РАБОЧАЯ ИНСТРУКЦИЯ

Система менеджмента качества **ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ФГБОУ ВО «КнАГУ»**	**РИ С.003-2023** **Введена впервые**

СОГЛАСОВАНО

Начальник правового управления
_____ А.В. Ременников
«02» ноября 2023 г.

Начальник ИТ-Управления
_____ Е.Б. Абарникова
«1» 11 2023 г.

УТВЕРЖДАЮ

Ректор университета
_____ Э.А. Дмитриев
«03» 11 2023 г.

Комсомольск-на-Амуре
2023

Введена приказом № 369-О от 03.11.2023

Содержание

1 Общие положения

1.1 Назначение

Настоящая инструкция устанавливает порядок генерации, смены и прекращения действия паролей и блокирования (удаления) имен учетных записей пользователей в информационных системах персональных данных (далее - ИСПДн) федерального государственного бюджетного образовательного учреждения высшего образования «Комсомольский-на-Амуре государственный университет» (далее – Университет).

1.2 Сфера действия

Настоящий документ распространяет свое действие на все учетные данные и рекомендуется для использования на всех рабочих местах Университета.

1.3 Область применения

Указанные в настоящей инструкции правила и требования должны применять все сотрудники ФГБОУ ВО «КнАГУ», использующие в своей работе автоматизированные рабочие места и имеющих доступ к информационным ресурсам организации в соответствии и в рамках своих должностных обязанностей.

2 Нормативные ссылки

Настоящая инструкция составлена 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».

Приказа ФСТЭК России 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».

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

3 Термины и определения

В настоящей инструкции применяются следующие термины с соответствующими определениями:

Автоматизированная система – система, состоящая из персонала и

комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Антивирусная программа (антивирус) – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов, а также предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Данные – информация, представленная в электронной форме.

Интернет – всемирная система объединённых компьютерных сетей для хранения и передачи информации.

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Пользователь – сотрудник университета, использующий АРМ.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

4 Ответственность

4.1 Ответственность за организацию парольной защиты в ИСПДн, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности (далее – АИБ).

4.2 Периодический контроль соблюдения установленного порядка организации парольной защиты и выполнением требований настоящей Инструкции пользователями ИСПДн осуществляется АИБ.

5 Организация парольной защиты

5.1 Требования к паролям

5.1.1 При формировании парольной информации независимо от способов формирования паролей, должны выполняться следующие требования:

- длина пароля пользователя должна быть не менее 6 символов;
- длина пароля привилегированных пользователей должна быть не менее 8 символов;
- в пароле должны присутствовать прописные и строчные буквы латинского алфавита (A…Z, a…z), арабские цифры (0…9) и (или) специальные знаки (!»№;%:?* и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 1 символе.

5.1.2 При формировании парольной информации запрещается:

- использовать простые пароли типа «P@ssw0rd», «1QaZ@wSx»;
- использовать в паролях имена и даты рождения, телефонные номера, номера автомобилей и т.п. (пароли которые можно подобрать, основываясь на информации о пользователе);
- использовать в качестве паролей комбинацию символов, набираемых в закономерном порядке на клавиатуре «qwerty12345», «1qaz2wsx» и т.п.
- использовать в качестве паролей один и тот же повторяющийся символ или комбинацию из нескольких символов.

5.1.3 В случае если в системе невозможно установить требования к парольной информации, выполнение требований к парольной информации реализуется организационными мерами.

5.2 Порядок смены паролей

5.2.1 Плановая смена паролей должна производиться не реже одного раза в 180 дней (если иными документами не установлены иные сроки).

5.2.2 Внеплановая смена пароля пользователя производится в случае компрометации или утери пароля пользователем.

5.2.3 В случае увольнения и (или) перехода на другую должность АИБ, должна осуществляется внеплановая смена паролей всех учетных записей ИСПДн.

5.2.4 Внеплановая смена всех паролей ИСПДн проводится в случае компрометации пароля АИБ.

5.2.5 В случае увольнения пользователя или его перехода на другую должность, не предусматривающую наличие прав по доступу к ресурсам ИСПДн, его учетная запись должна быть заблокирована в срок, не позднее следующего рабочего дня после увольнения (перехода).

5.3 Хранение и ввод паролей

5.3.1 При хранении паролей пользователями и АИБ ИСПДн должны выполнятся следующие требования:

- запрещается записывать пароли на бумаге, в файле, в записной книжке, в электронных устройствах и других носителях информации, в том числе предметах мебели и интерьера;
- запрещается сообщать другим пользователям свой пароль, а также осуществлять работу в ИСПДн с использованием чужих паролей;
- запрещается осуществлять регистрацию других пользователей в ИСПДн под своим паролем;
- допускается хранение пароля пользователя в запечатанном конверте в личном сейфе, либо в сейфе у АИБ.

5.3.2 При вводе паролей пользователи и АИБ ИСПДн должны соблюдать следующие правила:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был сформирован;
- во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами;
- запрещено проговаривать пароль вслух при его вводе.

6 Обязанности лиц, использующих пароли

Лица, использующие пароли для доступа в ИСПДн или отдельным элементам ИСПДн обязаны:

6.1 Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию паролей;

6.2 Своевременно сообщать АИБ об утере, компрометации, несанкционированном изменении паролей, фактах нарушения настоящей инструкции пользователями ИСПДн.

7 Разработчики

Начальник ИТУ Е.Б. Абарникова

Специалист по защите информации ОССА А.А. Аверин

Введена приказом № 369-О от 03.11.2023

Лист регистрации изменений

	Номер приказа, дата утверждения изменения	Количество страниц изменения	Дата получения изменения	Подпись уполномоченного по качеству

Введена приказом № 369-О от 03.11.2023