖЕНИЕ № 1
к «Инструкции по управлению
событиями информационной безопасности»

ЖУРНАЛ
событий информационной безопасности.

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

№	Код события (в соответствии с перечнем регистрируемых событий ИБ)	Место события	Участники события	Дата	Подпись администратора безопасности
1	2	3	4	5	6

П-151/2019

ПРАВИЛА
по формированию и ведению журнала событий информационной безопасности.

ФОРМИРОВАНИЕ ЖУРНАЛА.

Журнал формируется из стандартных листов формата А4 в альбомной ориентации:

Обложка журнала изготавливается на отдельном листе.

Все листы журнала, за исключением листов обложки, нумеруются.

Все листы журнала, вместе с обложкой сшиваются.

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 (**например** – пароль пользователя не соответствует требованиям – **записать код 006**).

Графа 3 – указывается название рабочего места пользователя (**например – АРМ №3**).

Графа 4 – указываются участники события (**например** – для кода 006 это – пользователь **Иванов И.И.** и администратор безопасности **Сидоров С.С**.).

Графа 5 – для несъемных носителей указывается АРМ пользователя.

Графа 6 – ФИО пользователя (**например – Иванов И.И.**).

Графа 7 – дата события (**например – обнаружено 01.01.2017**).

Графа 8 – подпись администратора безопасности (**например – _____(Сидоров С.С.))**

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 № 2
к «Инструкции по управлению
событиями информационной безопасности»

ПЕРЕЧЕНЬ
регистрируемых событий информационной безопасности ИС «Государственная итоговая аттестация».

№ п/п	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 обрабатываемой информацией
		014	Несанкционированный вынос МНИ из зоны обработки информации
		015	Несанкционированная передача МНИ другому пользователю
		016	Хранение МНИ на рабочем столе пользователя
		017	МНИ, оставленный без присмотра
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 ИС 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 информации.
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	
6	ПО	046	Несанкционированная АБ установка (обновление) ПО
		047	ПО на дистрибутивных носителях не имеет лицензии.
		048	Хранение дистрибутивных носителей с устаревшим ПО
		049	Нет сведений о совместимости обновлений ПО с установленными СВТ
		050	

П-151/2019

Лист
ознакомления с «Инструкцией по управлению событиями информационной безопасности»

№ п/п	ФИО	Должность	Подпись, дата