МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

Рег. от 31.04.2020 № 12-50-90

УТВЕРЖДАЮ
Проректор по экономике и финансам
_____ Н.А. Заривной
«31» июля 2020 г.

Инструкция
по организации парольной защиты в информационных системах ДВФУ

ИН-ДВФУ-476/2-2020

Процесс	П-7 «Управление инфраструктурой»
Держатель документа	Проректор по экономике и финансам
Ответственность за использование действующей версии документа несёт его пользователь. Действующая версия документа находится в СЭД «DIRECTUM» / Общая папка / Реестр ВНД ДВФУ / Действующие; СЭД «DIRECTUM» / Общая папка/ Библиотека изменений	

Владивосток
2020

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах ДВФУ (далее – Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах федерального государственного автономного образовательного учреждения высшего образования «Дальневосточный федеральный университет» (далее – ДВФУ), а также контроль за действиями пользователей и технических специалистов, отвечающих за администрирование компонентов информационной инфраструктуры ДВФУ, при их работе с паролями.

1.2. Настоящая Инструкция утверждается взамен Инструкции по организации парольной защиты в информационных системах ДВФУ (ИН-ДВФУ-476/1-2018), утвержденной приказом от 05.07.2018 № 12-13-1290

1.3. Настоящая Инструкция является локальным актом ДВФУ, обязательным для исполнения всеми пользователями, а также сотрудниками ДВФУ, в должностные обязанности которых входит сопровождение информационной инфраструктуры, в том числе информационной системы персональных данных ДВФУ.

1.4. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами:

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

– Федеральный закон от 27.07.2006 № 152-ФЗ «О 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»;

– приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Термины, определения и сокращения

2.1. В настоящей Инструкции используются следующие термины и определения:

Нештатная ситуация – состояние информационной системы, не предусмотренное документацией и приводящее к сбоям и отказам системы, отсутствию предоставляемого пользователям сервиса и требующее вмешательства технических специалистов для восстановления штатного функционирования системы.

Пользователь – лицо, получившее в установленном порядке ЕУЗ, имеющее доступ к ИС ДВФУ, в том числе к ИСПДн (например, сотрудник, обучающийся ДВФУ).

Стойкость пароля – мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким-либо методом.

Технический специалист – сотрудник ДВФУ, отвечающий за администрирование, обеспечение работоспособности и защиту компонентов ИС и ИСПДн ДВФУ.

2.2. В настоящей Инструкции используются следующие сокращения:

ИС (информационная система) – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

ИСПДн (информационная система персональных данных) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

ПДн (персональные данные) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3. Правила формирования паролей

3.1. Пароли выбираются пользователями и техническими специалистами самостоятельно, а также могут генерироваться и распределяться централизованно специалистами подразделения, ответственного за вопросы информатизации, с учетом следующих требований:

3.1.1. Общие требования:

– пароль не должен содержать легко вычисляемые сочетания символов (имена, фамилии и т.д.), которые можно угадать, основываясь на информации о пользователе, а также общепринятые сокращения (LAN, ADMIN, USER и т.п.);

– пароль не должен содержать имя учетной записи пользователя или какую-либо его часть;

– при смене пароля новое значение должно отличаться от значений 6 предыдущих паролей;

– минимальный срок действия пароля составляет 1 день.

– максимальный срок действия пароля составляет 120 дней.

3.1.2. Правила формирования паролей для пользователей:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля должны присутствовать символы минимум трех категорий из числа следующих четырех:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры (от 0 до 9);

– неалфавитные символы (например: !, $, #, %).

3.1.3. Правила формирования паролей для технических специалистов и паролей к оборудованию:

– длина пароля должна быть не менее 16 символов;

– в числе символов пароля должны присутствовать символы всех

категорий:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- неалфавитные символы (например: !, $, #, %).

3.2. При выборе пароля необходимо учитывать ограничения на длину и категории символов в конкретном общесистемном и прикладном программном обеспечении, средствах защиты (например, запрет на использование символов русского алфавита, отдельных неалфавитных символов и т.д.). В случае наличия ограничения на длину и/или категории символов необходимо формировать пароль максимально приближенный к требованиям, установленным настоящей Инструкцией.

3.3. Для формирования стойких значений паролей могут применяться специальные программные средства.

3.4. В случае если генерация паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на подразделение, ответственное за вопросы информатизации.

4. Порядок ввода паролей

4.1. В целях обеспечения выполнения требований информационной безопасности и противодействия попыткам подбора пароля в ИС, в том числе ИСПДн, ДВФУ определены следующие правила ввода пароля:

- символы вводимого пароля не отображаются на экране в явном виде. Допускается отображение символов вводимого пароля в виде условных знаков «*», «?», либо иными символами;
- производится учёт в электронных журналах событий всех попыток (успешных и неудачных) ввода пароля при получении доступа к ресурсам ИС, в том числе ИСПДн.

4.2. Ввод пароля должен осуществляться непосредственно

владельцем пароля. Владельцу пароля запрещается передавать пароль другим лицам. Передача пароля другим лицам является нарушением правил парольной защиты и влечёт за собой ответственность.

4.3. Непосредственно перед вводом пароля для предотвращения возможности неверного ввода владелец пароля должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPSLOCK (если это необходимо), а также исключить возможность просмотра пароля посторонними лицами или техническими средствами.

4.4. При вводе пароля владельцу пароля запрещается проговаривать вслух вводимые символы.

4.5. С целью предотвращения несанкционированного доступа к ресурсам ИС, в том числе ИСПДн, методом подбора пароля установлено ограничение на количество неправильных попыток ввода пароля в размере 5 раз. При превышении данного количества неправильных попыток ввода пароля производится временная блокировка учетной записи. Снятие блокировки учетной записи производится автоматически через 15 минут после последней неудачной попытки ввода пароля.

5. Порядок смены паролей

5.1. Смена паролей пользователей и технических специалистов осуществляется в следующих случаях:

– истечение срока действия пароля;

– по собственной инициативе пользователя;

– при подозрении на компрометацию пароля со стороны пользователя;

– при получении информации о возможной компрометации пароля от подразделения, ответственного за вопросы обеспечения информационной безопасности.

5.2. В случае выявления фактов компрометации пароля пользователя

ИС, в том числе ИСПДн, должна производиться внеплановая смена пароля пользователя или блокировка его учетной записи (при необходимости).

5.3. Смена паролей производится в соответствии с эксплуатационной документацией (руководством администратора) на конкретное общесистемное, прикладное программное обеспечение, средства защиты информации.

5.4. Специалисты подразделения, ответственного за вопросы информатизации, оказывают необходимую консультацию пользователям в процессе смены пароля.

5.5. В случае если специалистами подразделения, ответственного за вопросы информатизации, пользователю был установлен временный пароль, пользователь обязан его сменить при первом входе в систему.

6. Правила хранения паролей

6.1. Запрещается записывать пароли на бумаге, в файлах, электронных записных книжках, иных предметах, не предназначенных для хранения паролей.

6.2. Пользователям запрещается сообщать личный пароль посторонним лицам.

6.3. Аутентификация пользователей в ИС, в том числе ИСПДн, ДВФУ может осуществляться с использованием специальных аппаратно-программных средств, прошедших обязательную сертификацию Федеральной службы по техническому и экспортному контролю Российской Федерации либо Федеральной службы безопасности Российской Федерации в зависимости от категории решаемых задач.

6.4. Для хранения паролей допускается использование специализированного программного обеспечения – менеджеров паролей.

7. Компрометация паролей

7.1. Компрометацией паролей считается наступление одного либо

нескольких следующих событий:

– физическая утеря носителя, содержащего пароли;

– передача паролей и/или иной идентификационной информации по открытым каналам связи, выходящим за пределы контролируемой зоны;

– проникновение / подозрение на проникновение (например, срабатывание сигнализации, повреждение замков и т.д.) постороннего лица в помещение, в котором хранятся носители с паролями;

– перехват пароля;

– сознательная передача пользователем своего пароля постороннему лицу.

7.2. При подозрении на компрометацию пароля пользователь обязан:

– незамедлительно воспользоваться сервисом по изменению пароля от учетной записи с целью недопущения ее несанкционированного использования третьими лицами;

– известить о факте компрометации пароля своего непосредственного руководителя;

– известить о факте компрометации пароля подразделение, ответственное за вопросы информатизации.

7.3.При подозрении на компрометацию пароля со стороны пользователя уполномоченный сотрудники подразделения, ответственного за вопросы информатизации, обязаны:

– обеспечить контроль смены скомпрометированного пароля;

– предпринять меры, направленные на недопущение в дальнейшем подобных фактов компрометации.

7.4.При получении информации о возможной компрометации пароля подразделением, ответственным за вопросы обеспечения информационной безопасности, сотрудники указанного подразделения обязаны:

– инициировать процесс временной блокировки учетной записи пользователя;

– уведомить пользователя о предполагаемой компрометации пароля

и необходимости смены пароля;

– обеспечить контроль смены скомпрометированного пароля;

– провести расследование причин и условий инцидента с целью недопущения в дальнейшем подобных фактов компрометации.

8. Ответственность

8.1. Ответственность за соблюдение требований данной Инструкции возлагается на всех сотрудников, работников и обучающихся ДВФУ, являющихся пользователями ИС ДВФУ.

8.2. Контроль за исполнением требований Инструкции в ДВФУ возлагается на держателя документа.

9. Управление Положением

9.1. Настоящая Инструкция, изменения и дополнения к ней утверждаются проректором по экономике и финансам или иным уполномоченным в установленном порядке лицом.

9.2. Ответственность за поддержание настоящей Инструкции в актуальном состоянии несет держатель документа.

9.3. Подлинник настоящей Инструкции хранится в Отделе документационного обеспечения и контроля Организационно-административного департамента согласно утвержденной номенклатуре дел.

9.4. Порядок периодической проверки документа / внесения в документ изменений / прекращения его действия определен Регламентом управления внутренними нормативными документами в действующей редакции.

9.5. Настоящая Инструкция подлежит обязательной рассылке проректорам, директорам школ/филиалов, руководителям структурных подразделений.