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

Организационно-правовая документация

УТВЕРЖДЕНА
приказом директора
от 01.06. 2023
№ 545 - ОД

ИНСТРУКЦИЯ

ПО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В САНКТ-ПЕТЕРБУРГСКОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ «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 № 4

УТВЕРЖДЕНА
приказом директора
от 01.06 2023
№ 545 -ОД

ИНСТРУКЦИЯ
по идентификации и аутентификации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

1. Введение

1.1. Настоящая «Инструкция по идентификации и аутентификации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства» (далее – Инструкция) определяет в организации Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Политехнический колледж городского хозяйства» (далее – Организация) порядок идентификации и аутентификации пользователей информационных систем персональных данных (далее – ИСПДн), являющихся сотрудниками Организации, порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации внешних пользователей ИСПДн, порядок идентификации/аутентификации устройств, а также обязанности пользователя ИСПДн и администратора безопасности.

2. Порядок идентификации и аутентификации сотрудников

2.1. Всем пользователям ИСПДн, являющимся сотрудниками Организации, допущенным в установленном порядке к работе с ИСПДн, присваиваются учетные записи в виде персональных идентификаторов (логины, имена пользователей). Идентификаторы определяют доступ к техническим средствам и информационным ресурсам ИСПДн и системам защиты информации ИСПДн.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в каждой ИСПДн и пароли, обеспечивающие аутентификацию (проверку подлинности) в каждой ИСПДн. Права пользователя по доступу к информационным ресурсам каждой ИСПДн, определяется должностью пользователя и матрицей доступа.

2.3. Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более *90* дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены из каждой ИСПДн при увольнении сотрудника Организации немедленно по окончании последнего сеанса работы

сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей каждой ИСПДн.

2.4. При приеме (увольнении) на работу сотрудника Организации или изменении полномочий (временное или бессрочное) действующего сотрудника Организации, изменения в его доступе к информационным ресурсам каждой ИСПДн и генерацию (уничтожение) идентификаторов и паролей, производит администратор безопасности.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и сообщаются пользователю.

2.6. При первом доступе к любой из ИСПДн пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в действующей редакции Инструкции по парольной защите в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства».

2.7. В случаях, предусмотренных нормативными документами по защите персональных данных (далее – ПДн), обрабатываемых в ИСПДн, либо по решению руководителя при особой ценности для Организации сведений, к которым необходимо обеспечить безопасный доступ, помимо паролей используются дополнительные атрибуты доступа – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надежную многофакторную аутентификацию.

2.8. Администратор безопасности осуществляет настройку в каждой ИСПДн параметров количества вводов неправильного пароля. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

2.9. Администратор безопасности организует настройку в каждой ИСПДн параметров блокирования сеанса доступа при превышении лимита времени бездействия пользователя.

3. Управление аппаратными средствами аутентификации

3.1. При использовании аппаратных средств аутентификации пользователей (смарт-карты, электронные ключи) выдачу, инициализацию, блокирование и утилизацию аппаратных средств аутентификации организует администратор безопасности.

3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор безопасности в журнале учета аппаратных средств аутентификации (**Приложение** к настоящей Инструкции).

4. Идентификация и аутентификация внешних пользователей

4.1. Присвоение идентификатора и выдача атрибутов аутентификации внешним пользователям каждой ИСПДн, осуществляется администратором безопасности. Учет внешних пользователей (если таковые требуются по эксплуатационной документации на систему), допущенных к обработке ПДн, осуществляет администратор безопасности.

5. Обязанности пользователя

5.1. Пользователь любой ИСПДн является частью системы защиты ПДн и обязан соблюдать следующие правила информационной безопасности:

5.1.1. Помнить свой идентификатор и пароль для каждой ИСПДн (если он является пользователем каждой ИСПДн).

5.1.2. Обеспечивать сохранность полученных аппаратных идентификаторов. Не предоставлять доступ к личному аппаратному идентификатору никому, кроме администратора безопасности.

5.1.3. Держать свои пароли в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Организации, в т.ч. руководителей) личные пароли.

5.1.4. Осуществлять ввод паролей только в условиях, исключающих их просмотр.

5.1.5. Не хранить записки-памятки с личными паролями на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.

5.1.6. Своевременно сообщать администратору безопасности о фактах компрометации паролей (когда пароли стали или может быть станут известны еще кому-либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора безопасности.

6. Обязанности администратора безопасности

6.1. Администратор безопасности осуществляет организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов в каждую ИСПДн, контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа.

6.2. Администратор безопасности обязан:

6.2.1. создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов к техническим средствам и информационным ресурсам каждой ИСПДн;

6.2.2. обеспечивать смену паролей пользователей с периодичностью не реже определенной в действующей редакции Инструкции по парольной защите в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства».

6.2.3. принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов;

6.2.4. сообщать ответственному за организацию обработки ПДн о подобных инцидентах;

6.2.5. выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.

6.3. Действия администратора безопасности при компрометации паролей и утрате аппаратных идентификаторов.
6.3.1. Заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора, к соответствующей ИСПДн.
6.3.2. Выявить действия, произведенные в ИСПДн с использованием скомпрометированных персональных идентификаторов и паролей доступа.
6.3.3. Доложить ответственному за организацию обработки ПДн об инциденте и предоставить результаты анализа инцидента.
6.3.4. Совместно с ответственным за организацию обработки ПДн определить необходимость расследования инцидента.
6.3.5. Создать и выдать пользователю новый персональный идентификатор и пароль доступа к соответствующей ИСПДн.

7. Заключительные положения

7.1. Пользователи каждой ИСПДн должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей инструкции.
7.2. Пользователи каждой ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы ИСПДн под роспись.
7.3. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. «Инструкция по идентификации и аутентификации».

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

Приложение №1
К Инструкции по идентификации и аутентификации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

ЖУРНАЛ

учета аппаратных средств аутентификации

Учетный № _____

202____ год. Листов (_____)

Наименование	ИНВ. №	ИСПДн	Дата периодического осмотра и подпись	Дата выдачи в индивидуальное пользование	Ф.И.О. Подпись индивидуального пользователя	Примечание
1	2	3	4	5	6	7

Лист_____

ПРАВИЛА
по формированию и ведению журнала учета аппаратных средств аутентификации

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 – наименование устройства (**например - ESMART Token USB 64K Metal**).
- Графа 2 – инвентарный или серийный номер устройства (**например – инв. № 000011.**).
- Графа 3 – название ИСПДн (**например – «АРМ передачи сведений в ФИС ГИА и Приема»**).
- Графа 4 – дата последнего осмотра и подпись администратора безопасности (**например – 01.01.2018 АБ _____ [И.О. Фамилия администратора безопасности информационной системы персональных данных]**).
- Графа 5 – дата передачи пользователю (**например – 12.06.2018**).
- Графа 6 – подпись пользователя (**например – _____ Иванов И.И.**).
- Графа 7 – любая информация, относящаяся к записанному устройству.

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

к «Инструкции по идентификации и аутентификации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «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

ЛИСТ ОЗНАКОМЛЕНИЯ

с «Инструкцией по идентификации и аутентификации в Санкт-Петербургском государственном бюджетном профессиональном образовательном учреждении «Политехнический колледж городского хозяйства»

(утверждена приказом от «1» 06 2023 № 545-Д

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата