бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский многопрофильный колледж»

УТВЕРЖДЕНА
приказом директора колледжа
от 19.02.2019 г. № 44

ИНСТРУКЦИЯ

«19» 02 2019 г. № 30

г. Великий Устюг

по использованию реквизитов доступа в ИСПД/ГИС/АС

1. Парольная политика

1.1. Общие требования к паролям:

- минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; ’] [{ } <> . и т.п.);

- минимальная длина пароля: не менее 8 (восьми) символов;

- максимальный срок действия пароля: 90 суток;

- запрет использования трех ранее использовавшихся паролей;

- пароль Пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.).

1.2. Правила использования паролей:

- хранить в тайне свой пароль, не сообщать его другим лицам;

- не предоставлять доступ в ИСПД/ГИС/АС другим лицам под своей учетной записью и паролем;

- изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПД/ГИС/АС;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.);

- запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ (автоматизированного рабочего места), на обратной стороне клавиатуры и т.д.;

- запрещается хранить пароли в записанном виде на отдельных листах бумаги.

1.3. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:

- в случае подозрения на компрометацию пароля;

- по окончании срока действия;

- в случае прекращения полномочий (увольнение, переход на другую работу внутри колледжа) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

- по указанию ответственного за организацию обработки персональных данных.

1.4. При увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

2. Применение личных идентификаторов в информационной системе персональных данных

2.1. Привязку идентификаторак пользователю (учетной записи) выполняет администратор безопасности АС.

2.2. Пользователи ИСПД/ГИС/АС получают свой идентификатор у администратора безопасности АС.

2.3. Пользователь ИСПД/ГИС/АС обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

2.4. Пользователю ИСПД/ГИС/АС запрещается передавать свой личный идентификатор.

2.5. В случае утери личного идентификатора, пользователь ИСПД/ГИС/АС должен немедленно доложить об этом администратору безопасности АС.

2.6. В случае прекращения полномочий учетной записи пользователя ИСПД/ГИС/АС (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности АС после окончания последнего сеанса работы данного пользователя в ИСПД/ГИС/АС.

2.7. В случае компрометации или утери личного идентификатора пользователя ответственным за осуществление контроля за состоянием уровня защищенности информационных ресурсов и обеспечением защиты информации в колледже должны быть немедленно предприняты меры в соответствии с п. 2.8. настоящей Инструкции.

2.8. Администратор безопасности АС должен провести служебное расследование для выяснения причин компрометации идентификатора с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

2.9. После проведения служебного расследования администратор безопасности АС должен предоставить отчёт директору колледжа.

СОГЛАСОВАНО
Советом Учреждения
Протокол № 2
«18» 02 20 19 г.

В дело № 01-14
«19» 02 20 19 г.