Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение
«Политехнический колледж городского хозяйства»

Организационно-правовая документация

УТВЕРЖДЕНА
приказом директора
от 01.06 2023
№ 546 - ОД

ИНСТРУКЦИЯ

ПО УПРАВЛЕНИЮ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ГОРОДСКОГО ХОЗЯЙСТВА

Санкт-Петербург - 2023

	Должность	Фамилия И.О.	Подпись	Дата
Разработал	Специалист по защите информаций	Бабин С.А.		01.06.2023
Согласовано	Зам. директора по ПО	Бурдин Е.В.		01.06.2023
Согласовано	Начальник отдела ИО и ПП	Ваганов С.Н..		01.06.2023
Согласовано	Начальник отдела ДОУ	Шорина А.В.		01.06.2023

Приложение № 2

УТВЕРЖДЕНА
приказом директора
от 01.06 2023
№ 546 -ОД

ИНСТРУКЦИЯ
по управлению событиями информационной безопасности в информационных системах Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

1. Введение

1.1. Настоящая Инструкция по управлению событиями информационной безопасности в информационных системах Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства» определяет для информационной систем (в том числе для информационных систем персональных данных - ИСПДн):

1.1.1. Перечень событий информационной безопасности (далее – события 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 ИБ в течение определенного времени хранения.

1.1.4. Порядок защиты информации о событиях ИБ.

2 Регистрация событий ИБ

2.1. В регистрируемые события ИБ должны быть включены события ИБ, имеющие отношение к возможности реализации угроз безопасности ПДн, обрабатываемых в информационных системах, описанных в моделях угроз безопасности информации для инфрмационных систем.

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

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

2.4. Критические события ИБ (степень критичности определяется экспертным образом администратором безопасности с учетом рекомендаций п.2.5. настоящей инструкции), не определяемые автоматически регистрируются 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 информационных систем и СЗИ осуществляет технический специалист отдела информатизации образовательного и производственного процессов в консультации с администраторм безопасности. Настройка осуществляется в соответствии с эксплуатационной документацией на программно – технические средства информационной системы.

3.2. Администратор безопасности должен с периодичностью не реже 1 раза в десять календарных дней просматривать журналы регистрации событий безопасности для каждой информационной ситемы.

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

3.4. Информация о критических событиях безопасности в информационной системе (уровень критичности определяетя экспертным мнением администратора безопасности и специалистов отдела информатизации образовательного и производственного процессов), 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 («на чтение») к файлам отчетов электронных журналов безопасности и настройкам журналов установлены администратору безопасности.

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

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 специалисты отдела информатизации образовательного и производственного процессов должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

5.2. Администратор безопасности и специалисты отдела информатизации образовательного и производственного процессов должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн.
5.3. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Разработчик:

Специалист по защите информации
отдела ИО и ПП С.А.Бабин

СОГЛАСОВАНО

Зам. директора по ПО
_____ Е.В.Бурдин
_____ 2023

Начальник отдела ИО и ПП
_____ С.В.Ваганов
_____ 2023

Начальник отдела ДОУ
_____ А.В.Шорина
_____ 2023

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

к «Инструкции по управлению событиями информационной безопасности в информационных системах Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

Информация о внесенных изменениях					
№ изменения	№ листа	№ и дата приказа	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, внесшего изменения
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					

Информация о проведении актуализации		
Дата ежегодной актуализации	Результаты актуализации	Подпись разработчика

Приложение №1
к Инструкции по управлению событиями информационной безопасности в информационных системах Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

ЖУРНАЛ

событий информационной безопасности

Учетный № _____

202___ год. Листов (_____)

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

Лист _____

ПРАВИЛА

по формированию и ведению журнала событий информационной безопасности

1. Формирование журнала.

1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.

1.2. Обложка журнала изготавливается на отдельном листе.

1.3. Все листы журнала, за исключением листов обложки, нумеруются.

1.4. Все листы журнала, вместе с обложкой сшиваются.

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 (**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 **[И.О. Фамилия администратора безопасности информационной системы персональных данных]**).
- Графа 5 – для несъемных носителей указывается АРМ пользователя.
- Графа 6 – ФИО пользователя (**например – Иванов И.И.**).
- Графа 7 – дата события (**например – обнаружено 01.01.2018**).
- Графа 8 – подпись администратора безопасности (**например –_____ ([И.О. Фамилия администратора безопасности информационной системы персональных данных]))**

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 в информационных системах Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

ПЕРЕЧЕНЬ

регистрируемых событий информационной безопасности ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема»

№ 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 ИСПДн 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	