МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГТУ», ВГТУ)

Система менеджмента качества

ИНСТРУКЦИЯ
ПО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Воронеж 2016

1 РАЗРАБОТАНО рабочей группой.

2 ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ начальник ОИСК Д.В. Макаров

3 УТВЕРЖДЕНА И ВВЕДЕНА В ДЕЙСТВИЕ приказом ректора ВГТУ
от 10.02.2016 № 05–01.18–0

4 ВВОДИТСЯ ВПЕРВЫЕ

1 Общие положения

1.1 Настоящая инструкция определяет в ВГТУ (далее - Организация) порядок действий администратора безопасности и пользователей информационной системы при прохождении процедур идентификации (узнавания) и аутентификации (подтверждении подлинности узнанного) пользователями в ИСПДн.

1.2 Настоящая Инструкция разработана на основе следующих нормативных документов:

– Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и защите информации».

– Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных».

– 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».

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

1.3 Пользователи ИСПДн должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

Пользователи ИСПДн должны быть ознакомлены с настоящей Инструкцией до начала работы с ИСПДн под роспись. Обязанность ознакомления пользователей с настоящей инструкцией лежит на ответственном по организации обработки ПДн.

1.4 Ответственным за создание, присвоение и уничтожение идентификаторов пользователей и устройств, хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации является **администратор безопасности.**

2 Порядок идентификации и аутентификации внутренних пользователей

2.1 К внутренним пользователям относятся работниками Организации, допущенные в установленном порядке к работе с ИСПДн, а также должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами Организации.

2.2 Пользователям присваиваются учётные записи в виде персональных идентификаторов (логины, имена пользователей).

2.3 Персональный идентификатор (учётная запись) пользователя создаётся администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют полномочия, определённые списком (матрицей) доступа в соответствии с Инструкцией по управлению доступом к информации.

2.4 В момент создания персонального идентификатора администратором безопасности генерируется и выдаётся пользователю первичный пароль под личную подпись в **журнале выдачи первичных паролей** (приложение 1).

2.5 При первом доступе пользователь обязан изменить выданный ему первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции (п. 2.7).

2.6 При приёме (увольнении) на работу работника Организации или изменении полномочий (временное или бессрочное) действующего работника Организации, включение (исключение) его данных в список доступа к информационным ресурсам ИСПДн и генерацию (уничтожение) идентификатора и пароля, производит администратор безопасности на основании приказа по Организации о предоставлении (запрете) работнику доступа к информационным ресурсам ИСПДн.

2.7 В случаях, предусмотренных нормативными документами по защите информации, обрабатываемой в ИСПДн, либо по решению руководителя при особой ценности для Организации сведений, к которым необходимо обеспечить безопасный доступ, помимо паролей используются дополнительные средства аутентификации – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надёжную многофакторную аутентификацию.

2.8 Требования к сложности пароля:

– длина пароля должна быть не менее шести символов;

– в числе символов пароля обязательно должны присутствовать строчные и прописные буквы;

– 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.);

– пароль действует не более 120 дней, по истечении которых пользователь обязан заменить его новым.

2.9 Администратор безопасности осуществляет настройку в информационной системе параметров количества вводов неправильного пароля. Максимальное количество неуспешных попыток аутентификации (ввода

неправильного пароля) до блокировки технического средства устанавливается равным 3-м попыткам. Разблокирование пароля осуществляет **администратор безопасности** при обращении к нему пользователя с заблокированным паролем.

2.10 Администратор безопасности организует настройку в информационной системе параметров блокирования сеанса доступа при времени бездействия пользователя более 15 минут или по запросу пользователя.

2.11 Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более 90 дней. Персональные идентификаторы должны быть удалены из информационной системы при увольнении работника Организации немедленно по окончании последнего сеанса работы работника, а уволенный работник должен быть исключён из числа пользователей ИСПДн.

3 Порядок управления 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 Учёт выдачи аппаратных средств аутентификации осуществляет администратор безопасности в **журнале учёта аппаратных средств аутентификации** (приложение 2).

4 Порядок идентификации/аутентификации внешних пользователей ИСПДн

4.1 Присвоение идентификатора и выдача атрибутов аутентификации пользователям ИСПДн не являющимся сотрудниками Организации (внешним пользователям), осуществляется администратором безопасности. Учёт внешних пользователей, допущенных к обработке персональных данных, осуществляет администратор безопасности в **матрице доступа.**

4.2 Выдачу и смену паролей, учёт паролей, учёт аппаратных средств аутентификации внешних пользователей, допущенных к обработке ПДн, организует администратор безопасности по правилам п.2, п.3 настоящей инструкции.

5 Обязанности пользователя ИСПДн

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

– помнить свой идентификатор и пароль;

– обеспечивать сохранность полученных аппаратных идентификаторов. Не предоставлять доступ к личному аппаратному идентификатору никому, кроме администратора безопасности;

– держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других работников Организации, в т.ч. руководителей) личный пароль;

– осуществлять ввод пароля только в условиях, исключающих его просмотр;

– не хранить записки-памятки с личным паролём на видном и/или в легко доступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п;

– своевременно сообщать администратору безопасности о фактах компрометации пароля (когда пароль стал или может быть известен ещё 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 и паролей доступа в ИСПДн, контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа.

6.2 Администратор безопасности обязан:

– создавать, вести учёт, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИСПДн;

– обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 120 дней; свой собственный пароль администратор безопасности должен изменять не реже одного раза в месяц;

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

– сообщать ответственному за организацию обработки персональных данных о подобных инцидентах;

– 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 ИСПДн.

6.3.2 Выявить действия, произведённые 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 ответственному за организацию обработки ПДн определить необходимость расследования инцидента.

6.3.5 Создать и выдать пользователю новый персональный идентификатор и пароль доступа к информационной системе.

Приложение 1

Журнал выдачи первичных паролей

Уч. № _____

2_____ год.

ФИО	Тип пользователя	Персональный идентификатор	Дата выдачи	Подпись	Примечания

Приложение 2

Журнал учёта аппаратных средств аутентификации

Уч. № _____

2_____ год.

_____

(наименование аппаратного средства)

Инв. №	Дата периодического осмотра	Результат периодического осмотра	Подпись лица, производившег о осмотр	Место нахождения	Дата выдачи в индивидуальное пользование	Ф.И.О., подпись индивидуальног о пользователя	Примечание