



УТВЕРЖДАЮ

Директор ЛОГКУ «Леноблэкомилиция»

А.В. Слюньков

«02» декабря 2024 г.

ИНСТРУКЦИЯ по идентификации и аутентификации

1. ВВЕДЕНИЕ

1.1. Настоящая инструкция определяет в организации ЛОГКУ «Леноблэкомилиция» (далее – Организация) порядок идентификации и аутентификации пользователей информационных систем (далее ИС) «АЦК Финансы»/«1С Бухгалтерия Государственного Учреждения»/«1С Зарплата и Кадры», являющихся сотрудниками Организации, порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации устройств, а также обязанности пользователя ИС и администратора безопасности.

2. ПОРЯДОК ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

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

2.2. Персональный идентификатор (учетная запись) пользователя создается специалистами Оператора (Комитет финансов Ленинградской области) по запросу администратора 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, определяются должностью пользователя и его

ролью согласно заявлению, направляемому Оператору по утвержденной форме. Формы заявлений можно скачать с официального сайта Оператора по адресу https://finance.lenobl.ru/ru/informatsionnye-sistemy/isubp/organizaciya-podklyucheniya-k-ubp/new_user/

2.3. Персональные идентификаторы блокируются Оператором при превышении времени неиспользования более 90 дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены из ИС при увольнении сотрудника Организации немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИС. Данная процедура осуществляется Администратором безопасности посредством направления Оператору заявления по утвержденной Оператором форме.

2.4. При приеме (увольнении) на работу сотрудника Организации или изменении полномочий (временное или бессрочное) действующего сотрудника Организации, необходимо в кратчайшие сроки уведомить об этом Оператора, для внесения изменения в его доступ к информационным ресурсам ИС и генерацию (уничтожение) идентификаторов и паролей посредством направления заявления по утвержденной форме.

2.5. Первичные пароли генерируются Оператором 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, обрабатываемой в 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 восьми 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 четырех символах;

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

2.8.6. Оператором установлено максимальное количество вводов неправильного пароля, равное 3. Разблокирование пароля осуществляет сотрудник техподдержки Оператора при обращении пользователя с заблокированным паролем.

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 ИС является частью системы защиты информации и обязан соблюдать следующие правила информационной безопасности:

4.1.1. Помнить свой идентификатор и пароль для ИС.

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 (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 ИС до специального разрешения администратора безопасности.

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:

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

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

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

5.2.1.4. 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. Немедленно сообщить Оператору о необходимости 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. Запросить у Оператора 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 Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством РФ.

7. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

7.1. 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».

7.2. 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».

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

ПРИЛОЖЕНИЕ № 1
к «Инструкции по идентификации и аутентификации»

ЖУРНАЛ
выдачи первичных паролей.

Начат: «__» _____ 20__ г.

Окончен: «__» _____ 20__ г.

1	2	3	4	5	6	7	8	9
№ пп.	ФИО работника	Должность	Подразделение	Тип доступа	ИС	Первичный пароль	Дата выдачи/блокирования	Подпись
1								
2								
3								
4								
5								
6								
7								
8								

1	2	3	4	5	6	7	8	9
№ пп.	ФИО работника	Должность	Подразделение	Тип доступа	ИС	Первичный пароль	Дата выдачи/блокирования	Подпись
9								
10								
11								
12								
13								
14								
15								

ПРАВИЛА

по формированию и ведению журнала 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 – тип доступа (пользователь или администратор).

Графа 6 – название ИС (при наличии нескольких ИС).

Графа 7 – пароль, назначаемый Оператором (**например – 1Qaz3Edc**).

Графа 8 – дата выдачи или блокирования пароля.

Графа 9 – 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 «Инструкции по идентификации и аутентификации»

ЖУРНАЛ

учета аппаратных средств аутентификации.

Начат: «__» _____ 20__ г.

Окончен: «__» _____ 20__ г.

1	2	3	4	5	6	7
Наименование	ИНВ.№	ИС	Дата периодического осмотра и подпись	Дата выдачи в индивидуальное пользование	Ф.И.О. Подпись индивидуального пользователя	Примечание
ESMART Token USB 64K Metal	инв. № 000011	«Государственная итоговая аттестация»	1.01.2017 АБ Иванов П.А.	12.06.2017	Григорьева Т.А.	Пример заполнения

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 – наименование устройства (**например - ESMART Token USB 64K Metal**).

Графа 2 – инвентарный или серийный номер устройства (**например – инв. № 000011.**).

Графа 3 – название ИС.

Графа 4 – дата последнего осмотра и подпись администратора безопасности.

Графа 5 – дата передачи пользователю.

Графа 6 – 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.