

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №8**

**ПО ДИСЦИПЛИНЕ «МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В КМПЬЮТЕРНЫХ СИСТЕМАХ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

**1 Опишите параметры локальной политики безопасности операционной системы (по выбору): – кто имеет доступ к компьютеру; – какие ресурсы могут использовать пользователи на компьютере; – включение и выключение записи действий пользователей или группы пользователей в журнале событий.**

-Кто имеет доступ к компьютеру;

Согласно политике управления доступом ([https://learn.microsoft.com/ru-ru/windows/security/identity-protection/access-control/access-control](https://vk.com/away.php?to=https%3A%2F%2Flearn.microsoft.com%2Fru-ru%2Fwindows%2Fsecurity%2Fidentity-protection%2Faccess-control%2Faccess-control&utf=1)) субъектами безопасности в windows 10 являются:

1. Локальные учетные записи
2. Учетные записи Active Directory
3. Учётные записи Microsoft
4. Учетные записи службы
5. Группы безопасности Active Directory

**2 Опишите параметры и значения параметров Политики паролей. Заполните таблицу**

|  |  |  |
| --- | --- | --- |
| Название | Описание | Значение |
| Требовать повторяемости паролей | Значение определяет ведется ли запись журнала паролей | 0-24 |
| Максимальный срок действия пароля | Определяет максимальный срок действия пароля | 1-999 |
| Минимальный срок действия пароля | Определяет минимальный срок действия пароля | 0-998 |
| Минимальная длинна пароля | Определяет минимальную длину пароля. В зависимости от значения параметра «Ослабить ограничения минимальной длинны пароля» принимает разные значения | 0-14/128 |
| Пароль должен отвечать требованиям сложности | Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям.  Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков  Иметь длину не менее 6 знаков  Содержать знаки трех из четырех перечисленных ниже категорий:  Латинские заглавные буквы (от A до Z)  Латинские строчные буквы (от a до z)  Цифры (от 0 до 9)  Отличающиеся от букв и цифр знаки (например, !, $, #, %) | Включен-Отключен |
| Хранить пароли всех пользователей в домене используя обратное шифрование | Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности. Хранение паролей с помощью обратимого шифрования - по существу то же самое, что и хранение паролей открытым текстом. По этой причине данная политика не должна применяться, пока требования приложения не станут более весомыми, чем требования по защите паролей. | Включен-Отключен |

**3 Опишите параметры и значения параметров Политики учетной записи. Заполните таблицу.**

|  |  |  |
| --- | --- | --- |
| Название | Описание | Значение |
| Пороговое значение блокировки | Параметр определяет максимальное кол-во неправильных попыток ввода пароля | 0-999 |
| Блокировка учетной записи на | Параметр определяет кол-во минут, которое должно пройти для снятия блокировки учётной записи | 0-99999 |
| Сброс счетчика блокировки через | Этот параметр безопасности определяет количество минут, которые должны пройти после неудачной попытки входа в систему до того, как счетчик неудачных попыток входа будет сброшен до 0. | 1-99999 |

**4 Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания.**

Для изменения значений политики паролей, необходимо войти в редактор групповой политики (win+r -> gpedit.msc), перейти по пути «Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности» -> «Политика учетных записей» -> «Политика паролей»

Изменение происходит путем двойного нажатия ЛКМ на необходимый параметр, и в открывшемся диалоговом окне выставляется необходимое значение параметра.

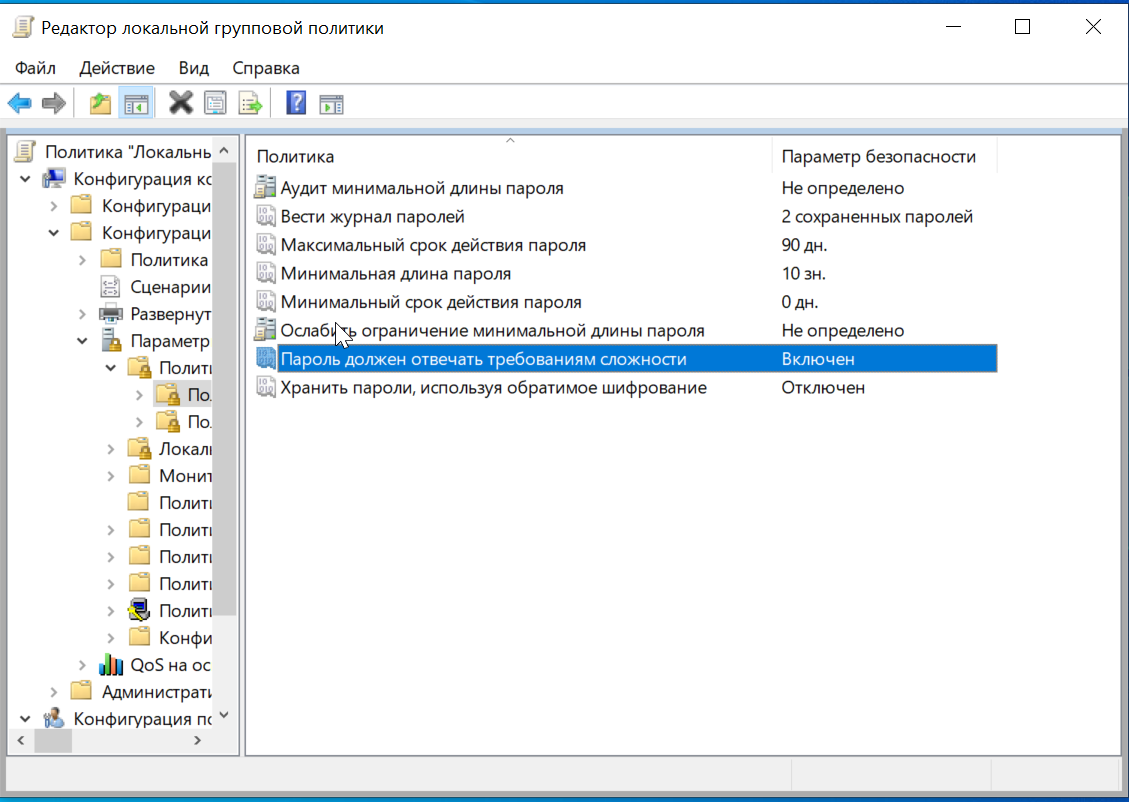
****

Рисунок 1- Изменение политик паролей

Изменение пароля происходит путем перехода в «Параметры» -> «Учетные записи» -> «Варианты входа» -> «Пароль» -> «Изменить».

В открывшемся диалоговом окне необходимо ввести действующий пароль (в случае если пароля не было шаг будет пропущен автоматически). В следующем окне необходимо ввести новый пароль, подтверждение пароля и подсказку для пароля (все поля обязательные). В данном случае вводится пароль из 10 нулей для демонстрации работы политики безопасности «Пароль должен отвечать требованиям сложности»

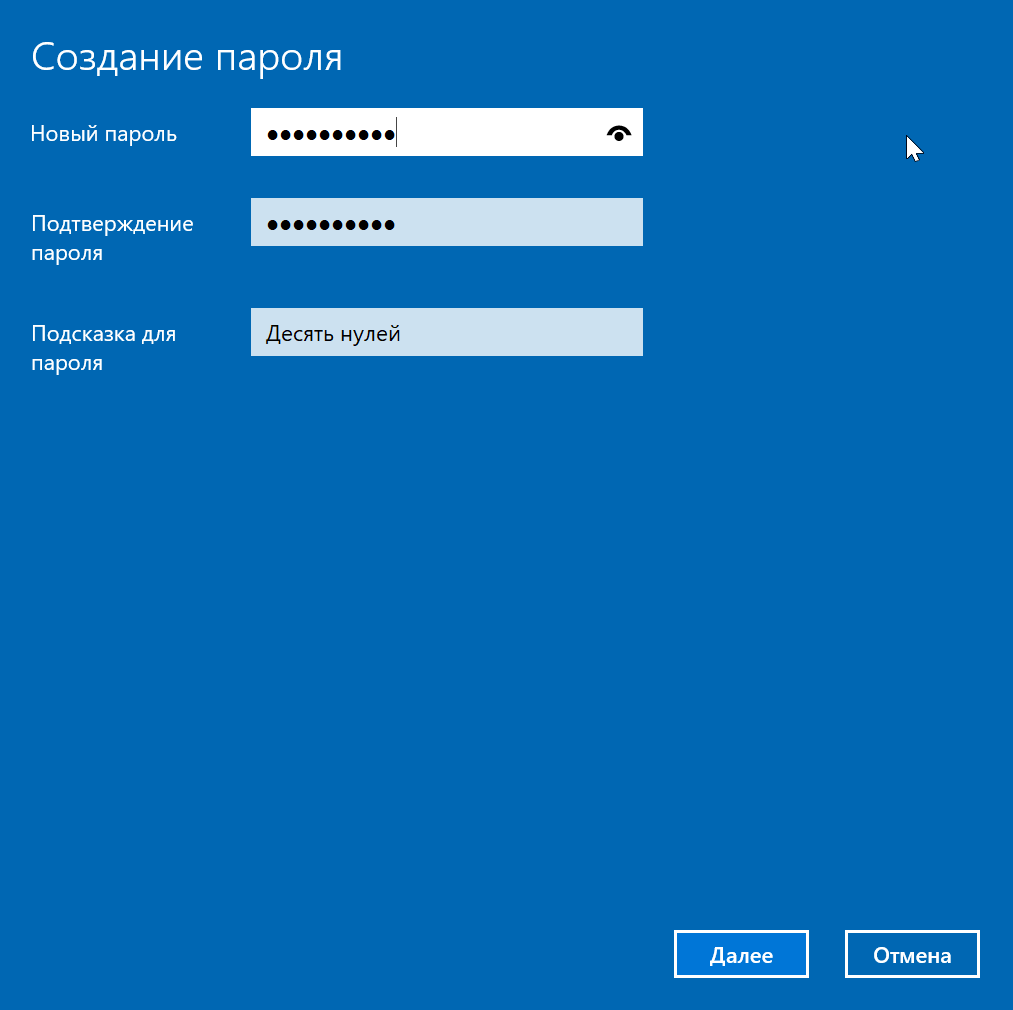
****

Рисунок 2 - Создание простого пароля

При нажатии на кнопку «Далее» происходит переход в окно подтверждения действий. В нашем случае пароль требованиям безопасности не соответствует, поэтому система выдает ошибку и требует другой пароль.

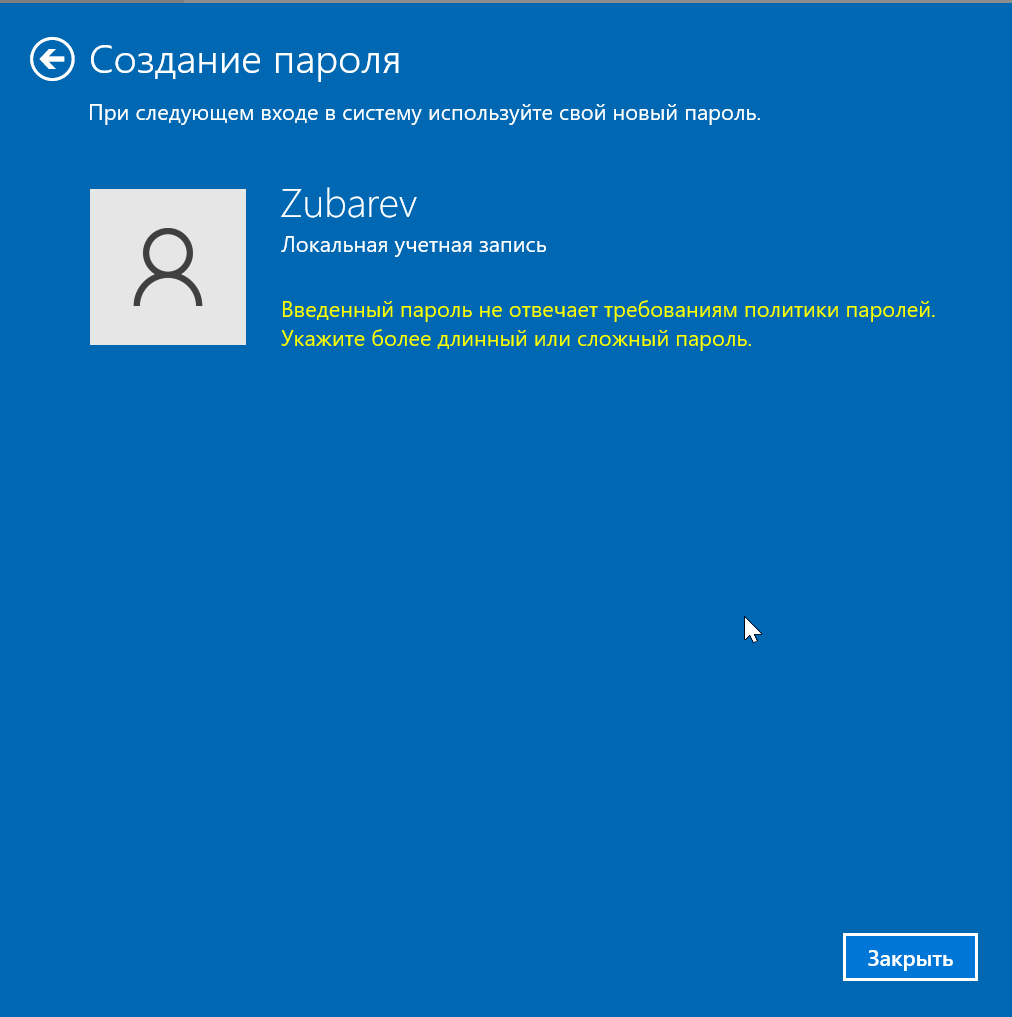


Рисунок 3 - Работа политики безопасности

Вернувшись на страницу ввода пароля вводим пароль который отвечает требованиям политики паролей (от 10 знаков, строчные и прописные буквы, спец. символы)

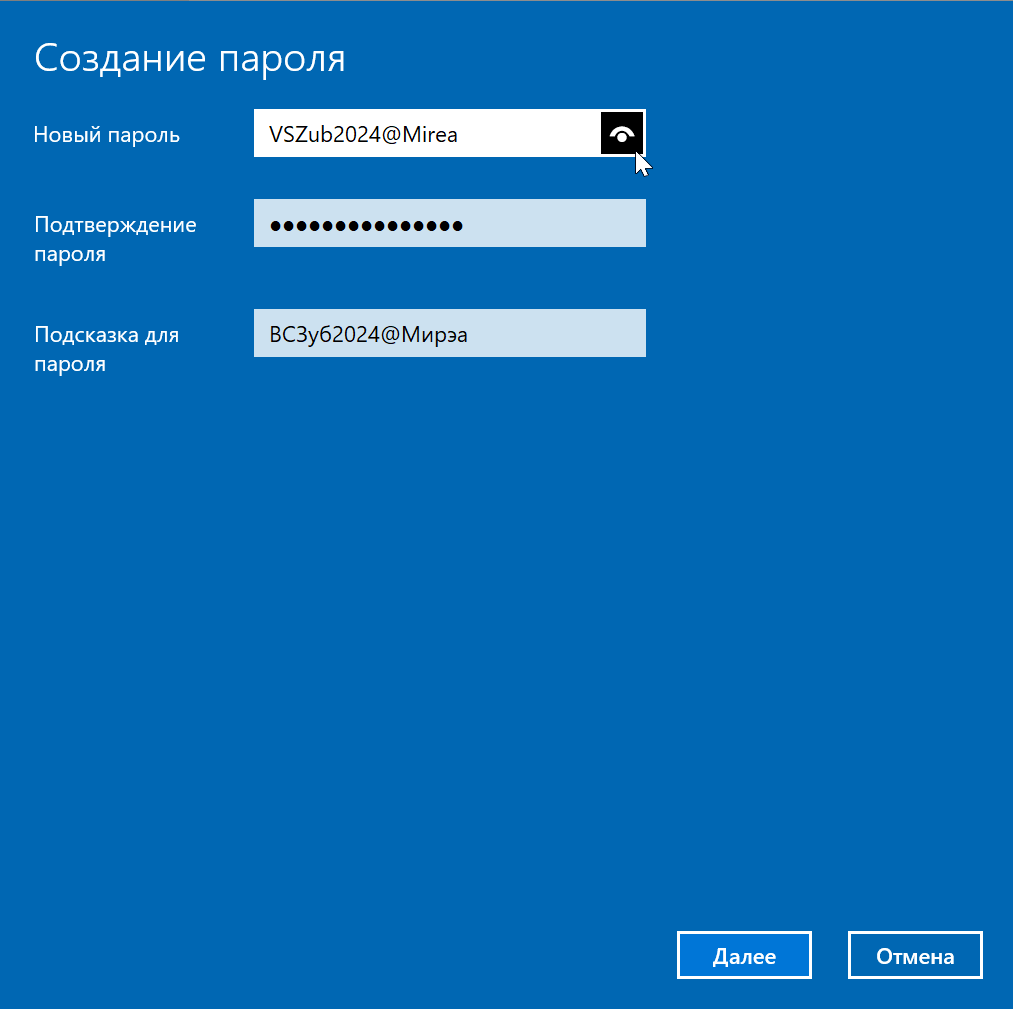
****

Рисунок 4 - Создание сложного пароля

**5 После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.**

Для изменения пароля необходимо проделать те-же действия, как и для его создания. В данном случае новый пароль будет копией старого, то есть будет отвечать требованиям сложности и проверять работу аудита журнала паролей.

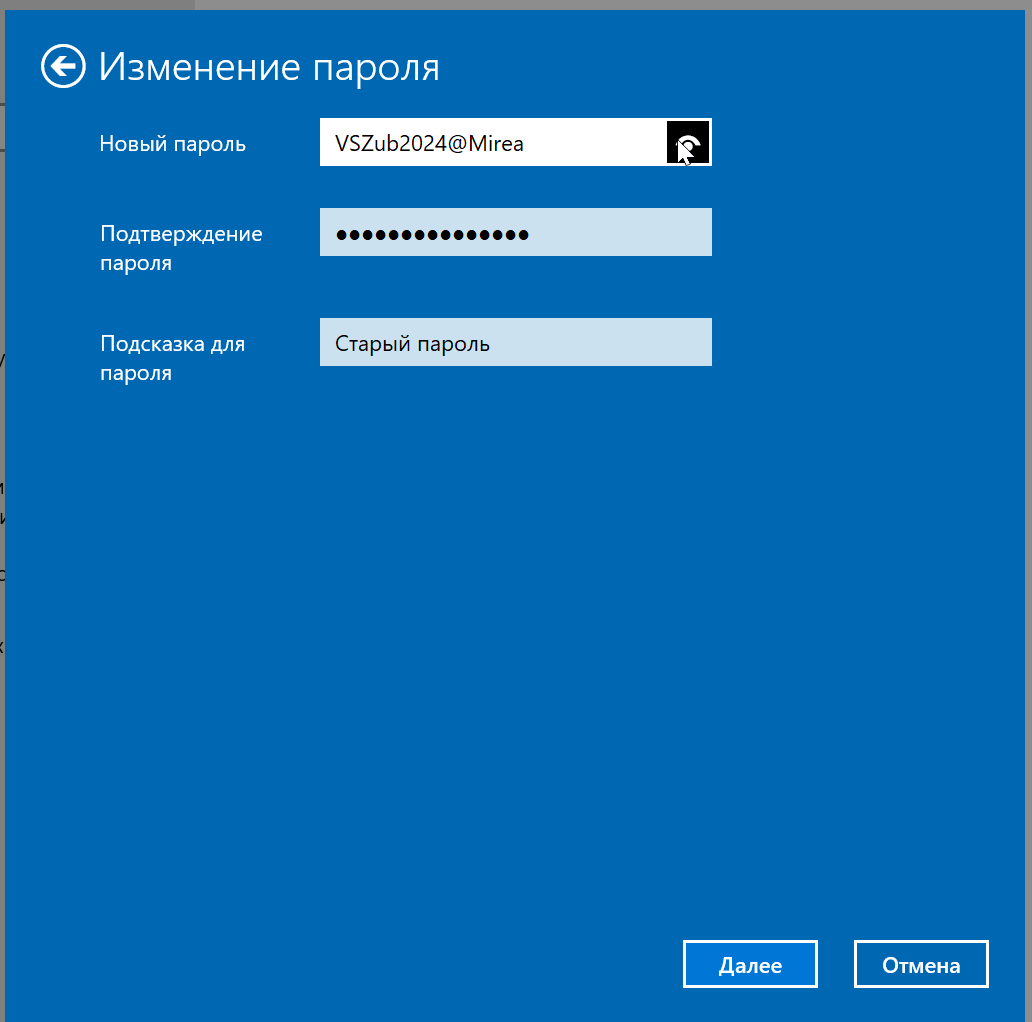


Рисунок 5 - Попытка изменения пароля

После попытки изменения пароля, система не позволила пользователю завершить изменение, так как ведённый пароль сохранен в журнале аудита паролей.

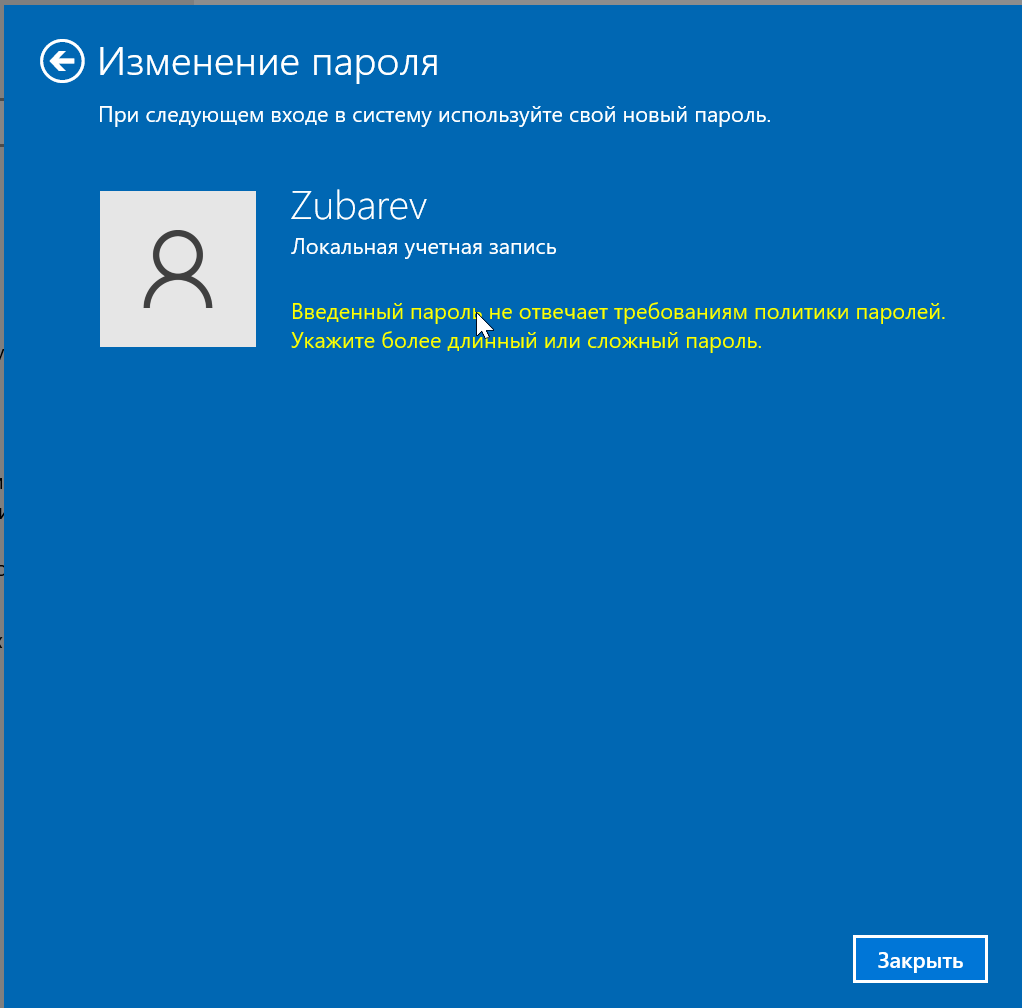


Рисунок 6 - Работа журнала аудита паролей

Система безопасности не дает возможности изменить ввести тот-же пароль (даже при соответствовании требованиям сложности), так как в политике паролей ведется журнал паролей (из 2-х записей). Эта политика препятствует использованию паролей, которые уже были использованы.

**6 Проведите эксперименты с другими параметрами Политики учетных записей.**

Изменение политики учетных записей происходит через Редактор локальной групповой политики

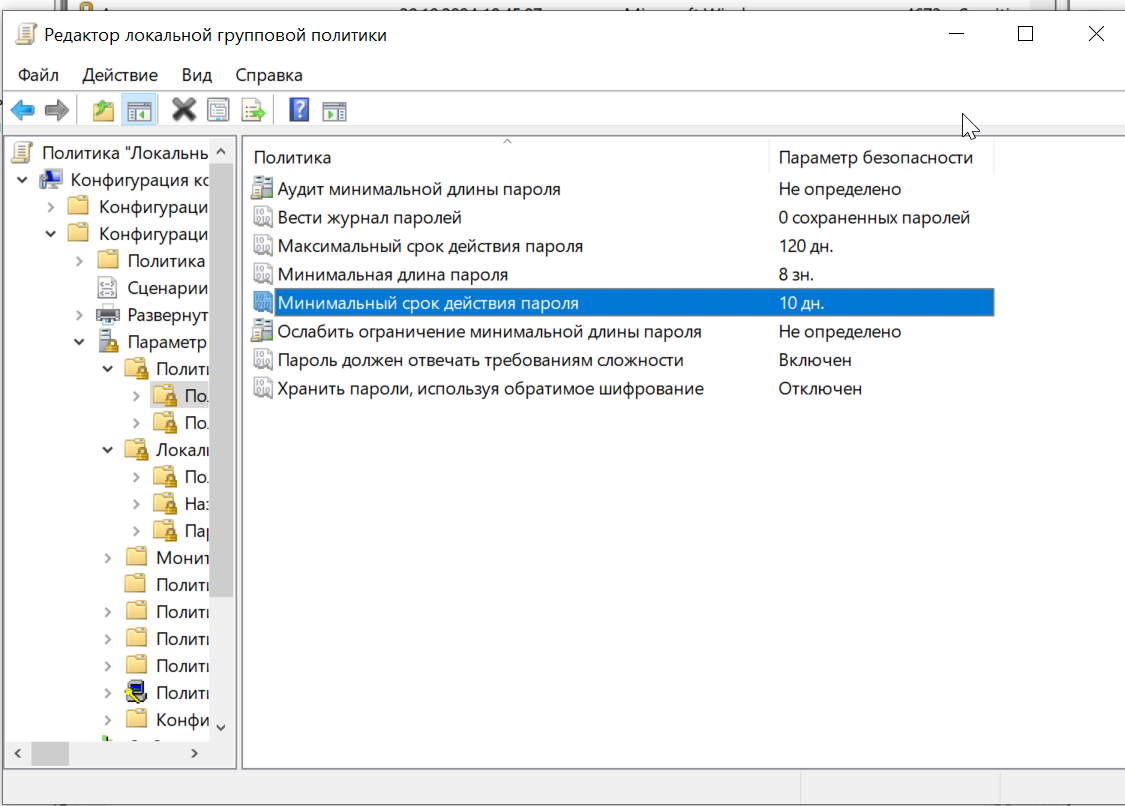
****

Рисунок 7 - Изменение политик паролей

«Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности» -> «Локальные политики» -> «Политика аудита»

Изменение происходит путем двойного нажатия ЛКМ на необходимый параметр, и в открывшемся диалоговом окне выставляется необходимое значение параметра.

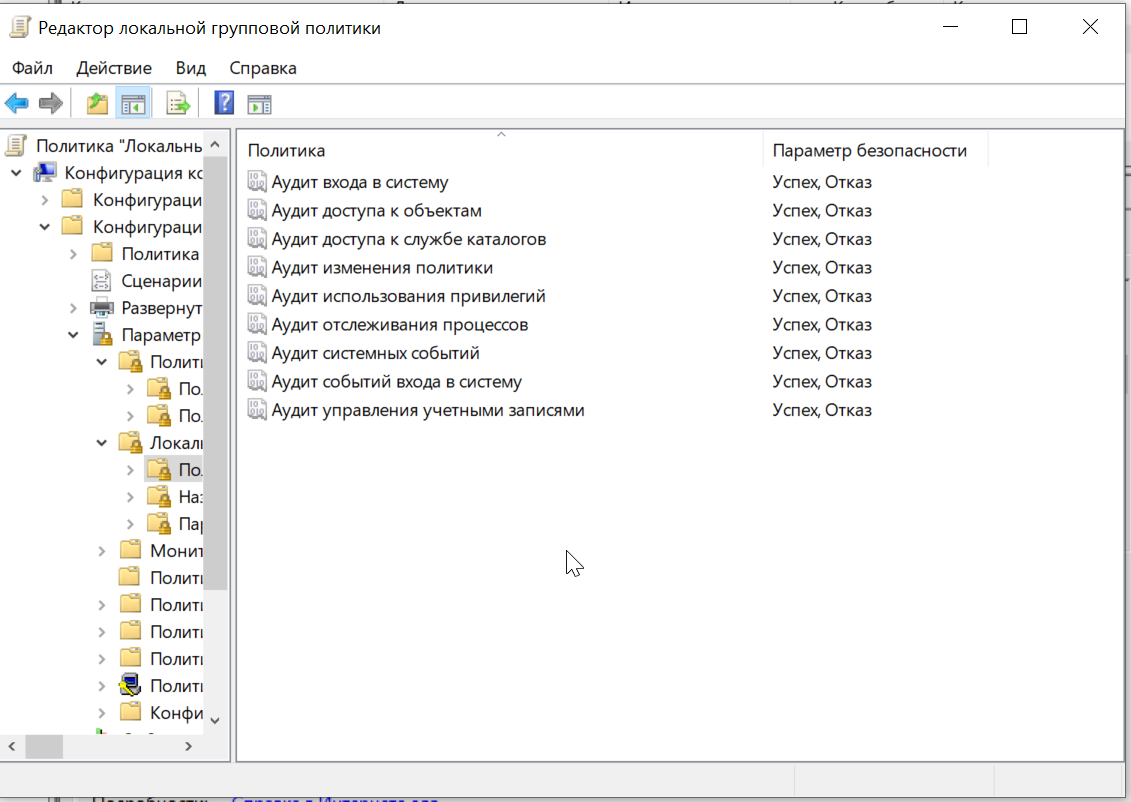
****

Рисунок 8 – Настройки политики аудита

**7 Приведите подтверждение выполненных действий с помощью журнала аудита (событий).**

Так как был выключен параметр «Аудит входа в систему», было произведено две попытки входа в систему (удачная и неудачная). Для просмотра журнала аудита надо (win+r -> eventwmr.msc), перейти по пути «Журналы Windows» -> «Безопасность». Так как целью было выявить работу аудита входа в систему, были применены фильтры для отсеивания других записей в журнале аудита. Коды успешного (4624) и неуспешного (4625) входа были прописаны в параметр фильтра. П

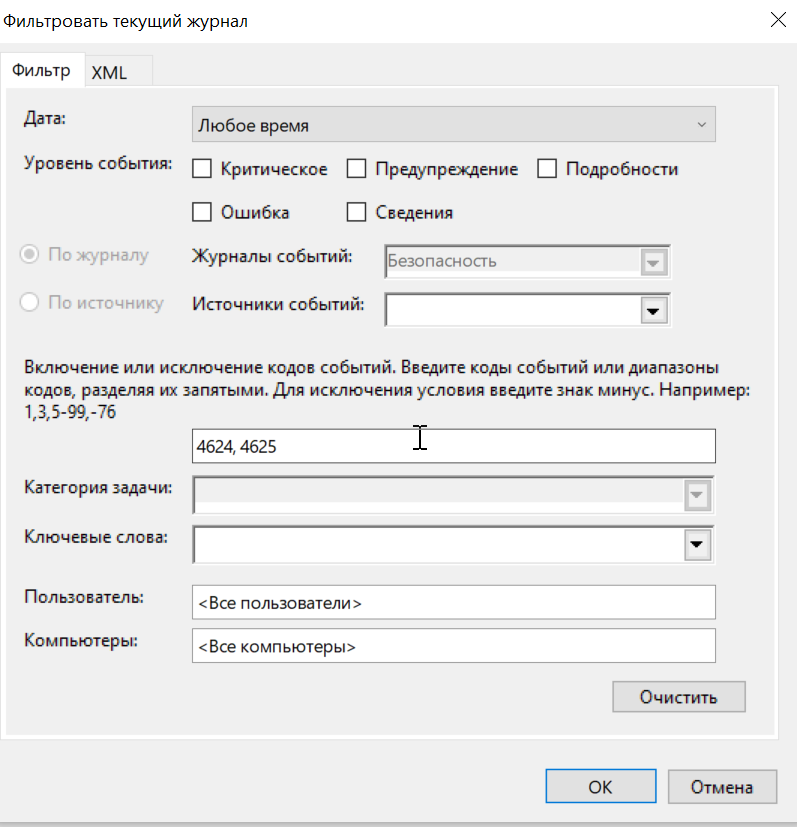


Рисунок 9 – Фильтр записей журнала аудита

После фильтровки записей была получена таблица успешных и неуспешных входов в систему. И предоставлены два случая аудита успеха и аудита отказа.

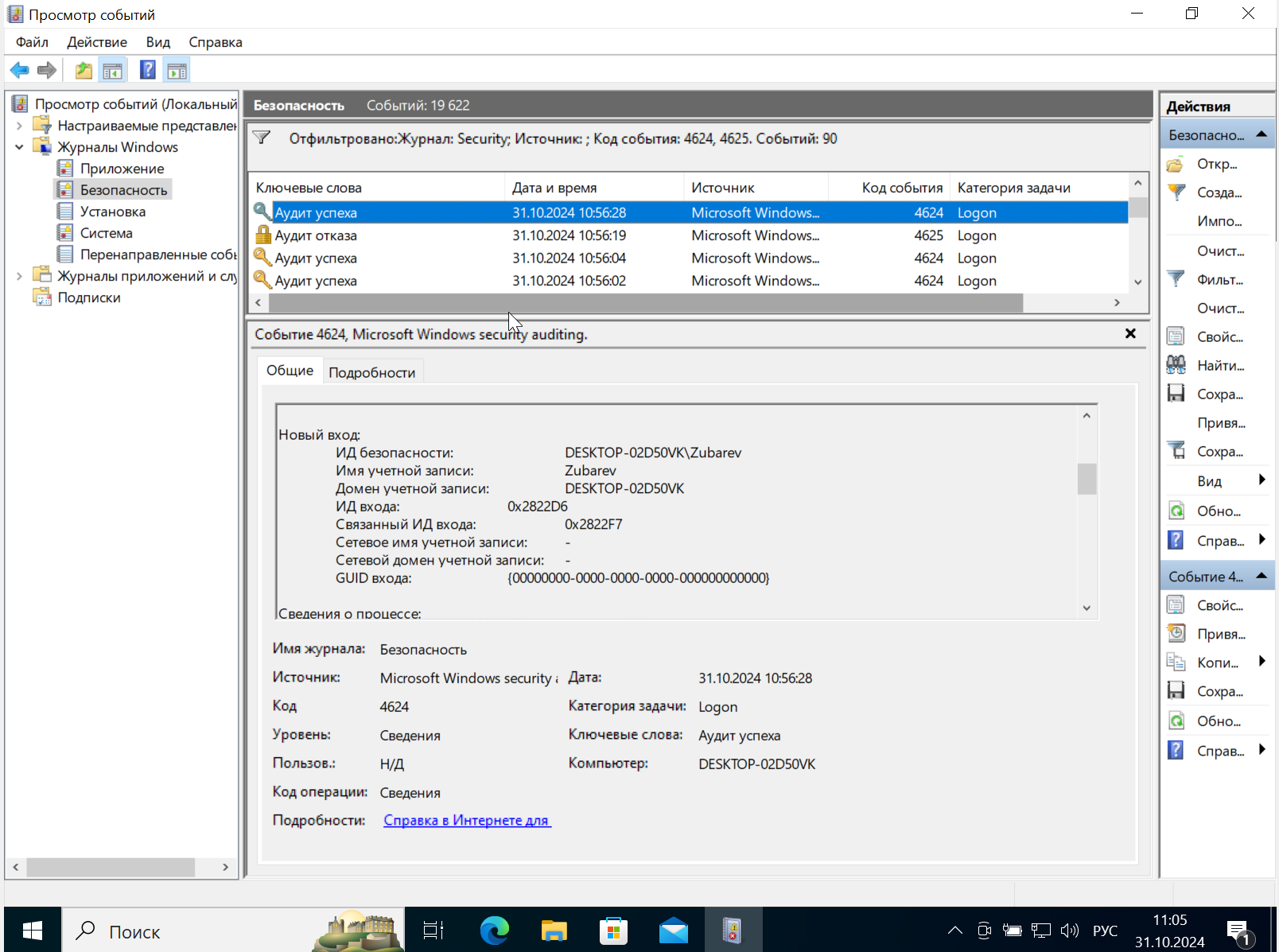
****

Рисунок 10 - Вход в систему (аудит успеха)

Во втором случае был несколько раз (7) введен неправильный пароль. После чего действие учетной записи было заблокировано, о чем свидетельствует код ошибки 0xC0000234 в записи журнала аудита.

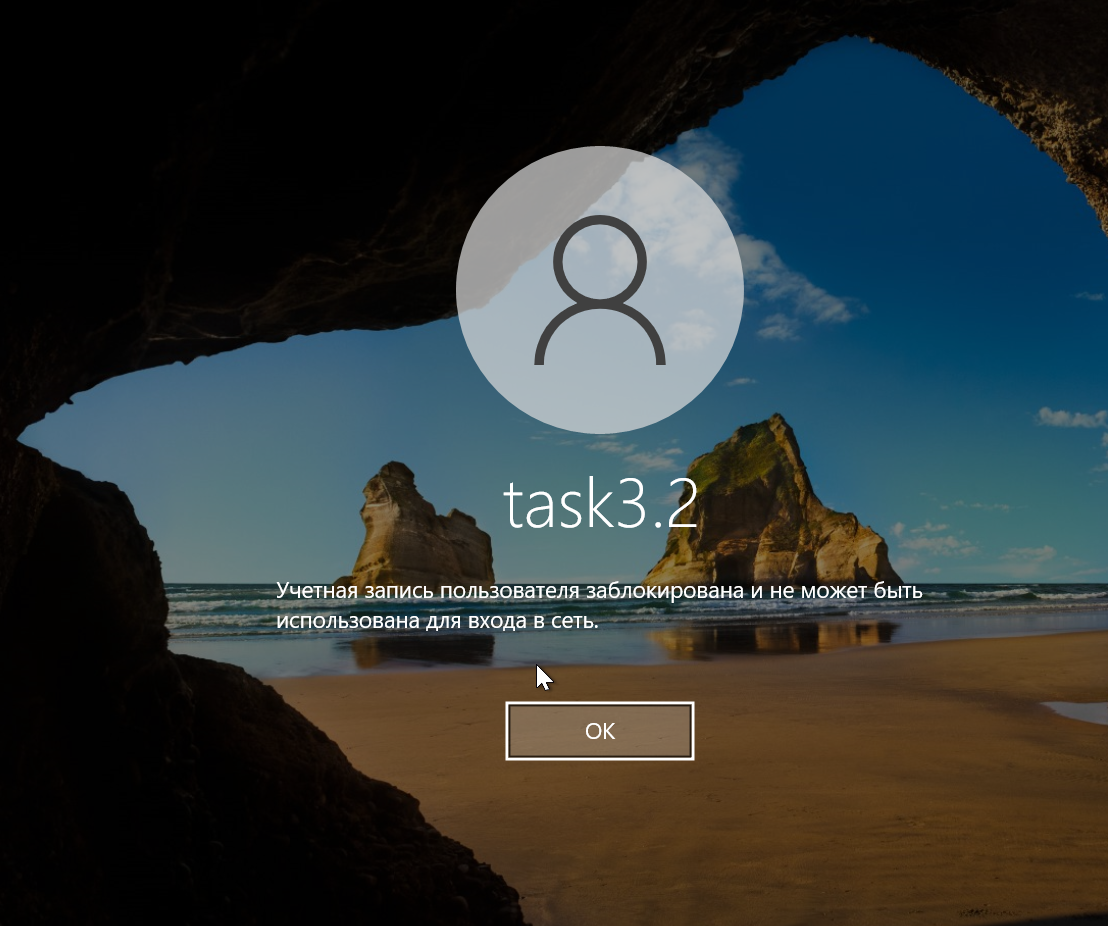


Рисунок 11 – Заблокированная действия учетной запись

Журнал аудита сформировал запись (аудит отказа) на действие учетной записи (вход в систему). Так как действие учетной записи было заблокировано в журнале аудита отобразилось сообщение об ошибке код (0xC0000234)

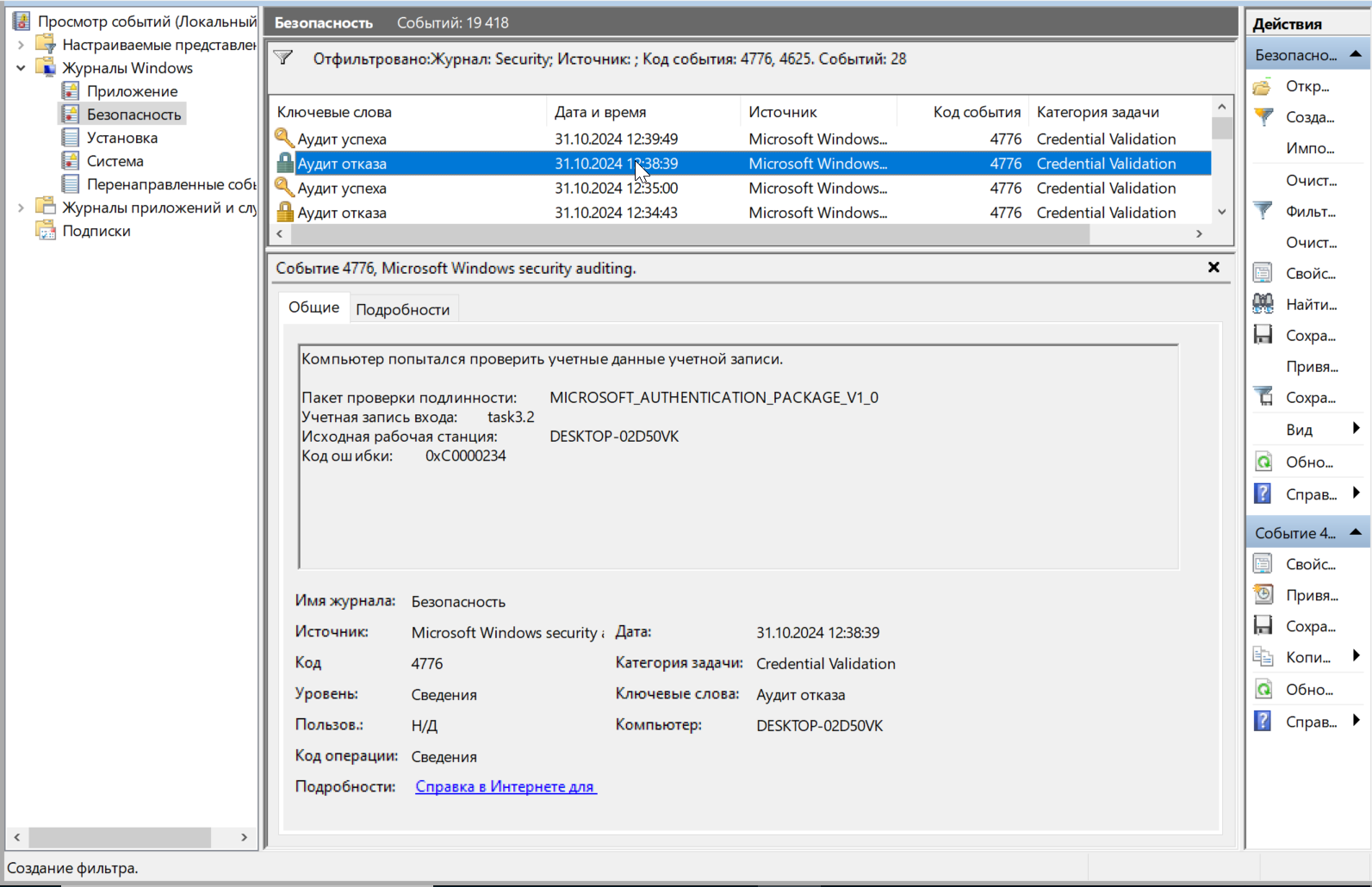


Рисунок 12 – Не успешный вход в систему (аудит отказа)