

Название работы:  
**МЕТОДИЧЕСКАЯ РАЗРАБОТКА ДЛЯ ПРОВЕДЕНИЯ ЗАНЯТИЯ  
ПО ТЕМЕ «НАСТРОЙКА ПАРАМЕТРОВ АУТЕНТИФИКАЦИИ  
WINDOWS»**

Автор работы:  
Гринь Диляра Халельевна, преподаватель

Образовательная организация:  
КГБПОУ «Канский технологический колледж», г.Канск

2025 г.

## **Пояснительная записка**

Данное практическое занятие по дисциплине «Разработка кода информационных систем» проводится в Канском технологическом колледже со студентами групп 3 курса, обучающихся по специальности 09.02.07 Информационные системы и программирование.

**Тема занятия:** «Настройка параметров аутентификации Windows»

**Цель занятия:**

Создание условий для применения теоретических знаний на практике.

**Задачи занятия:**

Образовательные:

Планируется, что к окончанию урока обучающиеся будут владеть умениями по настройке параметров аутентификации ОС Windows и знать алгоритм создания надежного пароля.

Воспитательные:

– Создание условий, обеспечивающих воспитание интереса к своей будущей специальности.

– Воспитание ответственного отношения к работе.

Развивающие:

– Содействие развитию умений применять полученные знания в типовых условиях.

– Создание условий развития умений рационально распределять рабочее время.

**Тип урока:** применение и совершенствование знаний.

**Вид урока:** практическая работа.

**Опорные знания:** понятие информационной системы, аутентификации, идентификации, политики безопасности.

**Оборудование урока:**

1. Интерактивные средства обучения:

1.1. Проектор;

2. Программные средства:

ОС Windows, Google forms, удаленный рабочий стол, on-line таблица, Wiki-документ

Методическое обеспечение:

2.1. Презентация

2.2. Методические указания для выполнения практической работы.

2.3. Оценочный лист

**План урока:**

1. Организационный момент.

2. Постановка цели и задач урока.

3. Актуализация ранее полученных знаний.

4. Инструктаж.

5. Применение знаний и умений.

6. Обобщение и систематизация знаний.

7. Информация о домашнем задании.

## 8. Рефлексия.

### Описание урока:

Этапы урока	Цели этапа	Содержание обучения	Организация процесса обучения (методы, организационные формы, средства)
Орг. момент Постановка цели и задач урока. Мотивация учебной деятельности <b>(5 мин.)</b>	Создание условий для возникновения у обучающихся внутренней потребности включения в учебную деятельность, способствовать повышению мотивации учения	Приветствие, определение отсутствующих. Раскрытие целей и содержания урока.	Форма: фронтальная. Метод:опрос
Актуализация ранее полученных знаний <b>(5 мин.)</b>	Обобщение и закрепление знаний. Определить ошибки и пробелы в знаниях, стимулировать активность при тестировании	Решение теста, составленного по предыдущим лекциям, повторение основных понятий и определений	Метод: тестирование. Форма:индивидуальная. Средства: Проектор/googleforms
Инструктаж <b>(2 мин.)</b>	Определить цель работы, последовательность и время, отведенное на ее выполнение, критерии оценивания и правила представления результата	Описание цели практического занятия, последовательности выполнения заданий, установление критериев оценивания выполнения заданий.	Метод: демонстрация основных приемов работы. Форма: фронтальная. Средства: Проектор.
Применение знаний и умений <b>(40 мин.)</b>	Сформировать навыки по настройке параметров аутентификации ОС Windows, умение рационально распределять рабочее время	Настройка параметров аутентификации ОС Windows. Консультирование студентов преподавателем в ходе выполнения заданий.	Метод: практическое задание. Форма: индивидуальная. Средства: Методические указания для выполнения практической работы. Раздаточный материал

Обобщение и систематизация знаний <b>(32 мин.)</b>	Закрепить и систематизировать теоретические знания	Составление алгоритма.	Форма: фронтальная Средства: совместная доска ВИКИ
Информация о домашнем задании <b>(1 мин.)</b>	Создать условия для актуализации знаний по теме.	Написание отчета по практической работе	Форма: индивидуальная.
Рефлексия <b>(5 мин.)</b>	Получить обратную связь.	Составление синквейна	Метод: синквейн Форма: индивидуальная

## **Ход урока:**

### **1. Организационный момент. Постановка цели и задач урока. Мотивация учебной деятельности (5 мин)**

Здравствуйте, рада вас видеть, начнем наш урок.

Хотелось бы начать с новости. На сеть французских телеканалов TV5 Monde была совершена мощная хакерская атака, которая началась поздно вечером, когда хакеры заблокировали официальный сайт телесети, а уже спустя час получили доступ и к социальным аккаунтам телеканалов.

Затем злоумышленники добрались и до всех 11 каналов телевизионной группы: в течение пяти часов зрителям был доступен лишь чёрный экран с символами международной террористической организации. В ходе инцидента выяснилось, что пароли, которыми могли воспользоваться злоумышленники, были показаны в эфире французского телевидения самими сотрудниками телевизионной группы.

Как вы думаете, почему появилась уязвимость и стало возможным совершение атаки?

Следовательно, причиной кибератаки стало безответственное отношение сотрудников телесети к её безопасности.

### **2. Актуализация ранее полученных знаний (5 мин.)**

Сегодня мы на практике закрепим навыки настройки политики безопасности, в частности настройку параметров аутентификации домена и выведем правила создания надежного пароля и способы его хранения.

Но прежде чем мы приступим к работе, предлагаю пройти тестирование на знание теории. Ведь как известно «Теория без практики мертва, практика без теории слепа».

Перейдите по ссылке и выполните тестовое задание в googleформах. На это вам отводится 4 минуты, по их истечении вам необходимо отправить результат.

Анализ выполнения *тестового задания (результаты тестирования в google форме отображены на проекторе), разбор вопросов с ошибочными ответами.*

Молодцы! Справились и повторили. Занесите результаты теста в оценочный лист (**Приложение 1**). Эти знания помогут вам при выполнении заданий.

Проведем инструктаж к выполнению практической работы

### **3. Инструктаж (2 мин)**

Практическая работа состоит из 2 частей: общей части и задания для самостоятельной работы.

На это задание у вас 15 минут.

### **4. Применение знаний и умений (40 мин.)**

Перейдите к удаленному рабочему столу. Воспользуйтесь методическими указаниями (**Приложение 2**). Необходимо настроить политику безопасности, политику паролей и политику блокировки учетной записи.

А теперь сконфигурируйте надежный пароль и проверьте его с помощью специального сервиса <https://password.kaspersky.com/ru/>.

Результат проверки внесите в онлайн таблицу.

<https://docs.google.com/spreadsheets/d/1GMReHXXsOuiCxo0b7ZbxeU4R013zoNWV6cO1xF1PXcA/edit?usp=sharing>

Занесите результаты в оценочный лист.

## **5. Обобщение и систематизация знаний (32 мин.)**

По результатам работы давайте сформулируем основные правила создания и хранения пароля на совместной доске WIKI.

- 1. Использовать 12 символов;*
- 2. Используется три набора символов: маленькие буквы, большая буква «А», цифра «6» вместо буквы «б», специальные символы «@» и «-»;*
- 3. Не использовали общедоступную информацию (ни имя, ни дату рождения, ни номер телефона);*
- 4. Пароль не содержит словарных слов, значит его невозможно подобрать по словарю;*
- 5. Для разных сайтов используются разные пароли.*

Оцените свою работу, внесите оценку в лист самооценки.

## **6. Информация о домашнем задании ( 1 мин.)**

Домашнее задание, составить отчет по практической работе, прикрепить его к электронному курсу в Moodle.

## **7. Рефлексия (5 мин.)**

Вы все знакомы с понятием «синквейн».

Составьте синквейн к слову пароль или аутентификация на выбор (1 минута).

Что получилось? Сегодня вы на практике научились настраивать параметры аутентификации ОС Windows и сформулировали алгоритм создания надежного пароля.

Спасибо за работу.

### **Список использованных источников:**

1. **Партыка Т.Л., Попов П.П.** Информационная безопасность: Учебное пособие для студентов учреждений среднего профессионального образования. - М: ФОРУМ: ИНФРА-М, 2019.
2. **Анин Б.Ю.** Защита компьютерной информации. - СПб.: БХВ - Санкт-Петербург, 2020. - 384 с.
3. **Аскеров Т.М.** Защита информации и информационная безопасность: Учебное пособие/Под общей ред. Курбакова К.И. - М.: Рос. экон. академия, 2021. - 387 с.
4. **Горбатов В.С., Кондратьева Т.А.** Информационная безопасность. Основы правовой защиты: Учебное пособие. - 2-е изд., испр. и доп. - М.: МИФИ, 2021.
5. **Петров В.А., Пискарев А.С., Шейн А.В.** Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учебное пособие. - 2-е изд., испр. и доп. - М.: МИФИ, 2023.



## **Самоанализ урока**

**Тема:** «Настройка параметров аутентификации Windows»

**Цель занятия:**

Создание условий для применения теоретических знаний на практике.

**Задачи занятия:**

**Образовательные:**

Планируется, что к окончанию урока обучающиеся будут владеть умениями по настройке параметров аутентификации ОС Windows и знать алгоритм создания надежного пароля.

**Воспитательные:**

Создание условий, обеспечивающих воспитание интереса к своей будущей специальности.

Воспитание ответственного отношения к работе.

**Развивающие:**

Содействие развитию умений применять полученные знания в типовых условиях.

Создание условий развития умений рационально распределять рабочее время.

Занятие проходило группе ИС.09.21.1 по специальности 09.02.07 Информационные системы и программирование. В группе 24 человека, на занятии присутствовало 20 человек.

В ходе разработки занятия были учтены типы восприятия обучающихся: аудиал – материал произносился вслух, визуал – компьютерная презентация, кинестет – самостоятельная проработка занятий.

Данное практическое задание является завершающим уроком по изучению параметров безопасности в ОС Windows.

Урок был составлен при использовании инструментария конкурса «Профессионалы». Такая технология проведения урока должна подвести к самому главному - к сдаче демонстрационного экзамена. При таком подходе обучающиеся учатся работать с определенными требованиями к заданию – это наши критерии. Понимают какое задание в какое время им нужно выполнить, и что именно это задание должно быть выполнено. Отрабатывается умение работать с текстом, а главным образом умение правильно читать и выделять главные мысли.

Занятие было начато с приветствия, отмечены отсутствующие.

При помощи программы GoogleForms была осуществлена проверка знаний. Для этого был разработан тест из 12 вопросов. С его помощи студенты вспомнили необходимую информацию для выполнения практической работы.

В ходе выполнения заданий обучающиеся были вовлечены в активный познавательный творческий процесс. Они погружены в процесс выполнения творческого задания, а вместе с ним и в процесс закрепления старых знаний по дисциплине, в рамках которой и проводился урок.

На данном этапе занятия обучающиеся представляли свои проекты, делились идеями. Аудитория оценивала вносила свои корректировки, комментировали удачные и не очень удачные моменты в работах. Подводя

итоги, студенты задумывались над тем, насколько важно рационально распределять рабочее время. Определяли, где в будущей профессии пригодятся полученные практические навыки.

На протяжении всего занятия была здоровая атмосфера, благоприятный климат, способствующий обучению и учению. Предложенные задания способствовали развитию навыков самоконтроля, учили самостоятельно принимать решения.

Каждый этап логически завершен, подведен итог и настроен на восприятие следующего этапа.

Оценку за работу ребята выставляли после всех изложенных комментариев в оценочные листы. В целом, у ребят положительные эмоции от занятия.

Ребятам было сообщено домашнее задание.

Подводя итог данного занятия, хочется отметить, что план занятия в полной мере был реализован, поставленные цели перед

Тип Урока - применение и совершенствование знаний.

Использование информационных технологий формы организации занятия дало ряд преимуществ перед стандартной системой обучения:

1. Повышение интереса студентов.

3. Повышение творческой активности.

4. Облегчение обработки и контроля знаний и т.д.

Проведенный урок способствовал формированию общих и профессиональных компетенций:

ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 4 Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9 Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием

## **Правила создания и хранения паролей**

### **1. Пароль должен быть сложным!**

1. **Хороший пароль** должен содержать **минимум 10 символов**, чтобы его было сложно взломать

2. **Надёжный пароль** должен содержать **12 символов и более**

3. **Сложный пароль** должен содержать **три набора символов**: **БОЛЬШИЕ** и **маленькие** буквы, **цифры**, **специальные символы** [**PochtiSlozhniyParol123%!**]

4. Пароль должен быть **без общедоступной информации** (имя, фамилия, ник, важные даты, номера телефонов, ИНН, адреса, как свои, так и родственников — это НЕ для пароля! [**MarinaAV1965** – плохой вариант])

5. Пароль должен быть **без словарных слов** и без простых сочетаний слов (используйте малораспространённые слова или вообще несуществующие слова [**Абырвалг**])

### **2. Для разных сайтов — разные пароли**

Возможно, вы скажете: «Зачем мне столько паролей?» Давайте посмотрим, зачем это нужно.

- **Самое важное в Интернете — это ваш e-mail**, так как почти все сервисы в Интернете привязаны к вашей электронной почте. Если кто-то получит доступ к вашей электронной почте, то сможет получить доступ ко всему остальному.

- **На малонадёжных сайтах e-mail и пароль лежат рядом!** Если такой сайт взломают, первое что сделают — проверят, подходит ли пароль к вашей электронной почте, затем попробуют получить доступ к аккаунту в социальной сети и средствам онлайн-оплаты.

- Злоумышленники продают друг другу **базы взломанных аккаунтов**, поэтому риск взлома всех ваших аккаунтов резко возрастает.

Как же быть?

Есть простой способ упростить задачу, разделив все сервисы на две группы:

1. Для обычных аккаунтов использовать более простые, похожие пароли;

2. Для важных аккаунтов (e-mail, интернет-банкинг) использовать сложные, уникальные пароли.

### **3. Храните пароль надёжно**

Память инструмент не самый надёжный, поэтому лучше использовать один из нескольких проверенных способов надёжного хранения паролей.

1. **Бумажный блокнот** — да, даже ведущие специалисты по информационной безопасности признают этот вариант. Вот только храните такой блокнот подальше от любопытных глаз, да и пароли в нём храните в непонятном виде (об этом мы поговорим в следующий раз).

2. **Менеджер паролей** — специальная программа, которая помнит пароли за вас, вам лишь нужно помнить один пароль для доступа к остальной базе.

3. **Текстовый документ** — не самый удачный вариант хранения паролей, но его тоже можно использовать, если вы сможете хранить документ безопасно: в архиве под паролем, но это уже вариант менеджера паролей

#### **Как НЕЛЬЗЯ хранить пароли**

1. На бумажке, прикрепленной к монитору или лежащей на столе под клавиатурой (есть прецеденты государственных масштабов)

2. В текстовом документе на рабочем столе (или на флешке, карте памяти телефона и т.д.)

3. В браузере тоже не рекомендуется хранить пароли! (Интересно, почему? Отвечу в комментариях)

#### **4. Проверьте параметры восстановления пароля**

Вашу почту могут попытаться взломать, попытавшись восстановить пароль.

Если у вас для восстановления доступа используется ответ на секретный вопрос, его можно угадать.

- **Ответ на секретный вопрос должен быть стойким к угадыванию** (используйте неожиданные ответы, например: «Ваш любимый цвет» — «Небо»)

Если же для восстановления используется второй e-mail, все правила из этой статьи тоже должны относиться к нему.

- **E-mail для восстановления должен быть надёжно защищён** (проверьте параметры безопасности сейчас, не откладывая)

#### **5. Используйте двухфакторную аутентификацию**

Для важных аккаунтов используйте двухэтапную или двухфакторную [аутентификацию](#).

Например, вы вводите пароль, а с помощью телефона получаете **дополнительный одноразовый код** для доступа к онлайн-сервису (это может быть SMS или сгенерированный в приложении код).

В этом случае взломать ваш аккаунт будет значительно сложнее.

6. Используется **12 символов**, что уже очень хорошо;

7. Используется **три набора символов**: маленькие буквы, большая буква «А», цифра «6» вместо буквы «б», специальные символы «@» и «-»;

8. Мы **не использовали общедоступную информацию** (ни имя, ни дату рождения, ни номер телефона);

9. Пароль **не содержит словарных слов**, значит его невозможно подобрать по словарю;

10. Для разных сайтов используются **разные пароли**.