Приложение № 7 к приказу
от 28.06.2019 № 01-09/315
УТВЕРЖДЕНА
приказом генерального директора
КГБОУ ХКЦВР Созвездие
от 28.06.2019 № 01-09/315

ИНСТРУКЦИЯ

по идентификации и аутентификации

1. ВВЕДЕНИЕ

1.1. Настоящая инструкция определяет: порядок идентификации и аутентификации пользователей, обрабатывающих персональные данные в информационных системах (ИС) в краевом государственном бюджетном образовательном учреждении «Хабаровский краевой центр внешкольной работы «Созвездие» (далее – учреждение), порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации устройств, а также обязанности пользователя и администратора безопасности.

2. ПОРЯДОК ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

2.1. Всем пользователям ИС, являющимся сотрудниками учреждения, допущенным к работе с ИС, в которой обрабатываются персональные данные, присваиваются учетные записи в виде персональных идентификаторов (логины, имена пользователей).

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

2.3. Персональные идентификаторы должны быть заблокированы при превышении времени неиспользования более 90 дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены при увольнении сотрудника Организации немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей.

2.4. При приеме изменении полномочий (временно или бессрочно) действующего сотрудника Организации, изменения в его доступе к информационным ресурсам ИС, производит администратор безопасности.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и выдаются пользователю под роспись в журнале учета выдачи первичных паролей (Приложение № 1 к настоящей инструкции).

2.6. При первом доступе к ИС пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей инструкции (п. 2.8).

2.7. В случаях, предусмотренных нормативными документами по защите информации, обрабатываемойв ИС, 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. Требования к сложности пароля:

2.8.1. длина пароля должна быть не менее шести символов;

2.8.2. в числе символов пароля обязательно должны присутствовать строчные и прописные буквы, цифры и специальные символы;

2.8.3. пароль не должен включать в себя легко вычисляемые значения символов (имена, фамилии, имена детей или домашних животных, наименования информационных систем, типичных для организации профессиональных терминов, номера телефонов, номера или марки автомобилей, адреса и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

2.8.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в трех символах;

2.8.5. Пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.9. Администратор безопасности осуществляет настройку в ИС параметров количества вводов неправильного пароля. Количество вводов неправильного пароля устанавливается равным 3. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

2.10. Администратор безопасности организует настройку в ИС параметров блокирования сеанса доступа при времени бездействия пользователя более 1 часа или по запросу 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 № 2 к настоящей инструкции).

4. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

4.1. Пользователь является частью системы защиты информациии обязан соблюдать следующие правила информационной безопасности:

4.1.1. Помнить свой идентификатор и пароль.

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

4.1.3. 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.

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

4.1.5. 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.

4.1.6. Своевременно сообщать администратору безопасности о фактах компрометации паролей, об утере или повреждении аппаратного идентификатора.

5. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

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

5.2. Администратор безопасности обязан:

5.2.1. Создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИС.

5.2.2. Обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены.

5.2.3. Свой собственный пароль администратор безопасности должен изменять не реже одного раза в месяц.

5.2.4. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов.

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

5.3. Действия администратора безопасности при компрометации паролей и утрате аппаратных идентификаторов.

5.3.1. Заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора.

5.3.2. Выявить действия, произведенные в ИС с использованием скомпрометированных персональных идентификаторов и паролей доступа.

5.3.3. Создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИС.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Пользователи ИС должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей инструкции.

6.2. Пользователи ИС должны быть ознакомлены с настоящей инструкцией до начала работы в ИС под роспись. Обязанность ознакомления пользователей с настоящей инструкцией лежит на администраторе безопасности.

6.3. Сотрудники учреждения, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

7. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

7.1. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7.2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Приложение № 1
к приказу Инструкции
по идентификации и аутентификации

ЖУРНАЛ

учета выдачи первичных паролей

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

№ пп.	ФИО работника	Должность	Подразделение	ИС	Первичный пароль	Дата выдачи	Подпись
1	2	3	4	5	6	7	8
1.							
2.							
…..							

ПРАВИЛА

по формированию и ведению журнала учета выдачи первичных паролей

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 – номер записи по порядку.

Графа 2 – ФИО сотрудника.

Графа 3 – занимаемая должность в организации.

Графа 4 – подразделение организации (если есть).

Графа 5 – название ИС (при наличии нескольких ИС).

Графа 6 – пароль, назначаемый администратором безопасности (**например – FJ78LY65**).

Графа 7 – дата выдачи или блокирования пароля.

Графа 8 – подпись сотрудника (при выдаче) или администратора безопасности (при блокировании).

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.

Приложение № 2
к приказу Инструкции
по идентификации и аутентификации

ЖУРНАЛ

учета аппаратных средств аутентификации

Начат: «___» _____ 20__ г.
Окончен: «___» _____ 20__ г.

№ п/п	Наименование	ИНВ.№	ИС	Дата выдачи в пользование	Ф.И.О. Подпись пользователя	Примечание
1	2	3	4	5	6	7
1.						
2.						
....						

ПРАВИЛА

по формированию и ведению журнала учета аппаратных средств аутентификации

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 – номер записи по порядку.

Графа 2 – наименование устройства (**например – ESMART TokenUSB 64KMetal**).

Графа 3 – инвентарный или серийный номер устройства (**например – инв. № 000011.**).

Графа 4 – название ИС.

Графа 5 – дата передачи пользователю.

Графа 6 – ФИО и подпись пользователя.

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.