МИНИСТЕРСТВО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ И ЗАНЯТОСТИ НАСЕЛЕНИЯ ПРИМОРСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«НАХОДКИНСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

СОГЛАСОВАНО	УТВЕРЖДАЮ
Заместитель директора по СВР	И.о. директора КГБ ПОУ «НГГПК»
_____С.В. Янгуразова	_____Е.Ю. Войстрик
«03» 06 2022	«03» 06 2022

ПОЛОЖЕНИЕ
О программе профессиональной пробы «Специалист по информационной безопасности»

Общие положения

1.1 Настоящее Положение определяет условия, порядок, организацию и проведение программы профессиональной пробы «Специалист по информационной безопасности» (далее – проба).
1.2 Организатором пробы является КГБ ПОУ «НГГПК».
1.3 Информационную поддержку пробы осуществляет КГБ ПОУ «НГГПК».
1.4 Срок проведения пробы – 19 июля 2022 года.
1.5 Участники пробы – русскоговорящие обучающиеся СПО очной формы обучения, учащиеся 6-11 классов.

II. Цель и задачи

2.1 Цель пробы – поддержка и развитие студенческих и ученических инициатив.
2.2 Задачи пробы:
- Ознакомить с профессией "Специалист информационной безопасности";

- Обучить учащихся выполнять базовые настройки системы, связанные с администрированием и разграничением доступа;
- Активизация и содействие инициативной социально-значимой деятельности студентов и учеников в пространстве своего города, страны;
- Поддержка русского языка в дружественных странах.

III. Организация

Организацию и проведение пробы осуществляет преподаватель аккредитованный как главный эксперт компетенции " Корпоративная защита от внутренних угроз информационной безопасности" по стандартам Ворлдскиллс (далее – преподаватель).

IV. Проведение пробы

4.1 Проба будет проводиться 19 июля в 17:00 по местному времени.
4.2 Перед началом мероприятия, на указанные электронные адреса (указанные в заявке на участие в графе "обратная связь") будут разосланы номера рабочих мест и пароли для подключения к ПК через программу AnyDesk:
4.3 Общие сведения находятся в приложении 1
4.4 Форма для подачи заявки размещена в приложении 2
4.5 План программы размещен в приложении 3

V. Материальное обеспечение

5.1 Организационный взнос не предусмотрен.

VI. Порядок внесений изменений в Положение

6.1 Изменения и дополнения в настоящее Положение вносятся Приказом директора КГБ ПОУ «НГГПК».

Приложение 1

Программа профессиональной пробы «Специалист по информационной безопасности»:

Предлагаем вам поучаствовать в пробе по программе «Специалист по информационной безопасности», которая будет **проводиться в дистанционном** формате, 19 июля в 17:00 (по местному времени). Для участия в программе необходимо заполнить форму заявки (Приложение 2) и отправить ее на электронный адрес **nggpk@yandex.ru** с темой **"Проба по ИБ".**

Уровень сложности	Формат проведения	Время проведения	Возрастная категория	Доступность для участников с ОВЗ
Базовый	online	90 минут	6-11 класс СПО	-

Требования к рабочему месту:

Наименование	**Рекомендуемые технические характеристики с необходимыми примечаниями**	**Количество**	**На группу/ на 1 чел.**
Персональный компьютер	- базовая тактовая частота не менее 2 ГГц - количество физических ядер не менее 2 - количество потоков не менее 4 ОЗУ: - объем не менее 4 Гб ПЗУ: - HDD объем не менее 500 Гб	1	1 человек
Периферия	USB совместимая мышь и клавиатура	1	
Программное обеспечение	Наличие программного обеспечения anydesk для удаленного подключения к рабочему месту	1	
Интернет	Наличие стабильного интернет-соединения скоростью от 1 мбит/с для трансляции изображения и подключения к удаленным рабочим местам	1	

Приложение 2

Форма заявки для участия

Заявка на участие

№	Ф.И.О. (полностью)
Ф.И.О. (полностью)	
Дата рождения	
Курс (класс)	
Специальность (если есть)	
Наименование образовательного учреждения	
Обратная связь (для предоставления доступа к рабочему месту)	
Примечание (если необходимо)	

Приложение 3

I. Содержание программы «Специалист по информационной безопасности»

Введение (25 мин)

1. Краткое описание профессионального направления «Специалист по информационной безопасности»:

Безопасность передачи данных в современном обществе – одна из самых больших проблем, как для простого пользователя, так и для организаций. Эффективность любой информационной системы в значительной мере определяется состоянием защищенности (безопасностью) перерабатываемой в ней информации. Безопасность информации – состояние защищенности информации при ее получении, обработке, хранении, передаче и использовании от различного вида угроз.

Для успешного противодействия угрозам и атакам информационных систем, необходимо провести анализ безопасности и рисков от возможного несанкционированного доступа и на основе данного анализа строить защиту информационной структуры.

Анализ угроз информационной безопасности позволяет выделить составляющие современных компьютерных угроз – их источники и движущие силы, способы и последствия реализации. Анализ исключительно важен для получения всей необходимой информации об информационных угрозах, определения потенциальной величины ущерба, как материальной, так и нематериальной, и выработки адекватных мер противодействия.

2. Место и перспективы профессионального направления «Специалист по информационной безопасности»:

В связи с повсеместной информатизацией всех рабочих процессов во многих сферах, рано или поздно, предприятиям придется задуматься о том, как соответствовать современным нормам обработки, хранения и передачи персональных согласно существующему законодательству или же для обеспечения сохранности и конфиденциальности своих данных, в результате чего - спрос на специалистов данной направленности только расти.

Необходимые навыки и знания для овладения профессией:

- Аналитический склад ума.
- Умение видеть и решать проблему.
- Терпеливость.
- Постоянное саморазвитие.
- Обучаемость.
- Внимательность к деталям.
- Обладать базовыми навыками работы с ПК.
- Иметь понимание принципа работы ПК и ПО.

3. Связь профессиональной пробы с реальной деятельностью:

В данной пробе, обещающийся, получит представление о базовых механизмах, используемых в деятельности профессионального направления «Специалист по информационной безопасности».

Приводим информации о вакансиях данной специальности на бирже труда, графики ежегодно сравнения зарплат в данной сфере, а также проводим краткий дискус на тему важности безопасности при работе с информацией.

Постановка задачи (5 мин)

Постановка цели и задачи в рамках пробы:

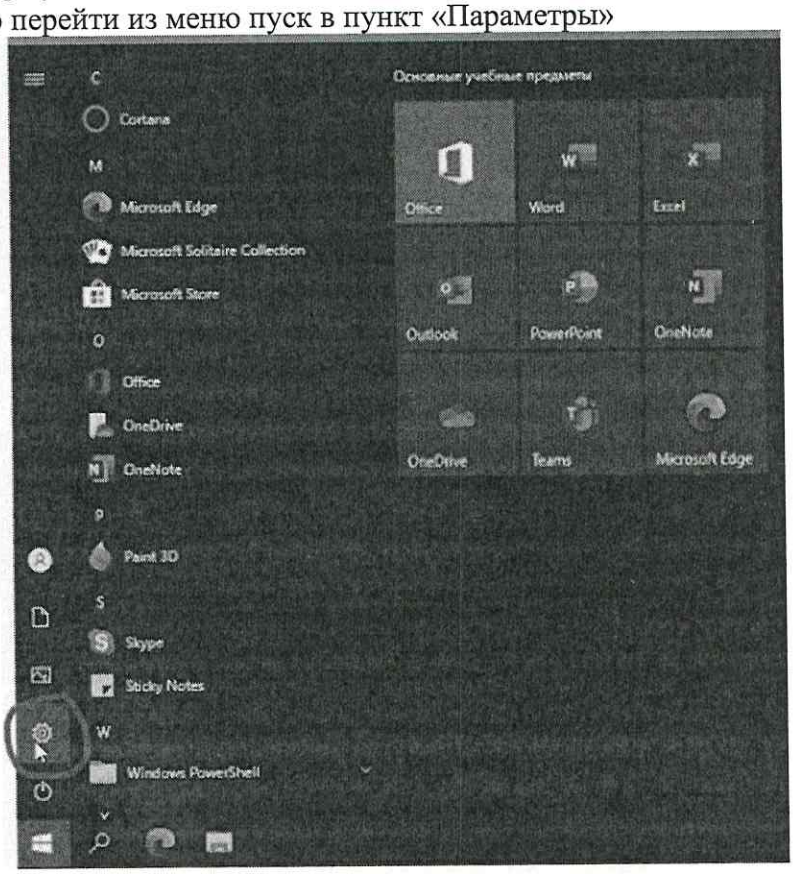
В данной пробе мы ознакомимся с самыми базовыми механизмами, доступными каждому человеку, для обеспечения первичной защиты информации от 3их лиц.

Выполнение задания (20 мин) – Основной модуль

Подробная инструкция по выполнению задания:

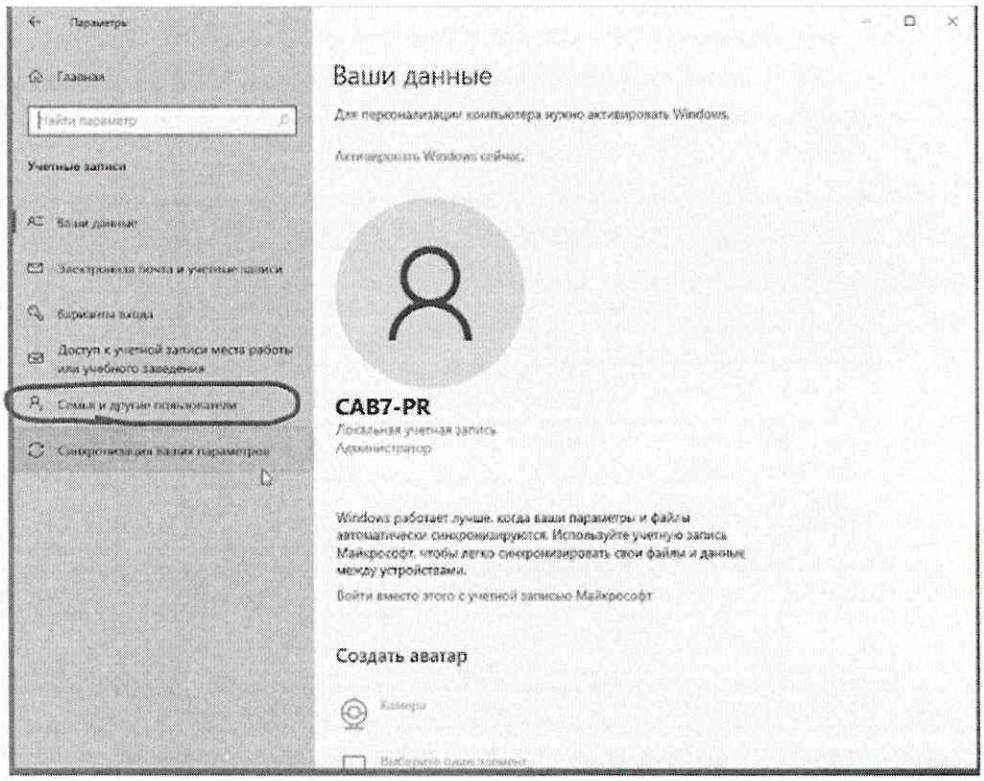
1. Создание учетной записи администратора с паролем и убрать права администратора у пользователя User:

- Необходимо перейти из меню пуск в пункт «Параметры»

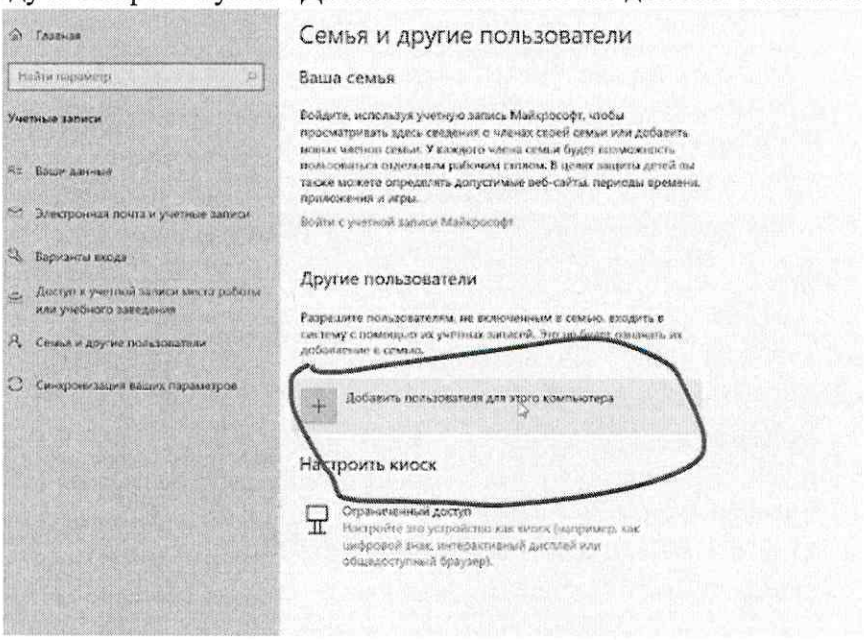


- Выбрать раздел «Учетные записи»

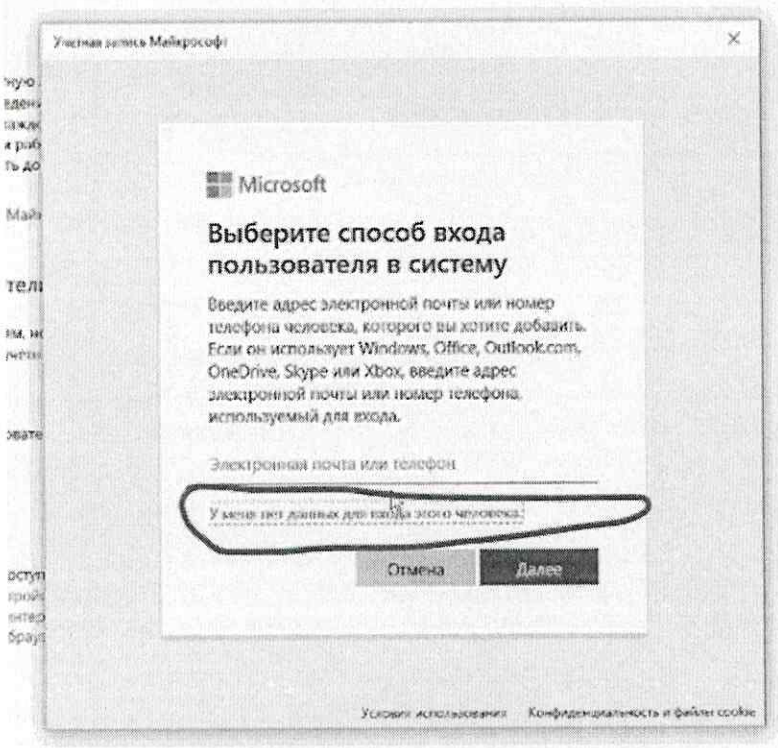
- В разделе учетные записи выбрать пункт «Семья и другие пользователи»

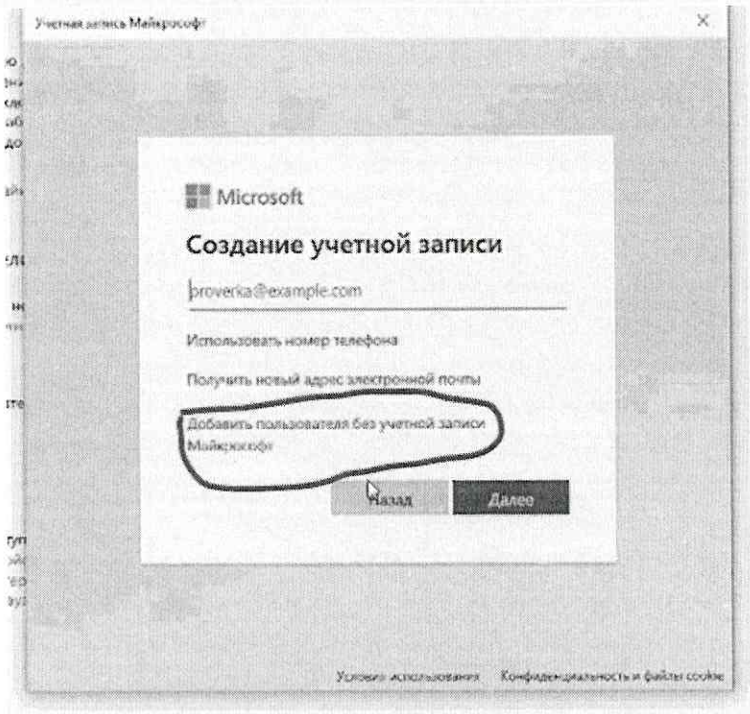


- Далее следует выбрать пункт «Добавить пользователя для этого компьютера»

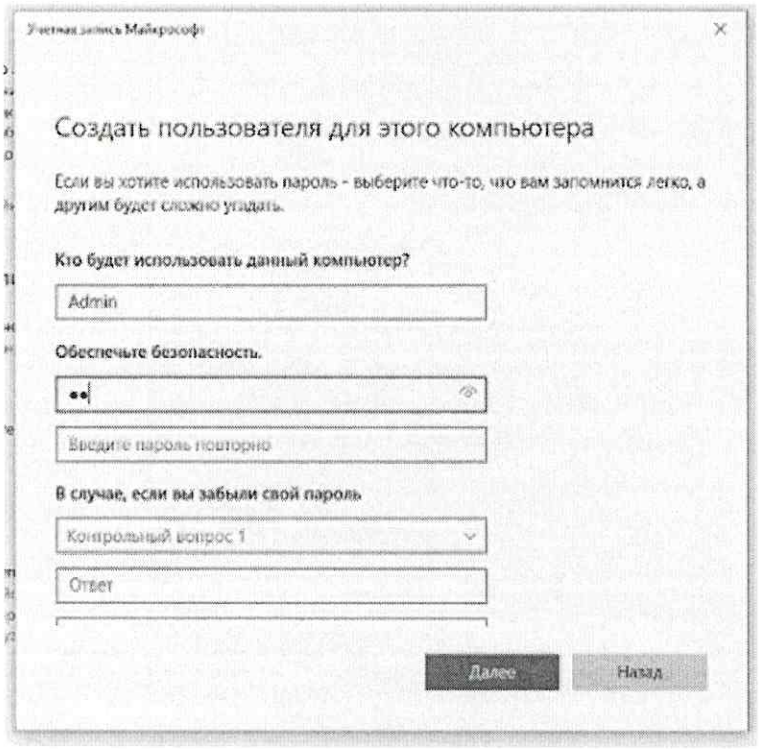


- Следом выбрать пункты «Уменя нет данных…» и «Добавить пользователя без учетной записи Майкрософт».

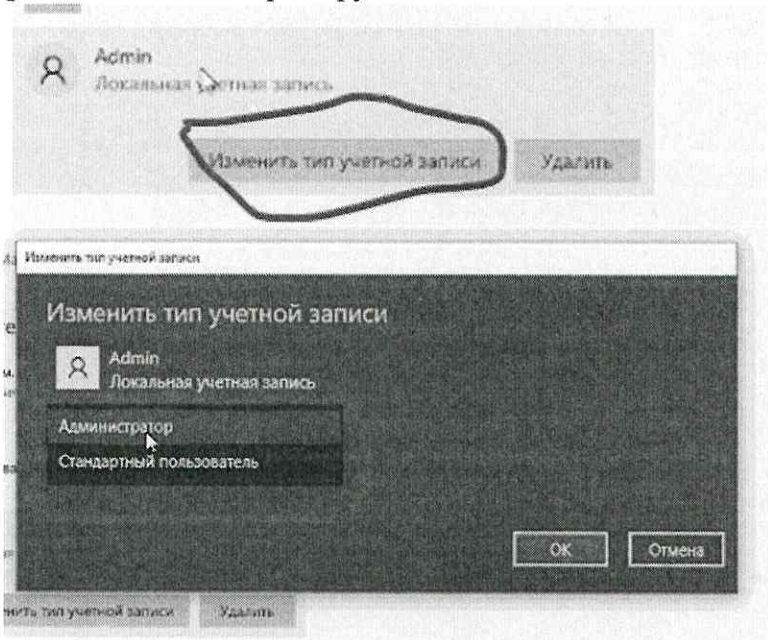


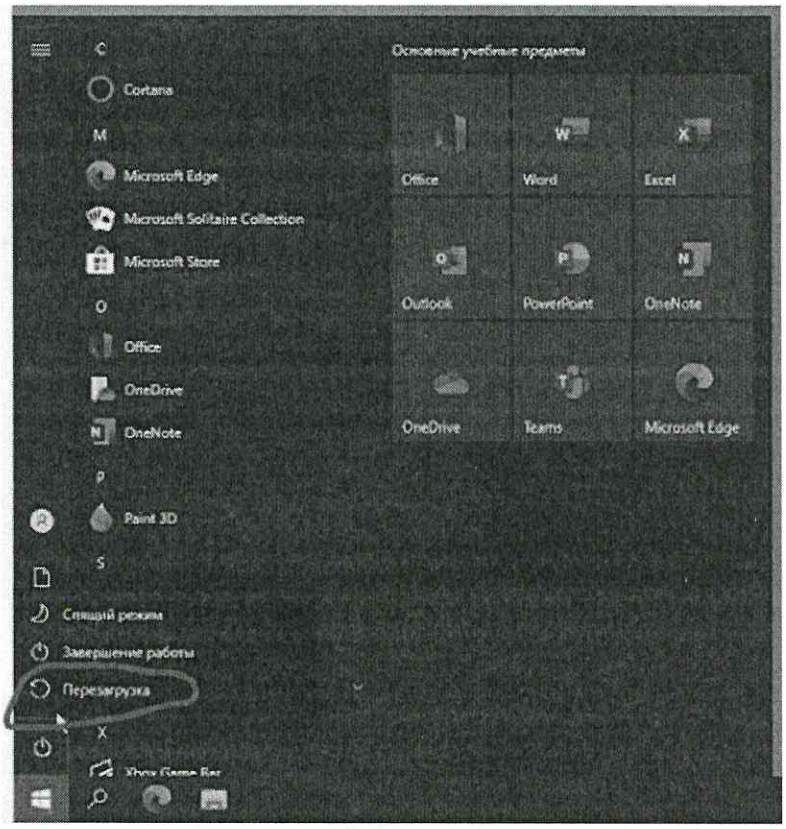


- После этого указываем данные для нашей новой учетной записи «Admin» и пароль (p@ssw0rd), заполнив контрольные вопросы

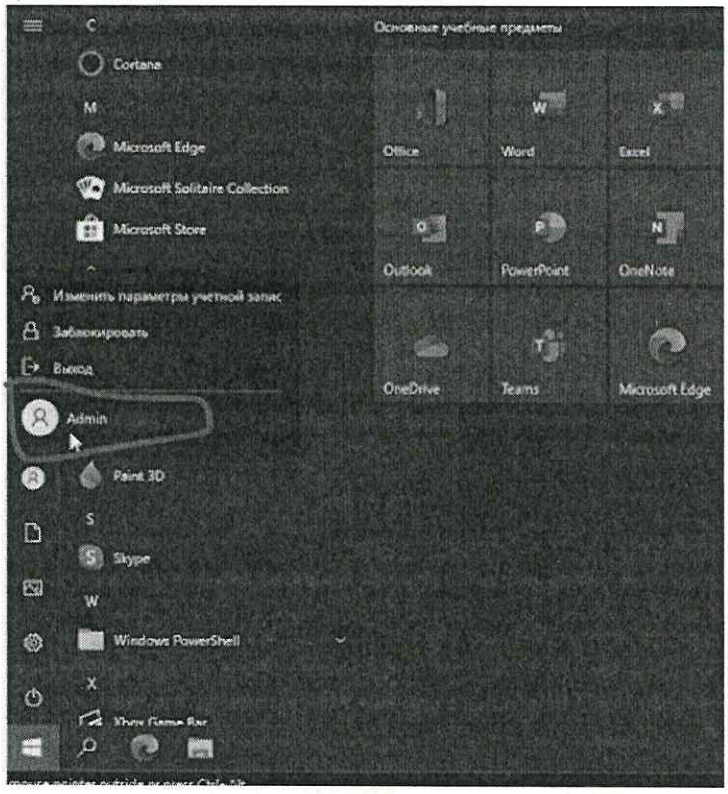


- Далее необходимо изменить тип учетной записи на учетную запись с правами администратора и после этого перезагрузить ОС.



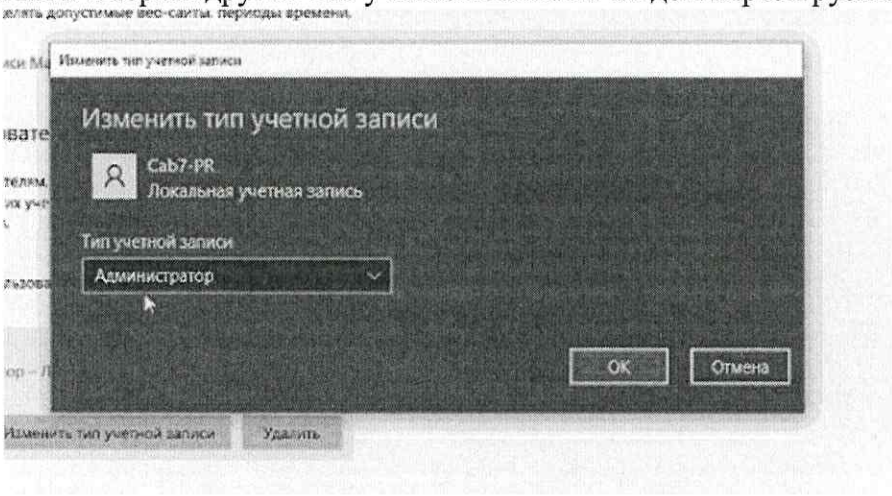


- После запуска ОС снова, необходимо переключиться на новую учетную запись через меню пуск, нажав на значок пользователя.



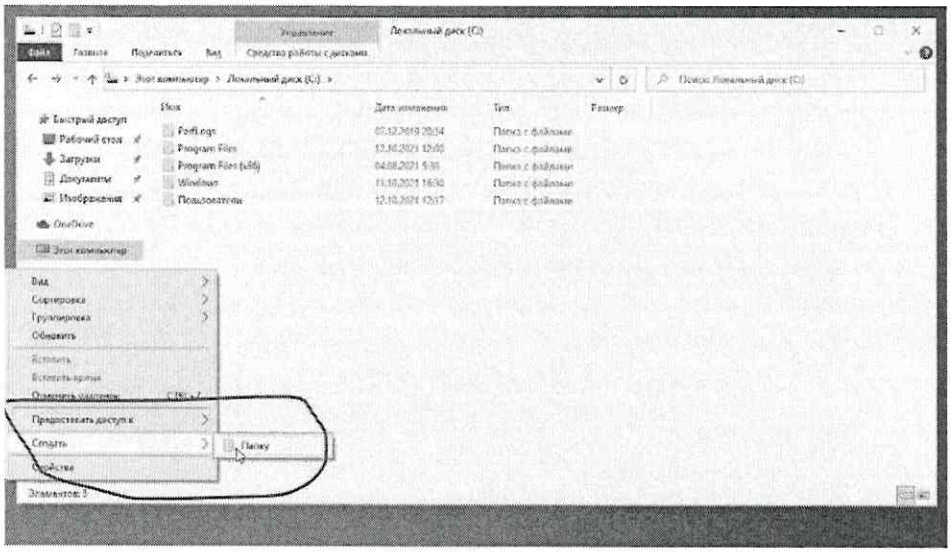
- После входа в учетную запись ново администратора, необходимо отозвать права админа и стандартного пользователя перейдя по пути: «Пуск – Параметры –

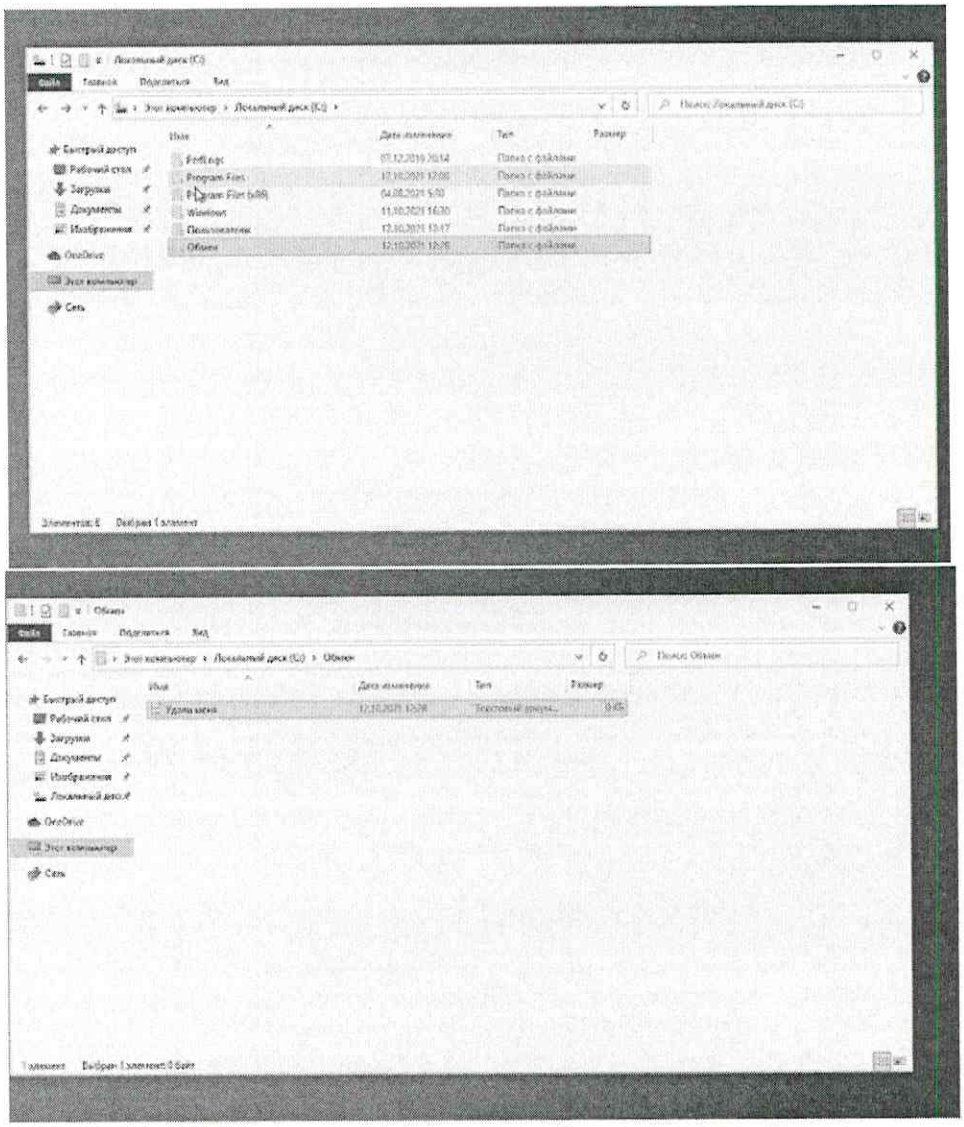
Учетные записи – Семья и другие пользователи» и выбрать учетную запись пользователя и выбрать другой тип учетной записи и следом перезагрузить ОС.



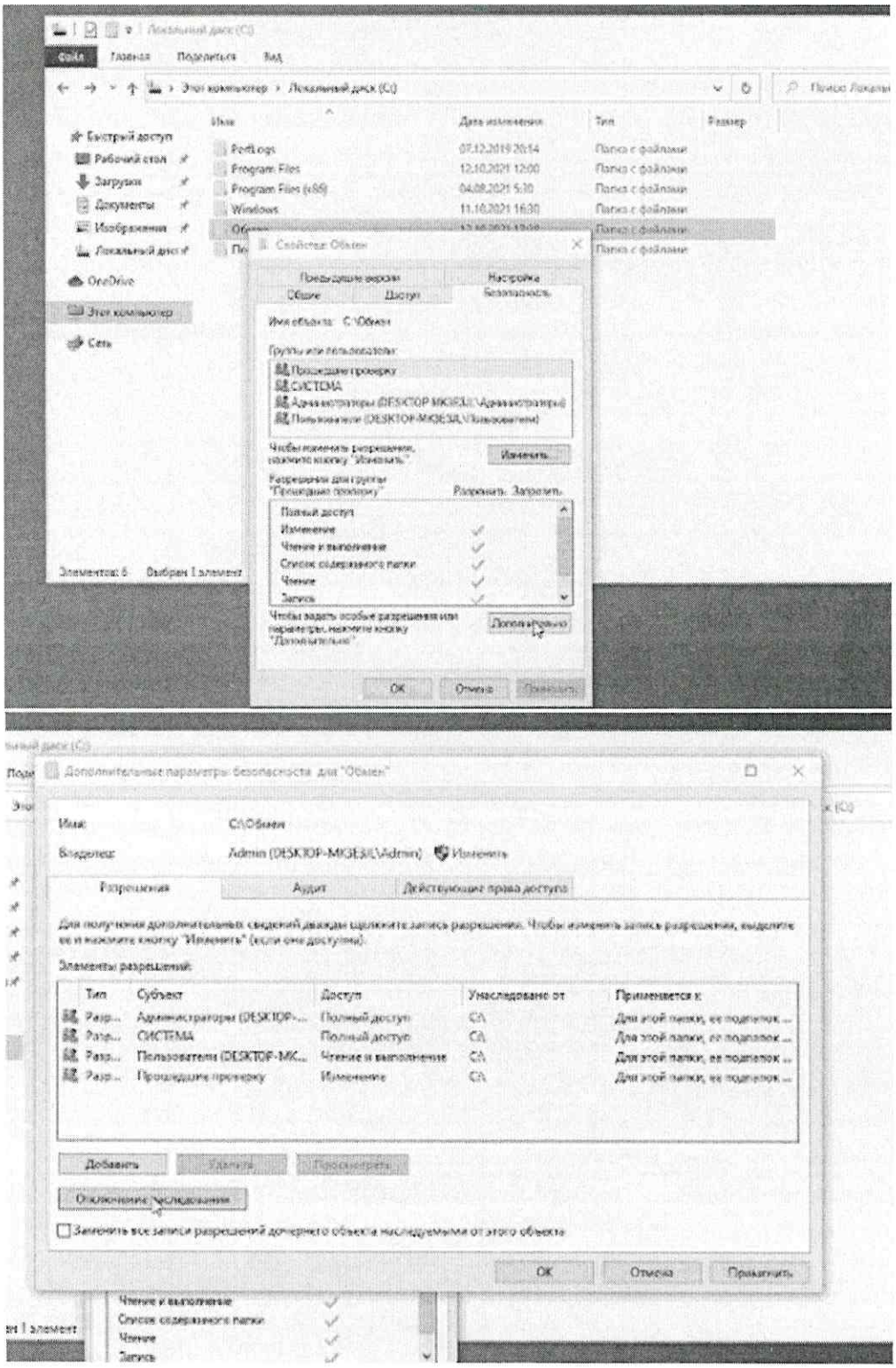
1. Создать папку с ограниченными правами для пользователя User:

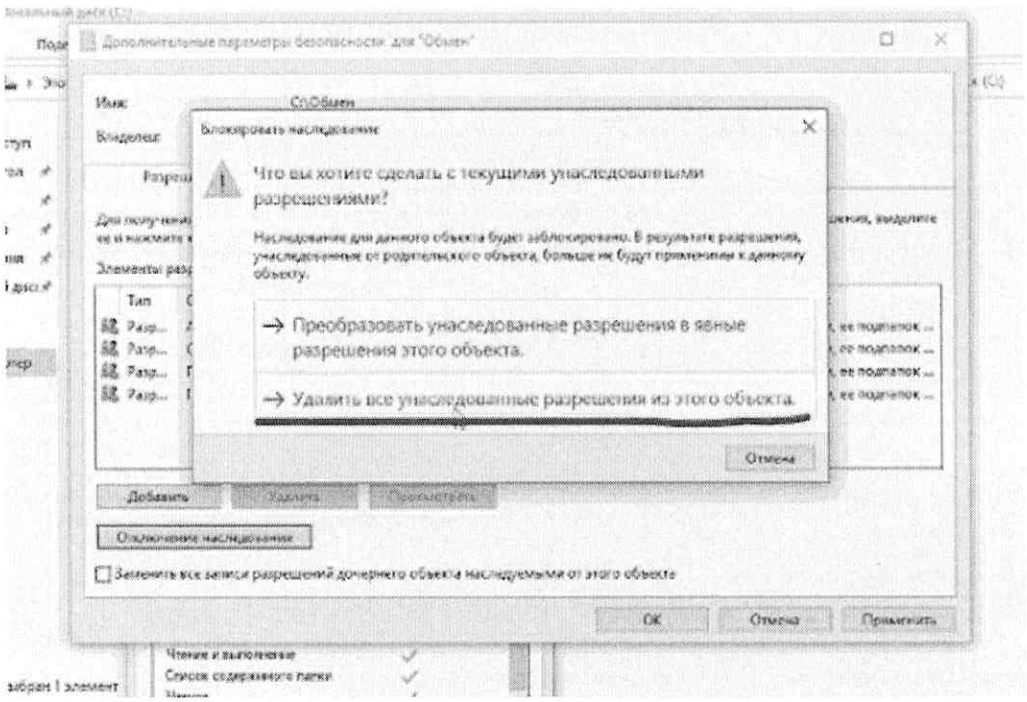
- После повторной перезагрузки, авторизуемся в учетной записи администратора, открываем проводник и переходим в корневой каталог диска «С». Тут мы создам Папку «обмен», которая в теории, будет использоваться для обмена данными между учетными записями. В данной папке создаем файл «Удали меня» для дальнейшего тестирования примененных параметров.



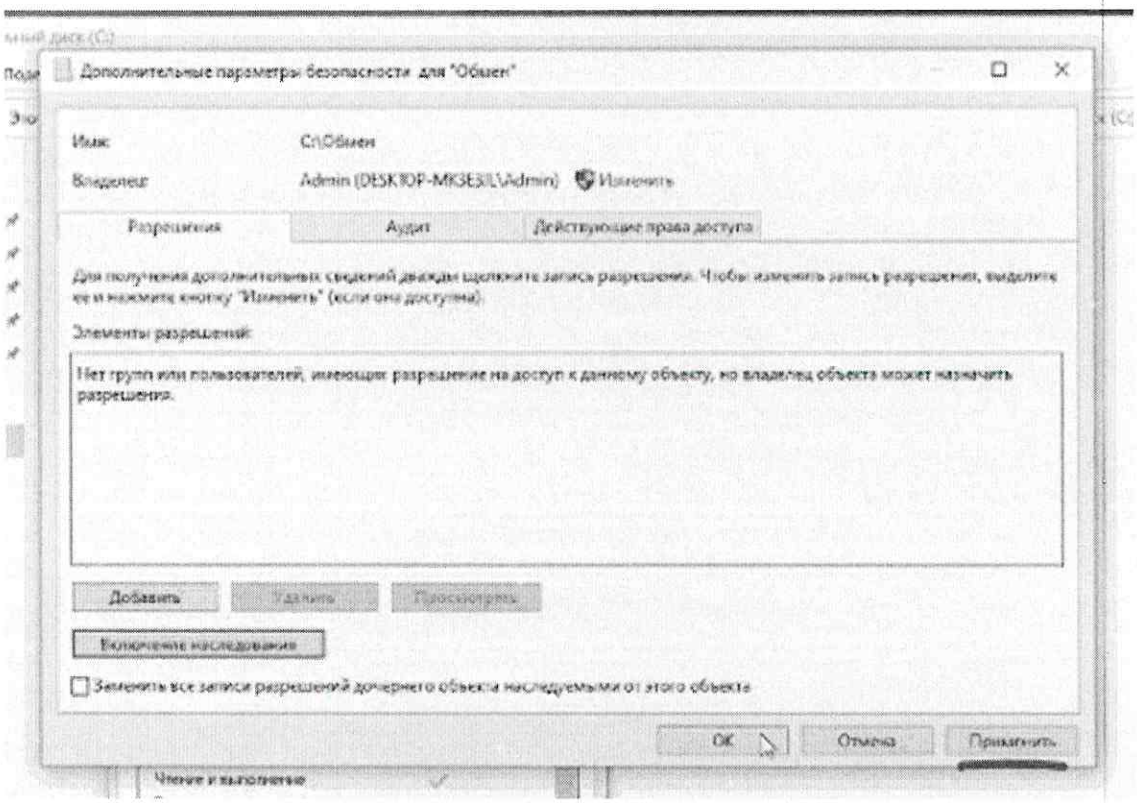


- Далее заходим в свойства папки «Обмен», выбираем раздел «Безопасность», далее выбираем пункт «Дополнительно» и отключаем наследование прав для всех пользователей системы.

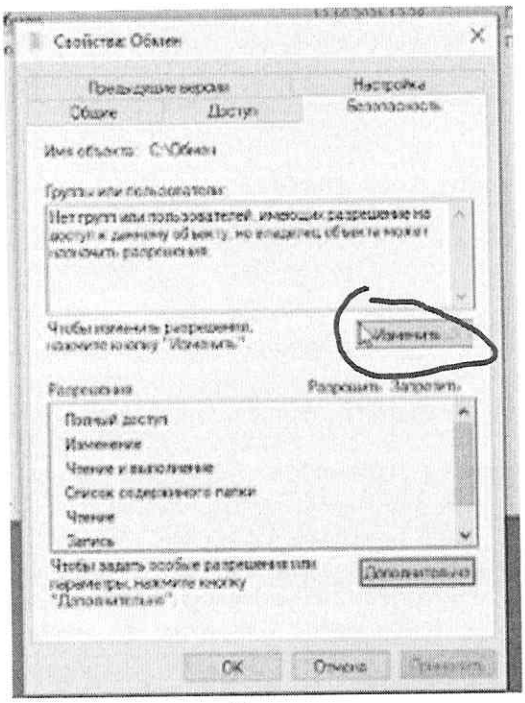

Файл
Главная
Поделиться
Вид
Этот компьютер › Локальный диск (C:)
Быстрый доступ
Рабочий стол
Загрузки
Документы
Изображения
Локальный диск
OneDrive
Этот компьютер
Сеть
Имя
Дата изменения
Тип
Размер
PerfLogs
Program Files
Program Files (x86)
Windows
Свойства: Обмен
Предыдущие версии
Настройка
Общие
Доступ
Безопасность
Имя объекта: C:\Обмен
Группы или пользователи:
Прошедшие проверку
СИСТЕМА
Администраторы (DESKTOP-MKGE3JE\Администраторы)
Пользователи (DESKTOP-MKGE3JE\Пользователи)
Изменить...
Разрешения для группы "Прошедшие проверку"
Разрешить
Запретить
Полный доступ
Изменение
Чтение и выполнение
Список содержимого папки
Чтение
Запись
Дополнительно
OK
Отмена
Применить
Элементов: 6
Выбран 1 элемент
Дополнительные параметры безопасности для "Обмен"
Имя:
C:\Обмен
Владелец:
Admin (DESKTOP-MKGE3JE\Admin)
Изменить
Разрешения
Аудит
Действующие права доступа
Для получения дополнительных сведений дважды щелкните запись разрешения. Чтобы изменить запись разрешения, выделите ее и нажмите кнопку "Изменить" (если она доступна).
Элементы разрешений:
Тип
Субъект
Доступ
Унаследовано от
Применяется к
Разр...
Администраторы (DESKTOP-...
Полный доступ
C:\
Для этой папки, ее подпапок ...
Разр...
СИСТЕМА
Полный доступ
C:\
Для этой папки, ее подпапок ...
Разр...
Пользователи (DESKTOP-MK...
Чтение и выполнение
C:\
Для этой папки, ее подпапок ...
Разр...
Прошедшие проверку
Изменение
C:\
Для этой папки, ее подпапок ...
Добавить
Удалить
Просмотреть
Отключение наследования
Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта
OK
Отмена
Применить



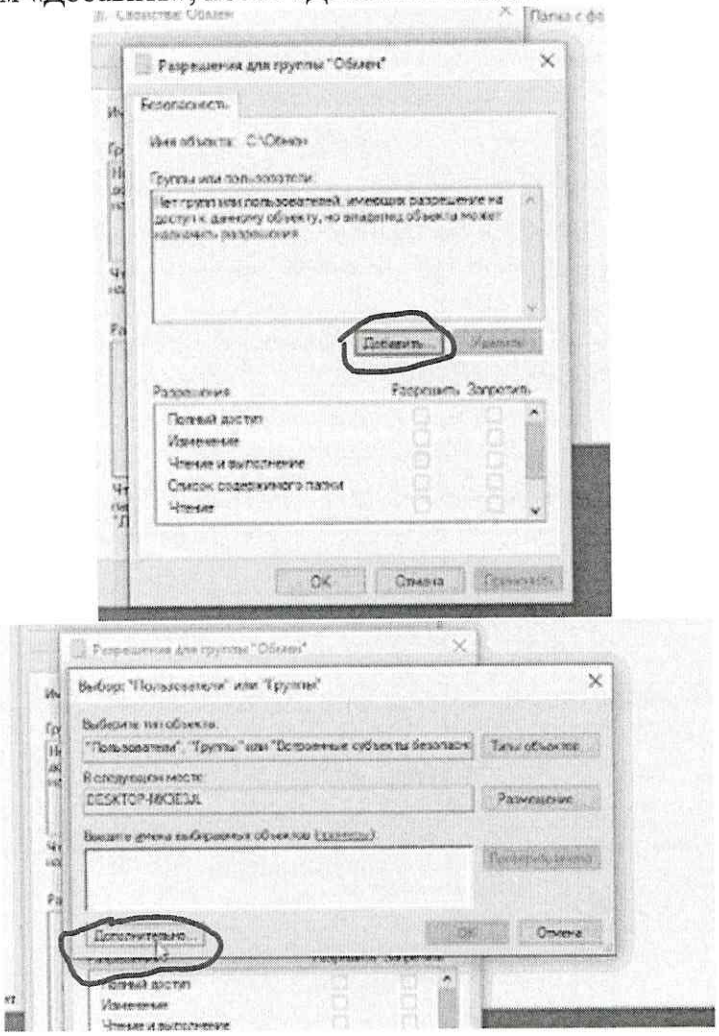
- После данной операции применяем изменения.



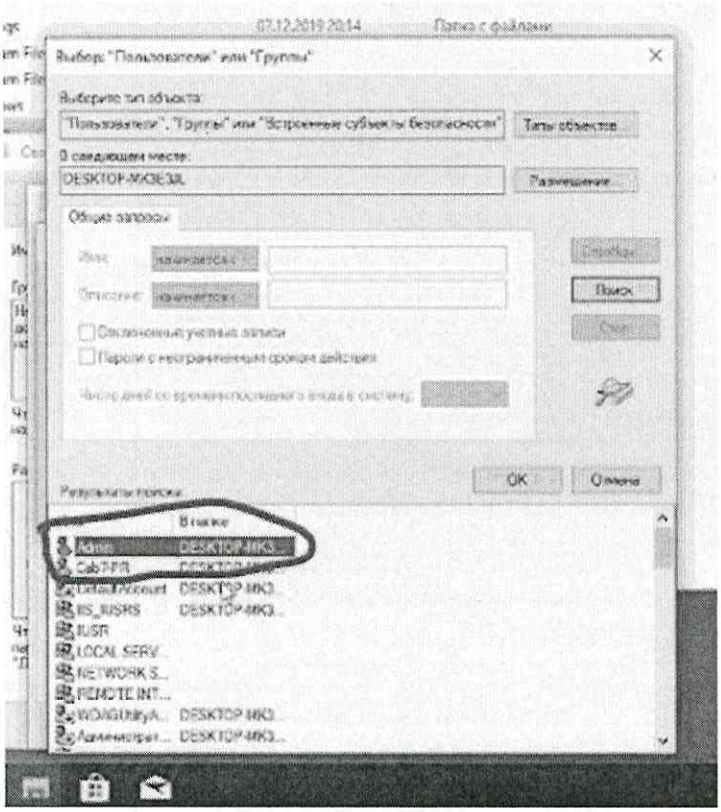
- Сейчас необходимо добавить наших пользователей и выдать им разрешения, для этого нажимаем кнопку «Изменить».



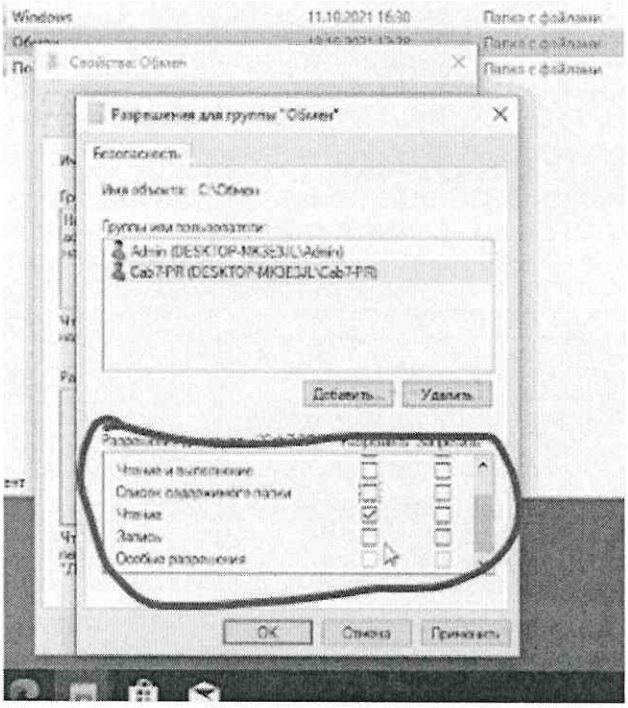
- Далее нажимаем «Добавить», после «Дополнительно».



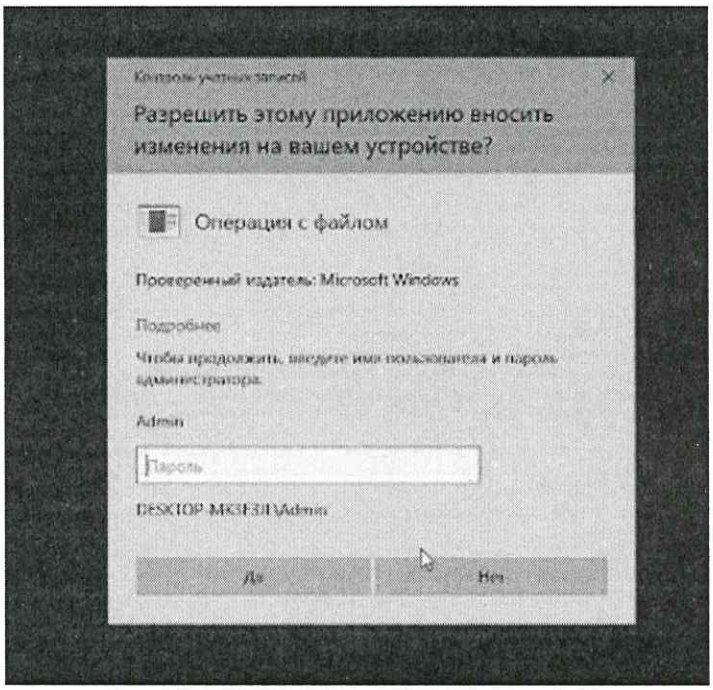
- Потом кнопку в правом блоке «Поиск» и выбрать наших пользователей (Admin и User) по очереди.



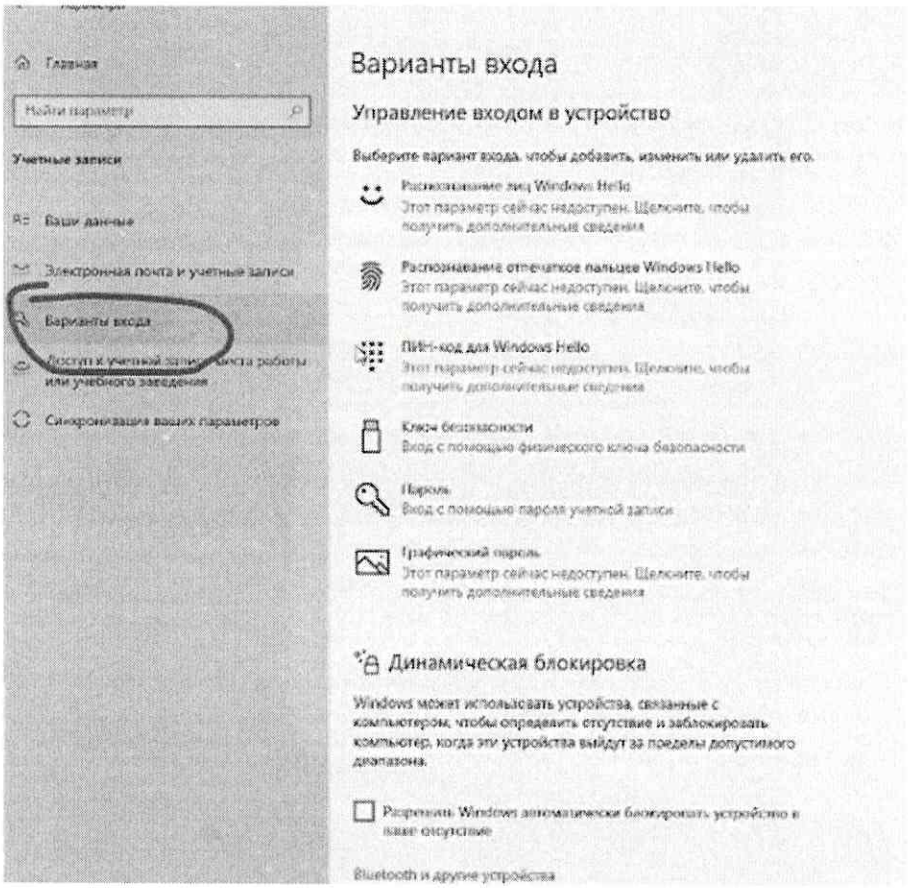
- После этого нажимаем на каждого пользователя и назначаем им права в нижнем окошке. Администратору ставим все галочки на пунктах разрешить, а нашему пользователю ставим галочку напротив пункта чтения. После нажимаем применить и закрываем окно свойств.

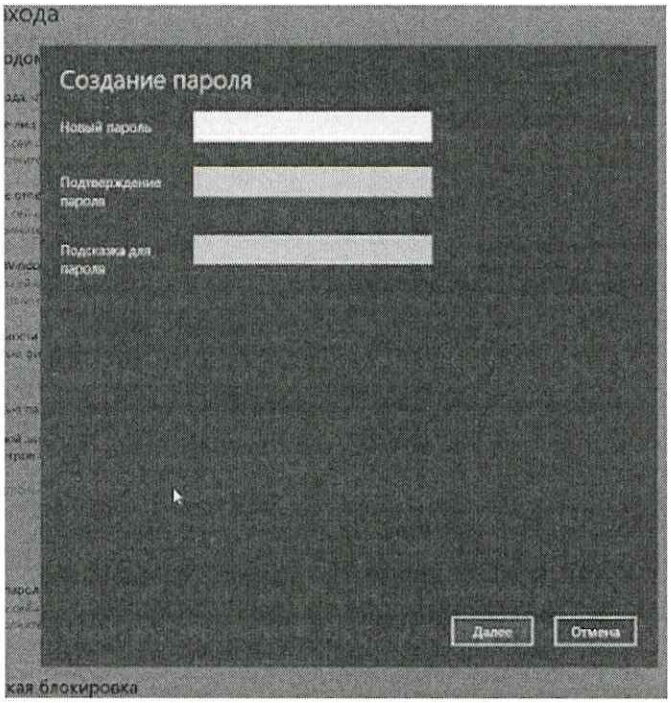


- Следующим шагом, мы заходим в учетную запись пользователя, переходим в корень диска «С» и пытаемся удалить нашу папку или файл внутри нее. Если все сделано верно, то при данной операции, потребуются права администратора.



2. Установить пароль на вход пользователю User
   - Теперь установим пароль нашему пользователю будучи авторизованным в нем, для этого переходим по пути: «Пуск – Параметры – Учетные записи – Варианты входа»

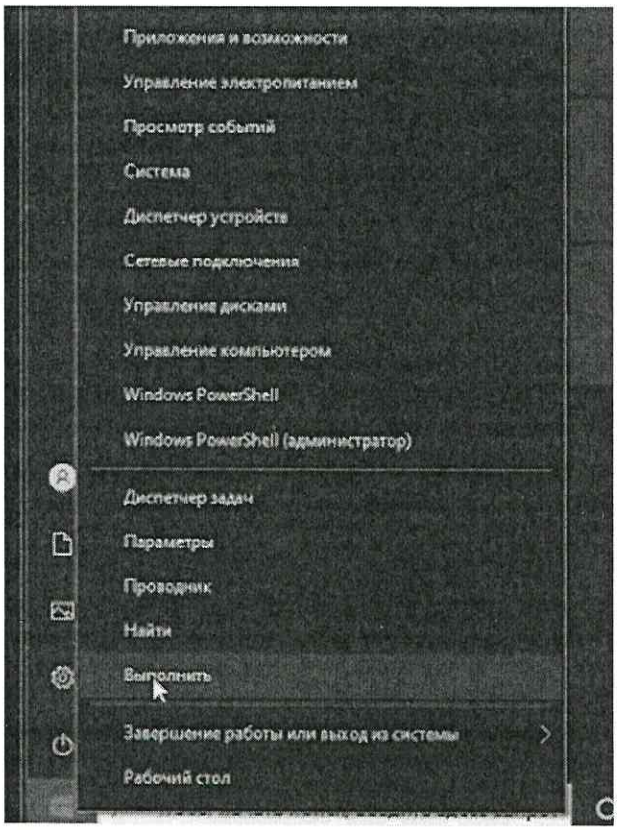


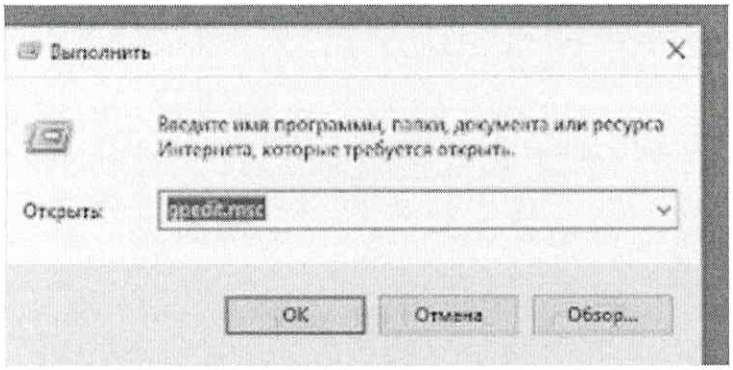


- Далее выбираем пункт «Пароль» у вас откроется окно для установки нового пароля и установите пароль «p@ssw0rd1»

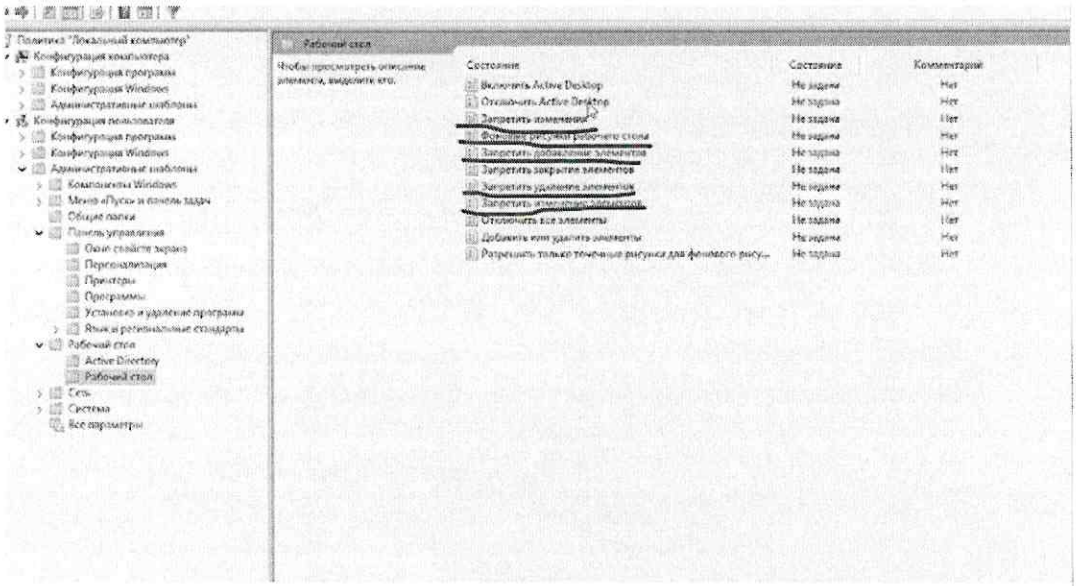
3. Работа с групповыми политиками:

В ОС редакции Pro есть еще один инструмент, который позволяет ввести ограничения на те или иные действия – Групповые политики. Для того чтобы заблокировать некоторые функции для пользователя User, перейдем в окно команд «Выполнить» (правой кнопкой мыши по пуски – «Выполнить», и введем команду gpedit.msc



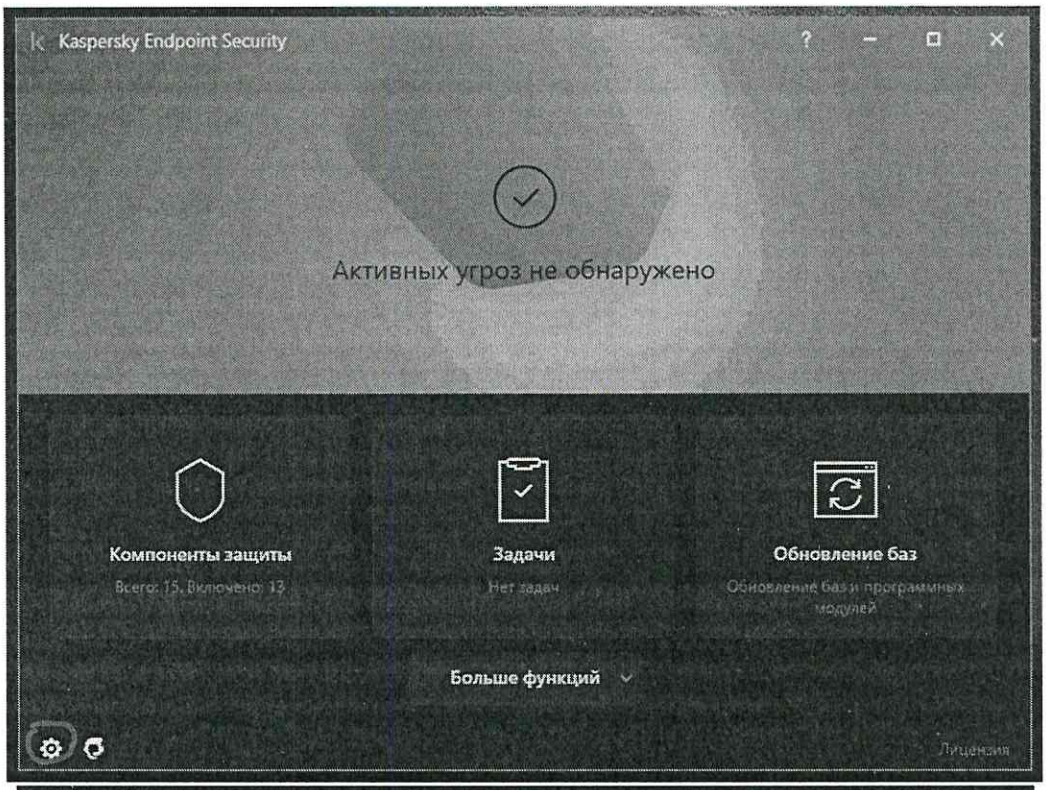


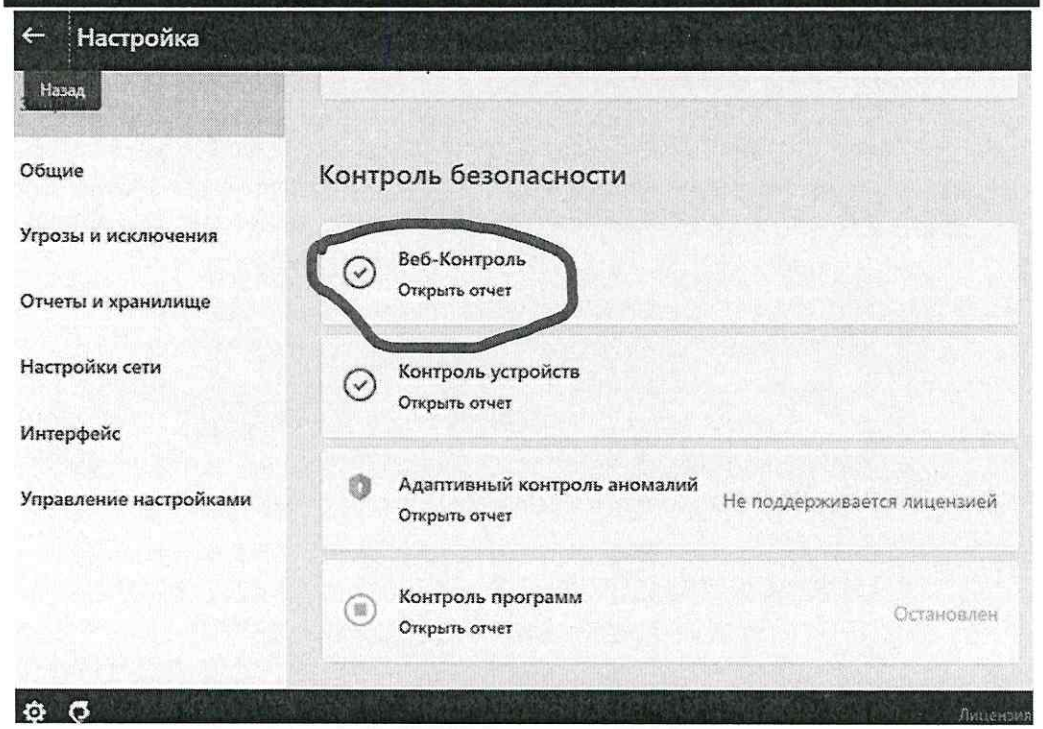
- После этого, в левом окне идем по пути: «Конфигурация пользователя – Административные шаблоны – Панель Управления – Рабочий стол» и включаем запреты на изменение, удаление, добавление элементов, а также настраиваем путь до своей картинки рабочего стола, которая будет неизменно установлена у пользователя User.

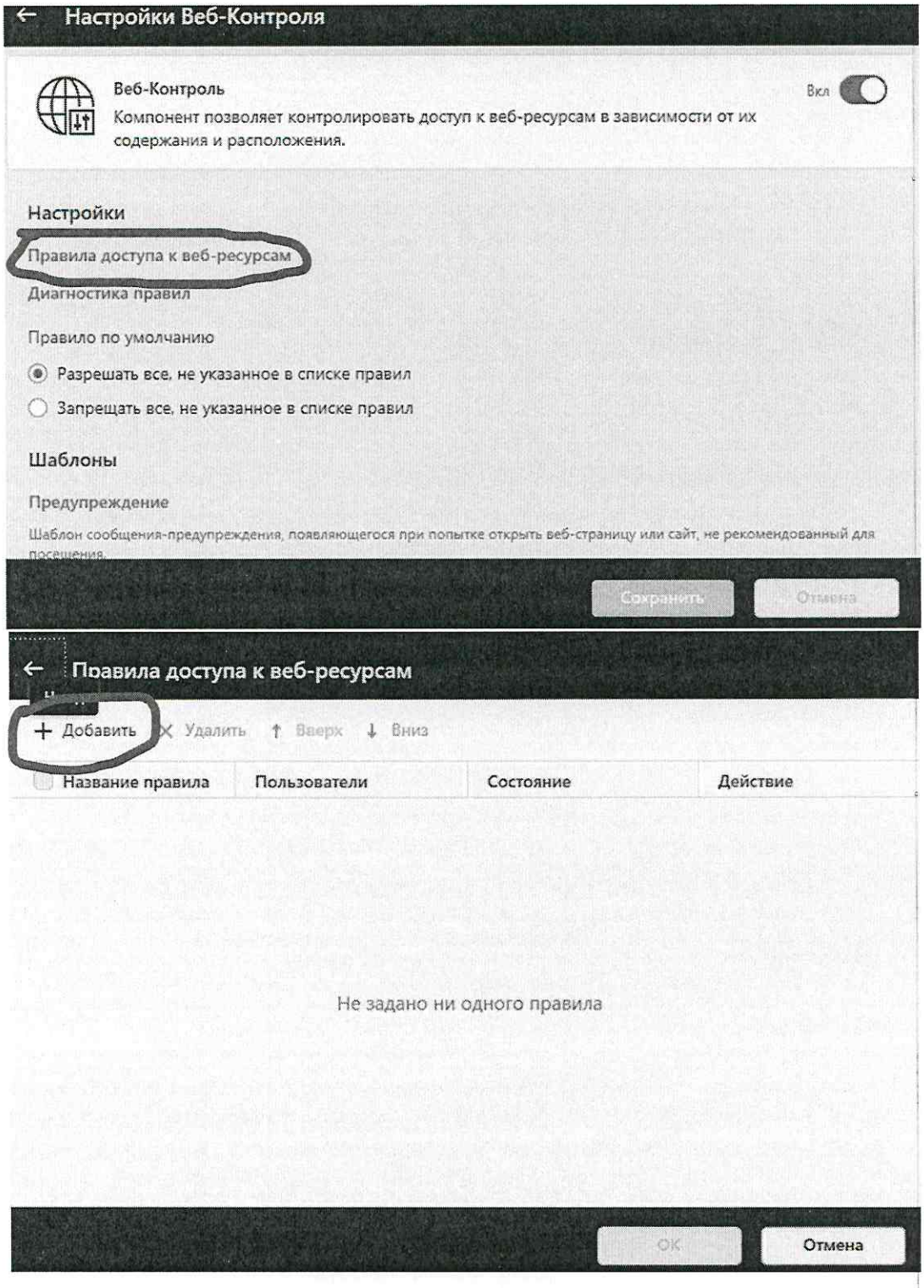


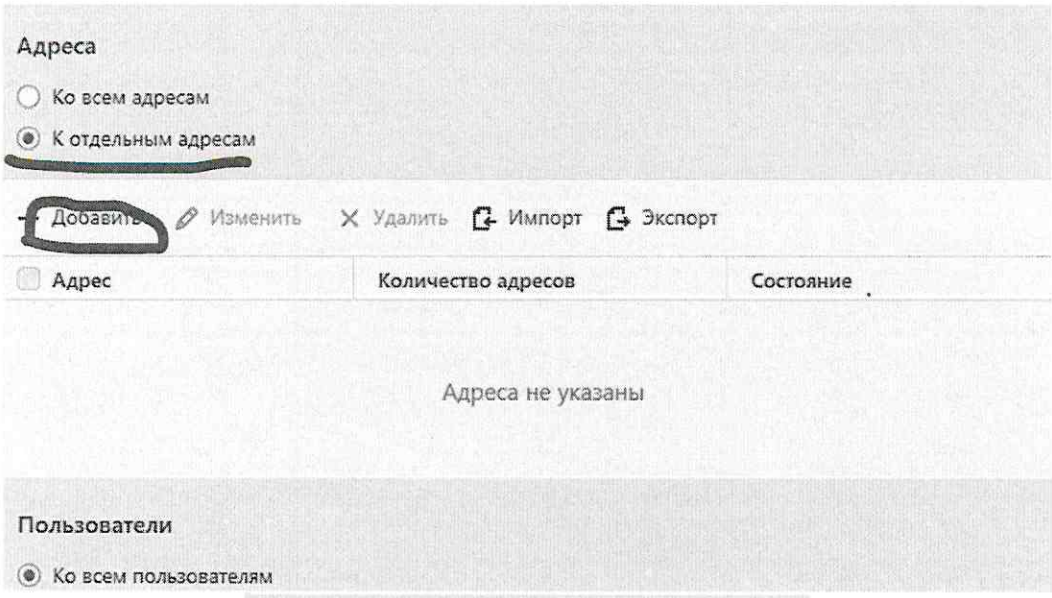
Выполнение задания (25 мин) – Добавочный модуль

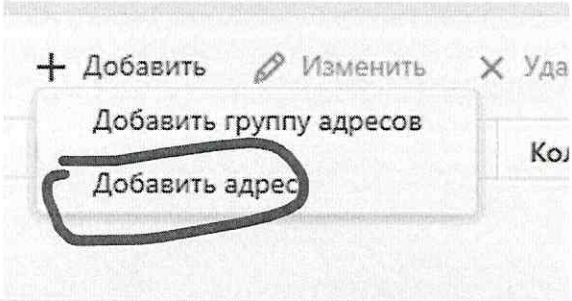
Блокировка интернет-ресурсов и приложений на примере антивирусного решения Kaspersky Internet Security. В данном модуле мы рассмотрим блокировку тех или иных ресурсов уже готовыми коммерческими решениями следующие вопросы:
-Блокировка веб ресурсов в индивидуальном порядке

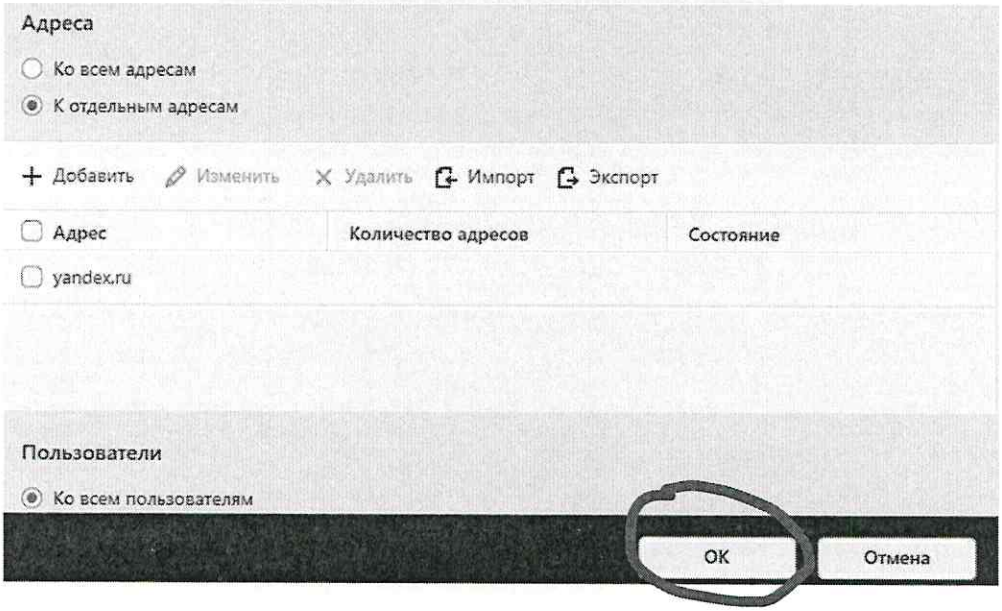

Kaspersky Endpoint Security
Активных угроз не обнаружено
Компоненты защиты
Всего: 15, Включено: 13
Задачи
Нет задач
Обновление баз
Обновление баз и программных модулей
Больше функций
Лицензия

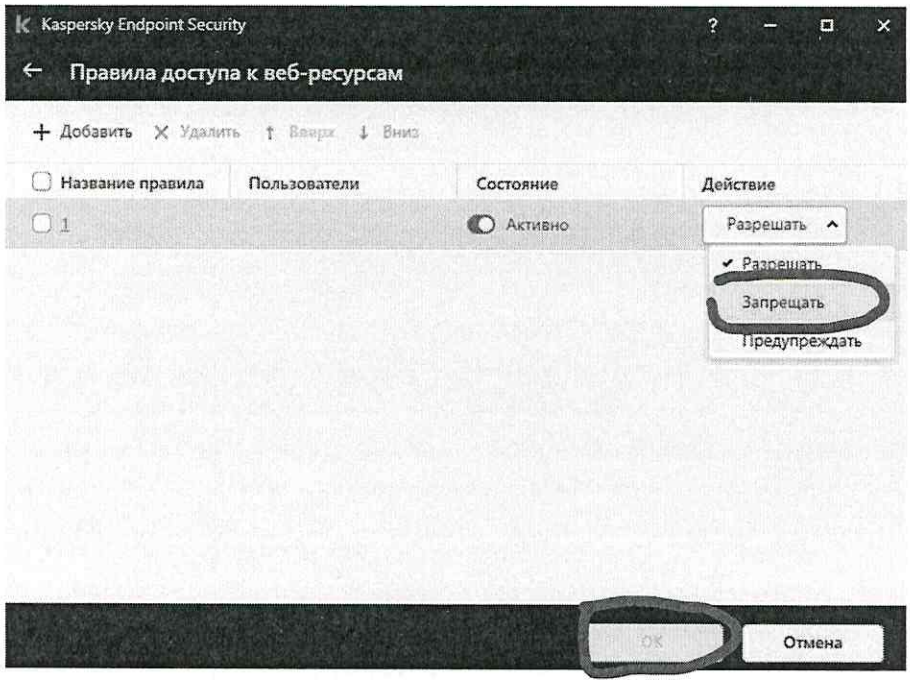

Настройка
Назад
Общие
Угрозы и исключения
Отчеты и хранилище
Настройки сети
Интерфейс
Управление настройками
Контроль безопасности
Веб-Контроль
Открыть отчет
Контроль устройств
Открыть отчет
Адаптивный контроль аномалий
Открыть отчет
Не поддерживается лицензией
Контроль программ
Открыть отчет
Остановлен
Лицензия

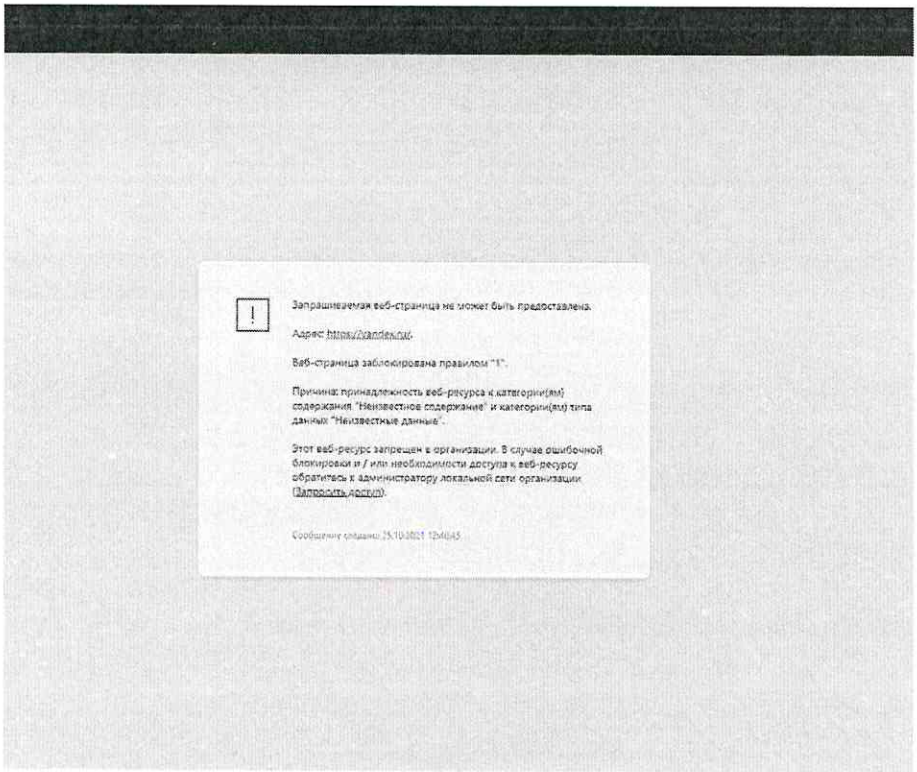

Настройки Веб-Контроля
Веб-Контроль
Компонент позволяет контролировать доступ к веб-ресурсам в зависимости от их содержания и расположения.
Вкл
Настройки
Правила доступа к веб-ресурсам
Диагностика правил
Правило по умолчанию
Разрешать все, не указанное в списке правил
Запрещать все, не указанное в списке правил
Шаблоны
Предупреждение
Шаблон сообщения-предупреждения, появляющегося при попытке открыть веб-страницу или сайт, не рекомендованный для посещения
Сохранить
Отмена
Правила доступа к веб-ресурсам
Добавить
Удалить
Вверх
Вниз
Название правила
Пользователи
Состояние
Действие
Не задано ни одного правила
OK
Отмена


Адреса
Ко всем адресам
К отдельным адресам
Добавить
Изменить
Удалить
Импорт
Экспорт
Адрес
Количество адресов
Состояние
Адреса не указаны
Пользователи
Ко всем пользователям

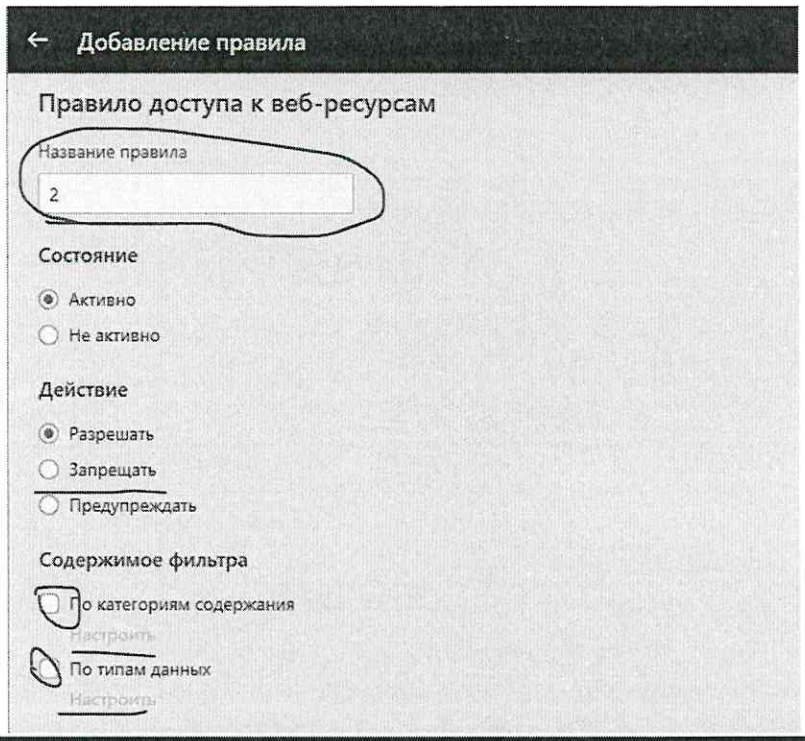

Добавить
Изменить
Добавить группу адресов
Добавить адрес

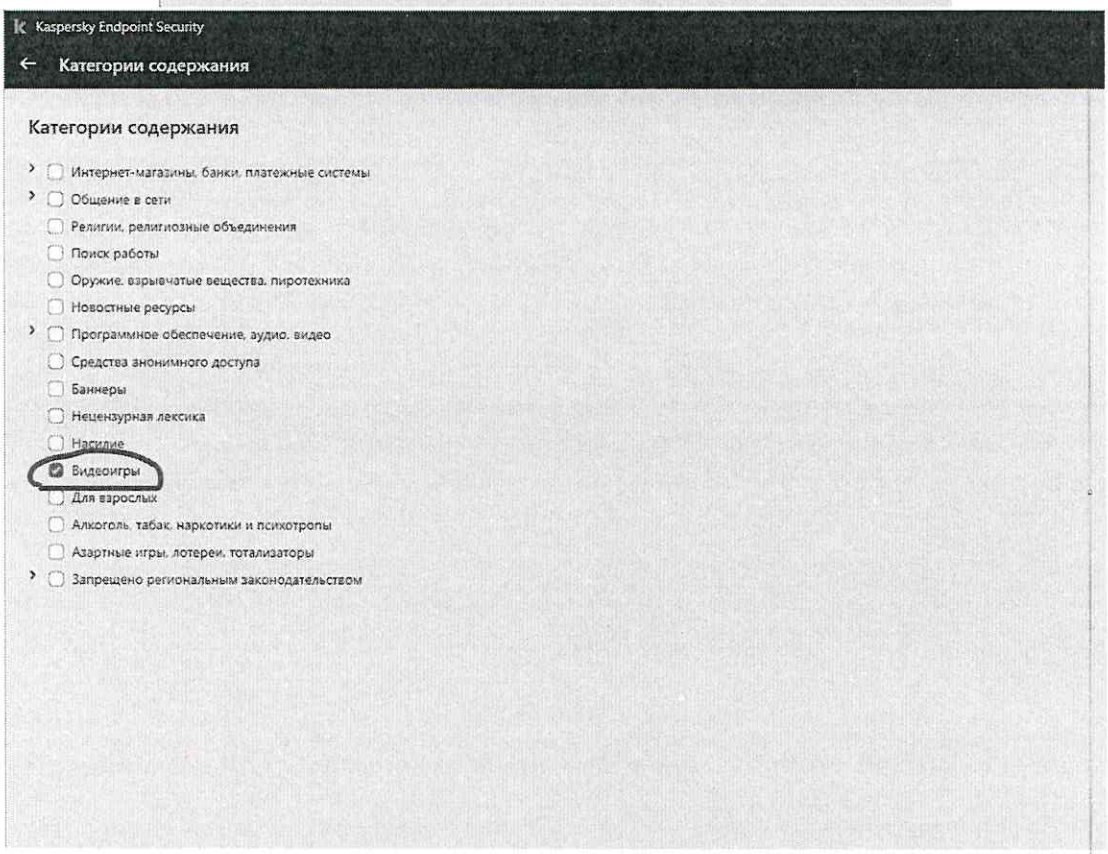

Адреса
Ко всем адресам
К отдельным адресам
Добавить
Изменить
Удалить
Импорт
Экспорт
Адрес
Количество адресов
Состояние
yandex.ru
Пользователи
Ко всем пользователям
OK
Отмена

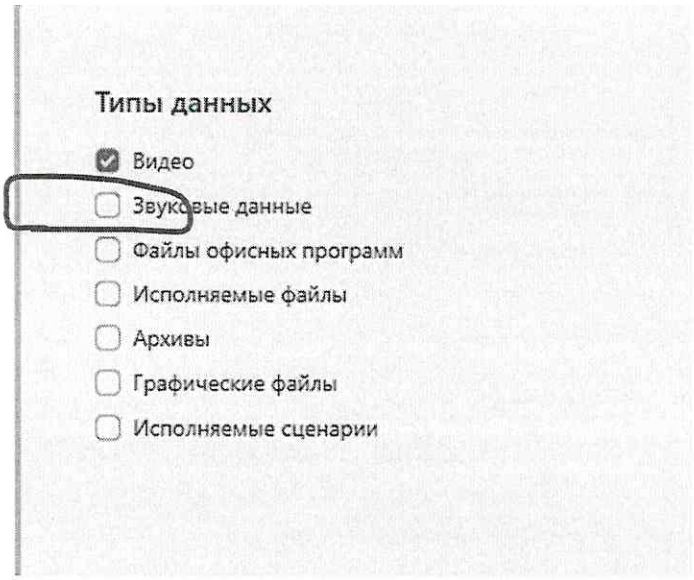




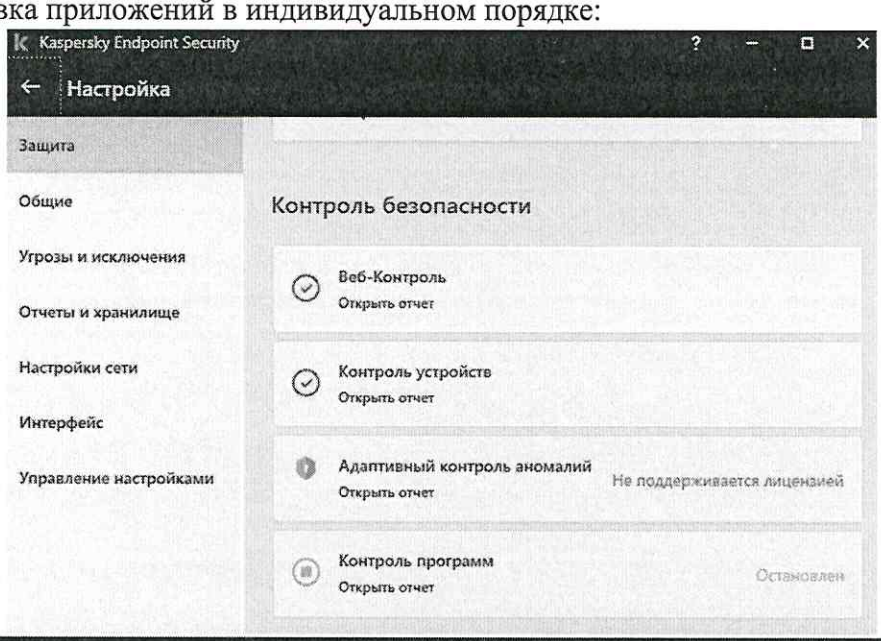
-Блокировка веб ресурсов по тематике.

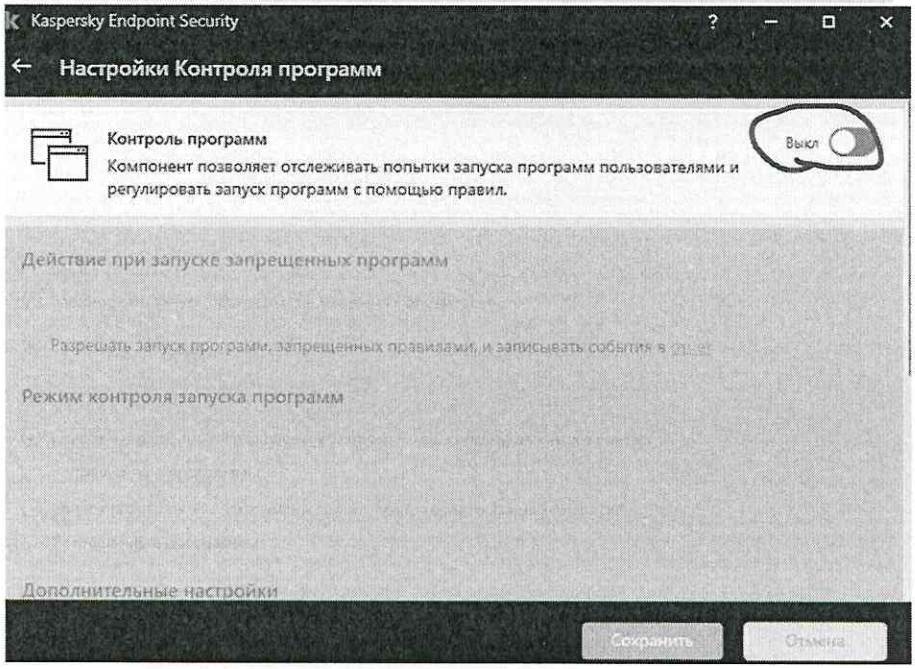

Добавление правила
Правило доступа к веб-ресурсам
Название правила
2
Состояние
Активно
Не активно
Действие
Разрешать
Запрещать
Предупреждать
Содержимое фильтра
По категориям содержания
Настроить
По типам данных
Настроить

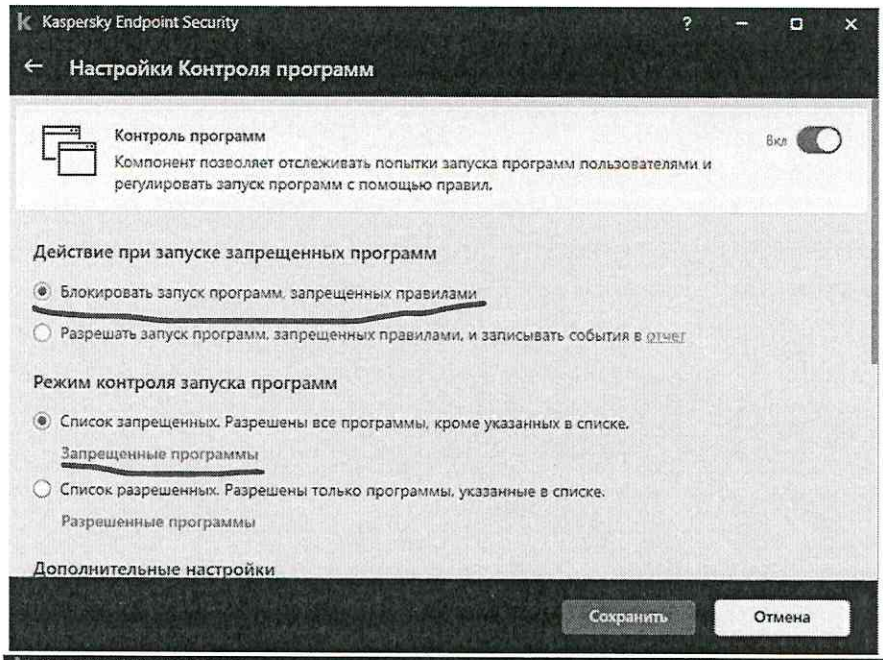

Kaspersky Endpoint Security
Категории содержания
Категории содержания
Интернет-магазины, банки, платежные системы
Общение в сети
Религии, религиозные объединения
Поиск работы
Оружие, взрывчатые вещества, пиротехника
Новостные ресурсы
Программное обеспечение, аудио, видео
Средства анонимного доступа
Баннеры
Нецензурная лексика
Насилие
Видеоигры
Для взрослых
Алкоголь, табак, наркотики и психотропы
Азартные игры, лотереи, тотализаторы
Запрещено региональным законодательством

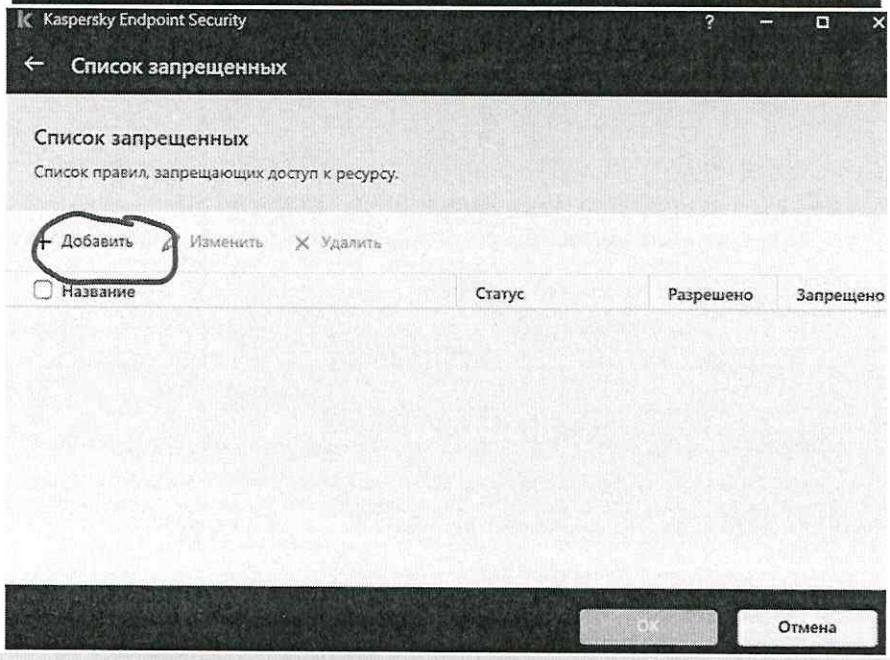


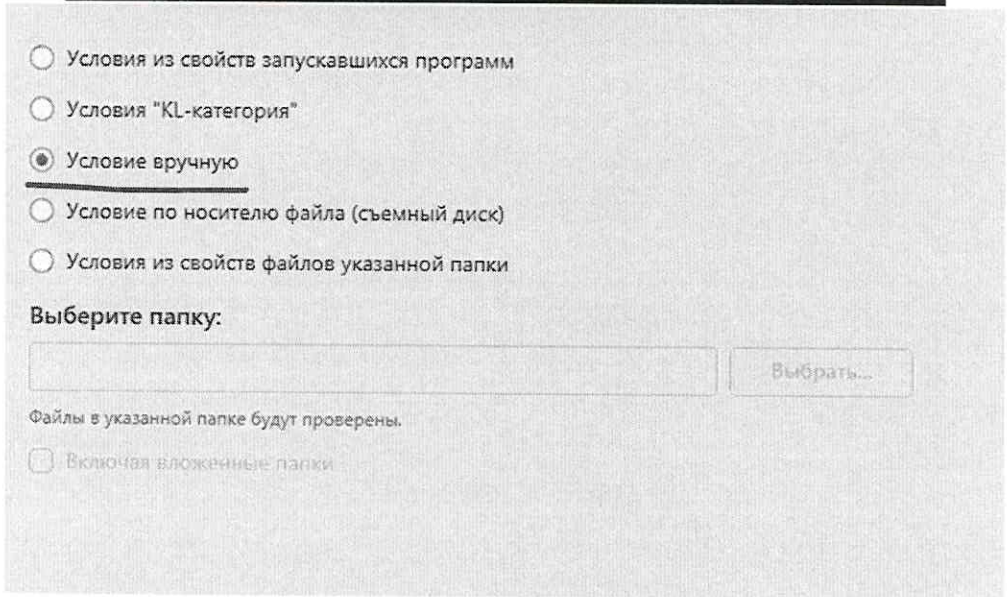
-Блокировка приложений в индивидуальном порядке:



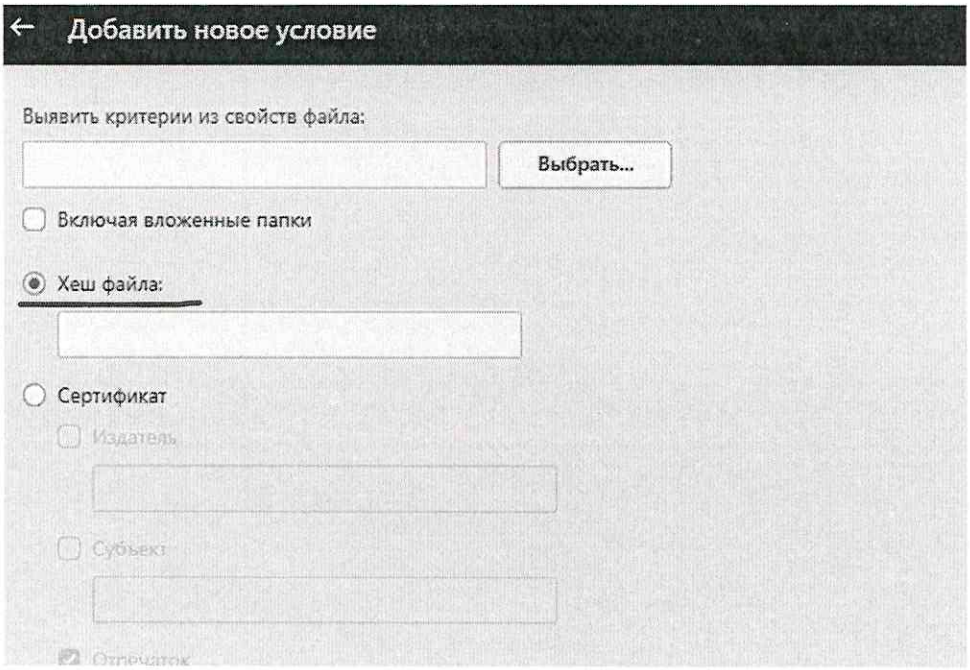




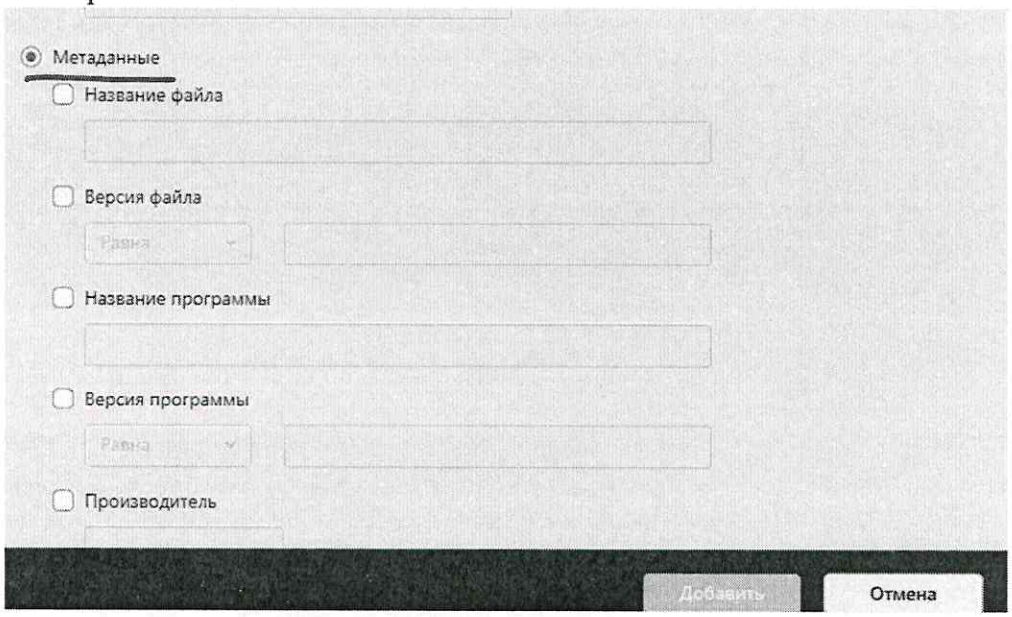




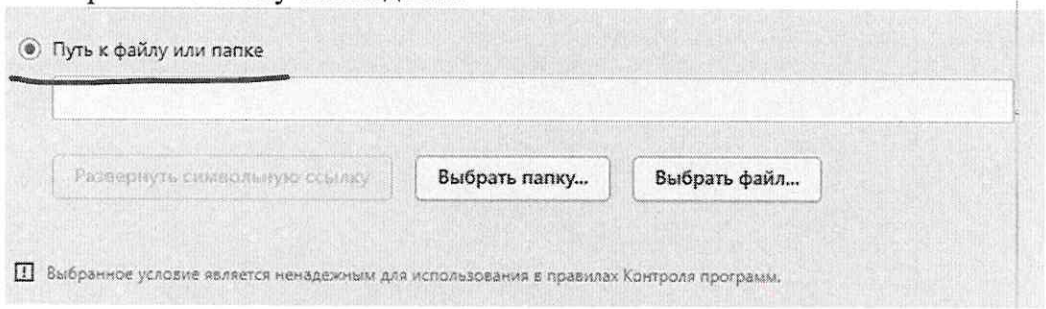
1. Блокировка по Хэш суммам



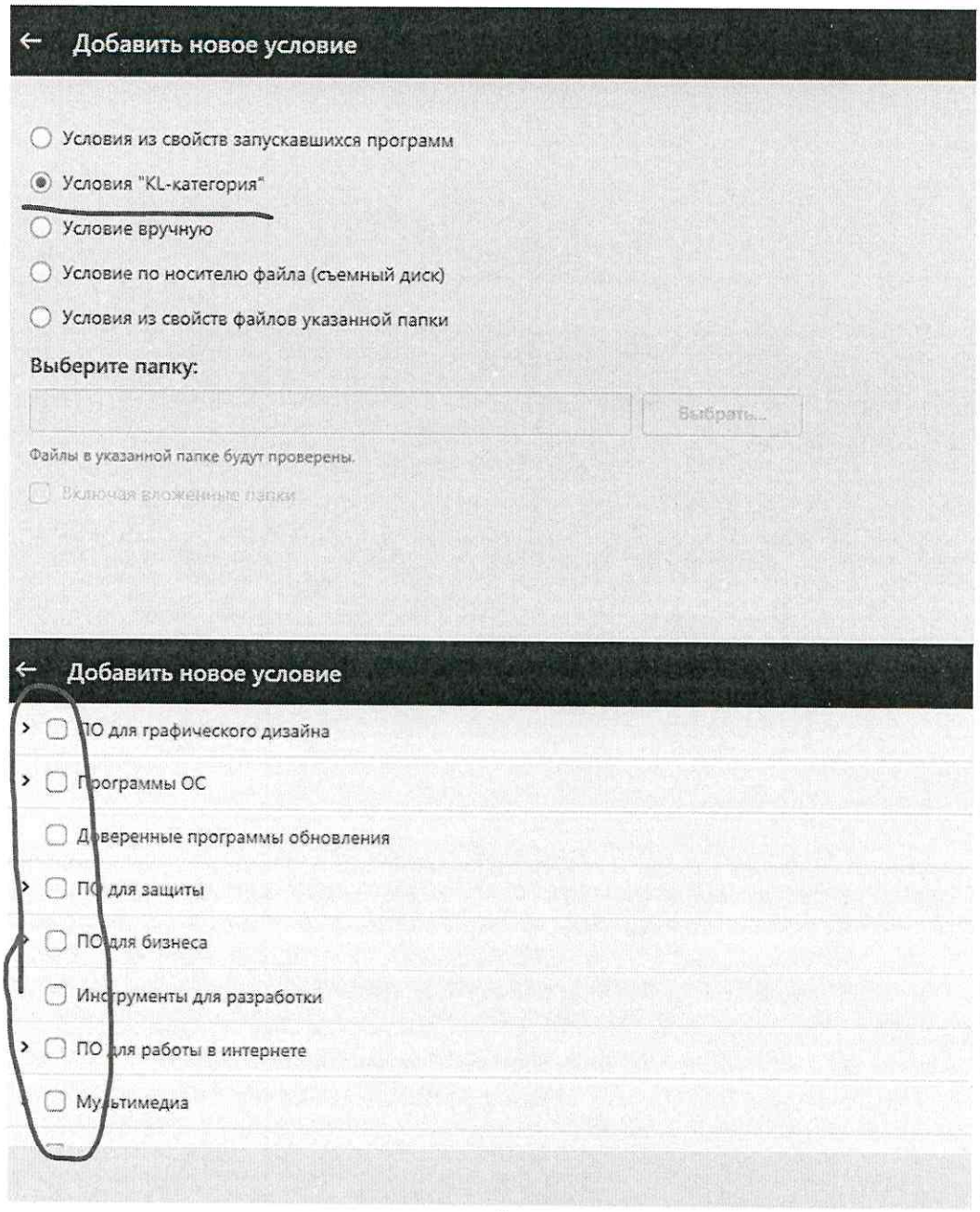
2. Блокировка по тэгам



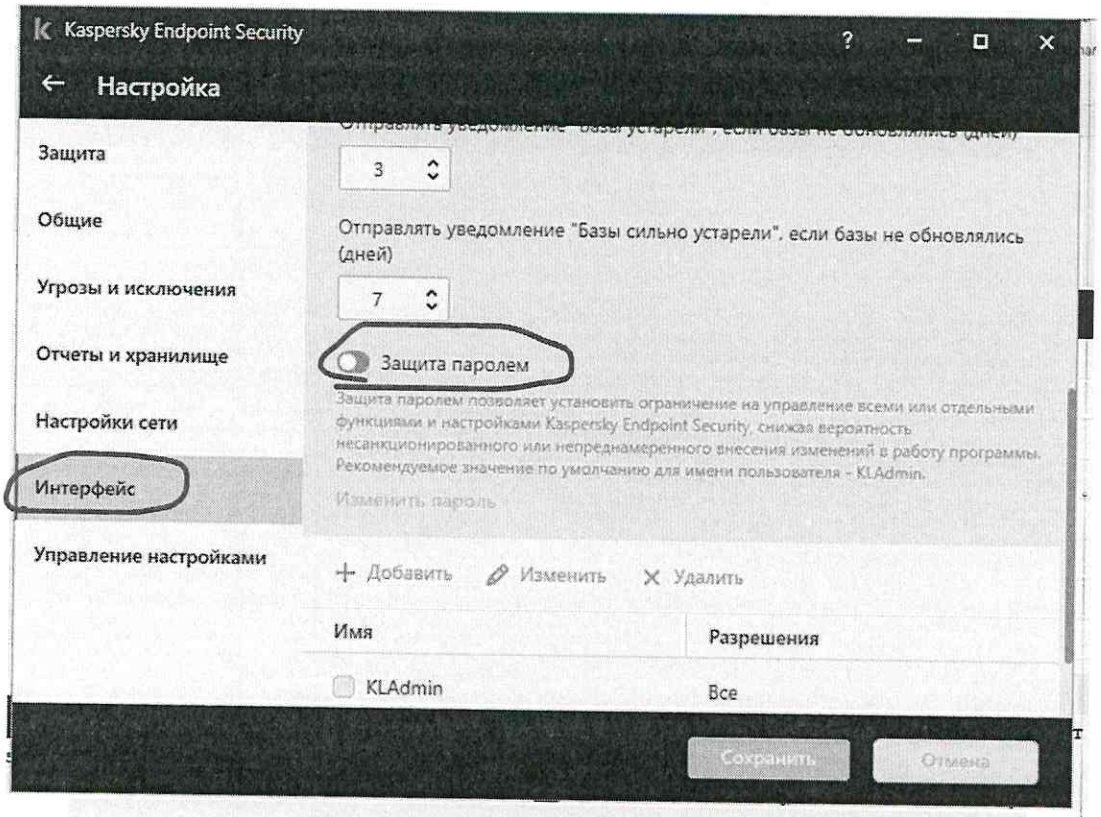
3. Блокировка по месту нахождения

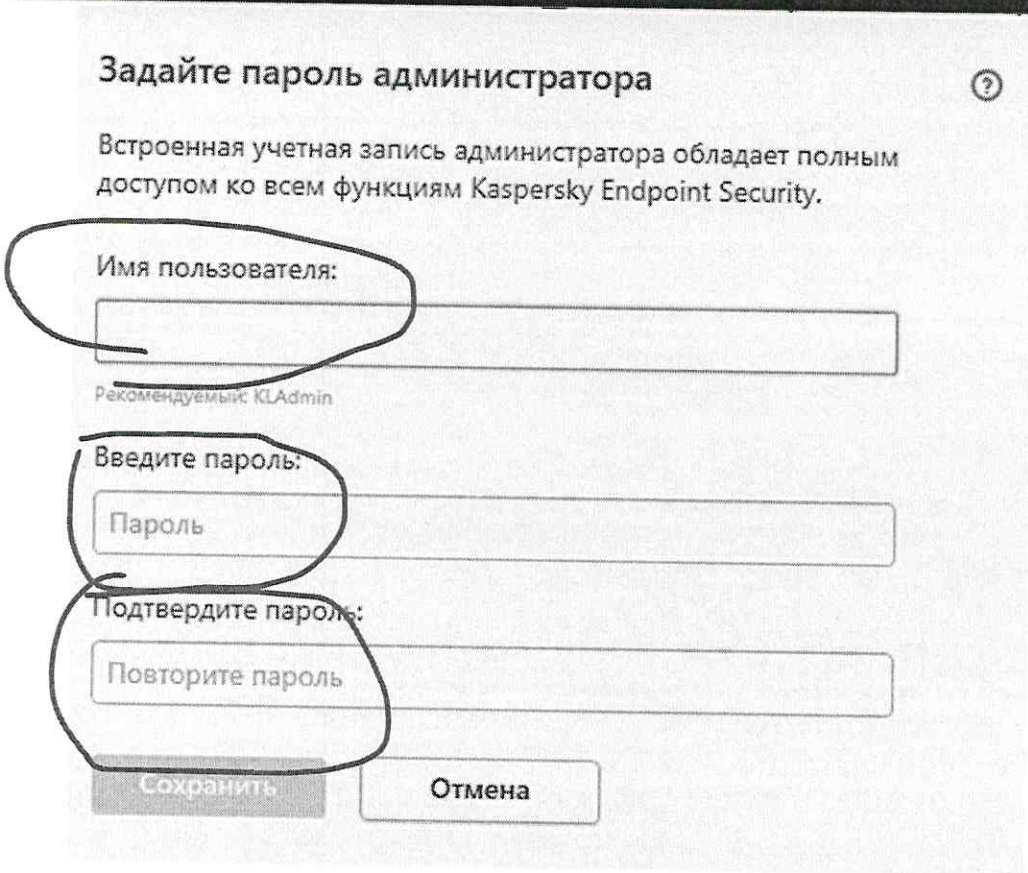


-Блокировка приложений по тематики использования



-Защита настроек антивируса от изменений не авторизованным юзером.





Контроль, оценка и рефлексия (15 мин)

1. Оценивание выполнения работы:

Проверка результатов работ обучающихся на полноту и правильность выполнения в соответствии с заданием.

2. Рекомендации для наставника по контролю результата, процедуре оценки:

– Наставник должен проконтролировать каждое рабочее место участника на

соответствие инфраструктурному листу, в случае затруднений – помочь участнику.

– Наставник должен помочь проверить работу программного обеспечения на каждом рабочем месте в тестовом режиме.

– Во время проведения профпроб наставник постоянно следит за происходящим на рабочих местах

– Наставник должен помочь участникам профпроб по решению возникающих в ходе работы вопросов.

– Наставник следит за временем, отведённым для прохождения модуля.

Критерии выполнения задания:

3. Вопросы для рефлексии учащихся:

Специалист по информационной безопасности – эта специальность появилась с развитием вычислительной техники или ранее она тоже существовала, но в иной форме?