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

Организационно-правовая документация

УТВЕРЖДЕНА
приказом директора
от 01.06 2023
№ 546 - ОД

ИНСТРУКЦИЯ

КОНТРОЛЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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 № 4

УТВЕРЖДЕНА
приказом директора
от 01.06 2023
№ 546 -ОД

ИНСТРУКЦИЯ
контроля защищенности персональных данных

1. Введение

1.1. Настоящая «Инструкция контроля защищенности персональных данных» (далее –Инструкция) определяет порядок выявления, анализа и устранения уязвимостей, недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков и порядок действий администратора безопасности информационной системы персональных данных (далее – ИСПДн) в организации Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Политехнический колледж городского хозяйства» (далее – Организация) при контроле защищенности персональных данных, обрабатываемых в ИСПДн.

2. Порядок контроля защищенности персональных данных

2.1. Контроль защищенности персональных данных для ИСПДн в соответствии с настоящей инструкцией выполняется комиссией в следующем составе: инженер отдела информатизации образовательного и производственного процессов, администратор безопасности, начальник отдела информатизации образовательного и производственного процессов (утверждает результаты) с периодичностью не реже один раз в год. По результатам контрольных процедур составляется справка. Допускается оформление единой справки для всех ИСПДн проконтролированных во время проверки, с детализацией (при необходимости) отклонений для конкретных ИСПДн.

2.2. Проведение проверки планируются в рамках проведения мероприятий внутреннего контроля в соответствии с действующей редакцией документа: «Правила осуществления внутреннего контроля обработки персональных данных на соответствие требованиям к их защите».

2.3. В целях повышения осведомленности руководства и принятия управленческих решений, по итогам выполнения контрольных процедур за год об общих результатх контроля защищенности персональныых данных, соответсвующей служебной запиской ифнормируется Заместитель директора по производственному обучению.

2.4. Внеплановый контроль приоизводится по распоряжению ответственного за организацию обработки ПДн при необходимости: по рекомендации администратора безопасности на основе анализа журналов

событий безопасности, в случае утечки ПДн, компоментации учетных данных, других нештатных систуаций.

3. Выявление анализ и устранение уязвимостей

3.1. Уязвимость – это недостаток ИСПДн или системы защиты персональных данных (далее – ПДн), который может привести к реализации угрозы безопасности персональных данных.

3.2. В ИСПДн должно осуществляться выявление и устранение следующих типов уязвимостей:

3.2.1. Недостатки и (или) ошибки программного обеспечения (далее – ПО) ИСПДн и ее системы защиты информации (далее – СЗИ).

3.2.2. Недостатки аппаратных средств ИСПДН, в том числе аппаратных средств защиты информации.

3.2.3. Организационно-технические недостатки.

3.3. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за организацию обработки ПДн. Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей ИСПДн является администратор безопасности.

4. Недостатки программного обеспечения

4.1. Проверка конфигурации и настроек программно – технических средств ИСПДн и их систем защиты информации на соответствие требованиям эксплуатационной документации и требований к защите ПДн.

4.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение ИСПДн.

4.3. Проверка наличия последних обновлений используемого программного обеспечения ИСПДн:

4.3.1. Проверка соответствия обновлений версиям программного обеспечения, установленного в ИСПДн и системе защиты информации.

4.3.2. Проверка соблюдения периодичности обновлений вирусных баз средств защиты информации от вредоносного кода.

4.3.3. Проверка обновлений баз решающих правил для средств обнаружения вторжений (*при использовании средств обнаружения вторжений – необходимость определяется эксплуатационной документацией*).

4.3.4. Проверка обновлений баз признаков уязвимостей.

4.4. Устранение обнаруженных недостатков на основании своих полномочий осуществляют специалисты отдела информатизации образовательного и производственного процессов.

5. Недостатки аппаратных средств

5.1. К недостаткам аппаратных средств, используемых в ИСПДн, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

5.2. При выявлении недостатков аппаратных средств во время проведения контрольных процедур анализируют:

5.2.1. Техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищенности ИСПДн.
5.2.2. Наличие сертификатов соответствия на примененные в ИСПДн и ее системе защиты информации аппаратные средства.
5.2.3. Наличие у поставщиков обновленных версий аппаратных средств, примененных в ИСПДн и системе защиты информации.
5.2.4. Перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств.
5.2.5. Конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.
5.3. Обнаруженные в ходе проверки отклонения от конфигурации ИСПДн устраняет администратор системы. Координирует работы администратор безопасности. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор системы принимает меры по ремонту или замене этих аппаратных средств.

6. Организационно – технические недостатки

6.1. Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите ПДн, обрабатываемых в ИСПДн.
6.2. Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД).
6.3. Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям.
6.4. Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям.
6.5. Проверка соответствия выполнения правил разграничения доступа к ПДн и ресурсам ИСПДн принятым требованиям.
6.6. Проверка соответствия полномочий пользователей принятым требованиям.
6.7. Проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.
6.8. Проверка состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемых зонах ИСПДн).
6.9. Проверка знания и соблюдения пользователями ИСПДн основных нормативно-правовых актов в области защиты ПДн и требований ОРД.

7. Проверка выполнения требований к применяемым средствам критографической защиты (СКЗИ)

7.1. Проверяются выполнение следующих требований для СКЗИ (с отражением результатов в справке):
7.1.1. Состояние и актуальность журнала учета СКЗИ.
7.1.2. Состояние и актуальность журнала учета пользователей СКЗИ.

7.1.3. Соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ технических средств требованиям эксплуатационной документации на СКЗИ, ИСПДн и систему защиты информации.
7.1.4. Знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ.
7.1.5. Знание и выполнение пользователями правил защиты СКЗИ.

8. Заключительные положения

8.1. Ответственные за обработку персональных данных, администраторы систем, пользователи и администратор безопасности ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.
8.2. Ответственные за обработку персональных данных, администраторы систем, пользователи и администратор безопасности ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн.
8.3. 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
01.06 2023
Начальник отдела ИО и ПП
_____ С.В.Ваганов
01.06 2023
Начальник отдела ДОУ
_____ А.В.Шорина
01.06. 2023

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

к «Инструкция контроля защищенности персональных данных»

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.					
13.					
14.					

Информация о проведении актуализации		
Дата ежегодной актуализации	Результаты актуализации	Подпись разработчика