ТЕМА: ОСОБЕННОСТИ СОВМЕСТНОЙ РАБОТЫ С ДОКУМЕНТАМИ В ОБЛАЧНЫХ СЕРВИСАХ.

ЧАСТЬ 3/3

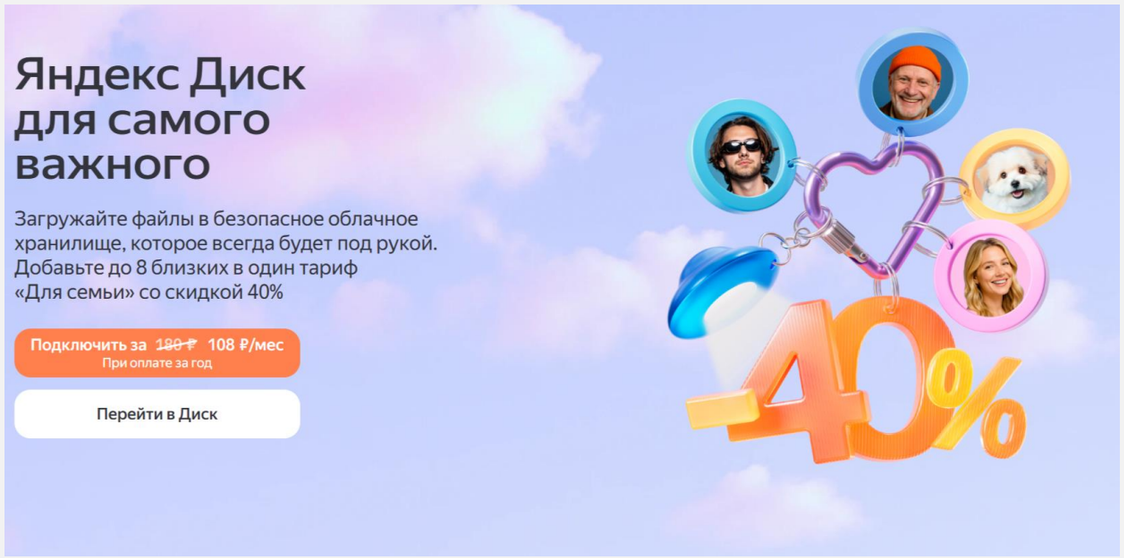
Преподаватель: Самарина Виктория Сергеевна

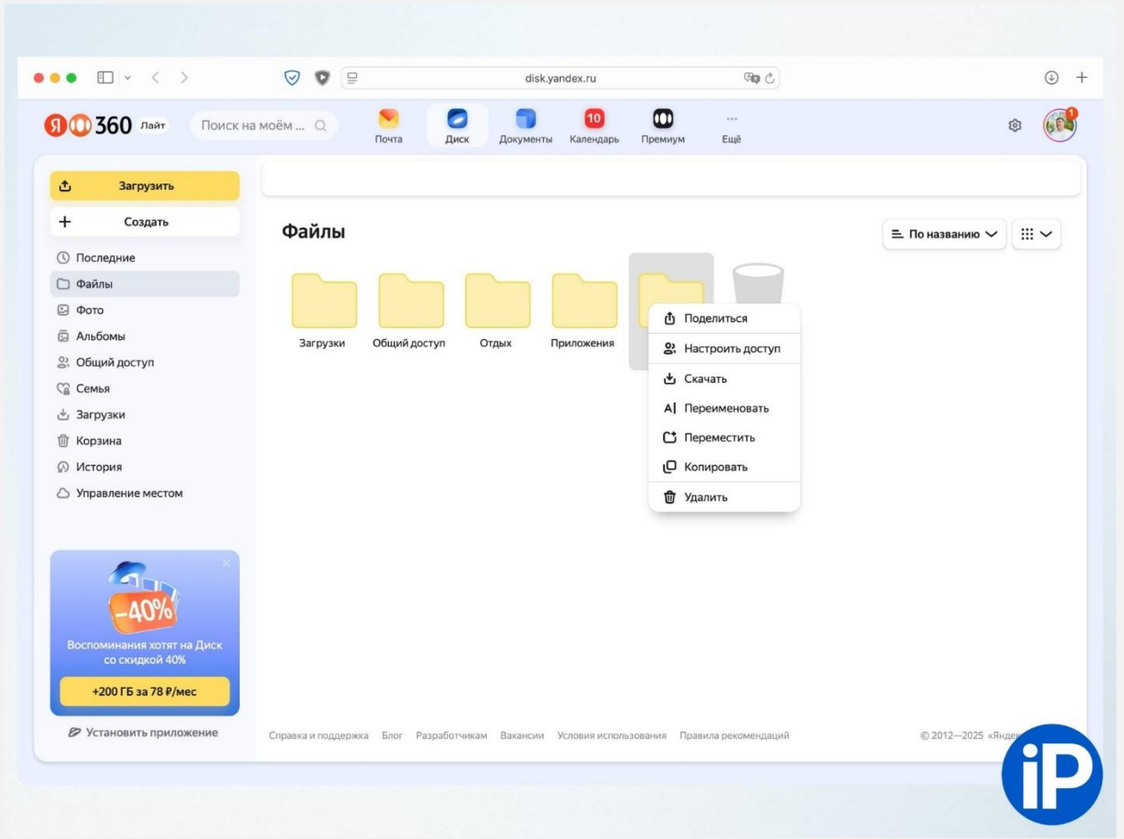
На Яндекс. Учебник выполнить следующие пункты:

Выполнение Урок 4. Облачное хранилище

1. Просмотр презентации «Облачное хранилище»
2. Выполнение заданий в рабочей тетради «Облачное хранилище»

1. Яндекс Диск





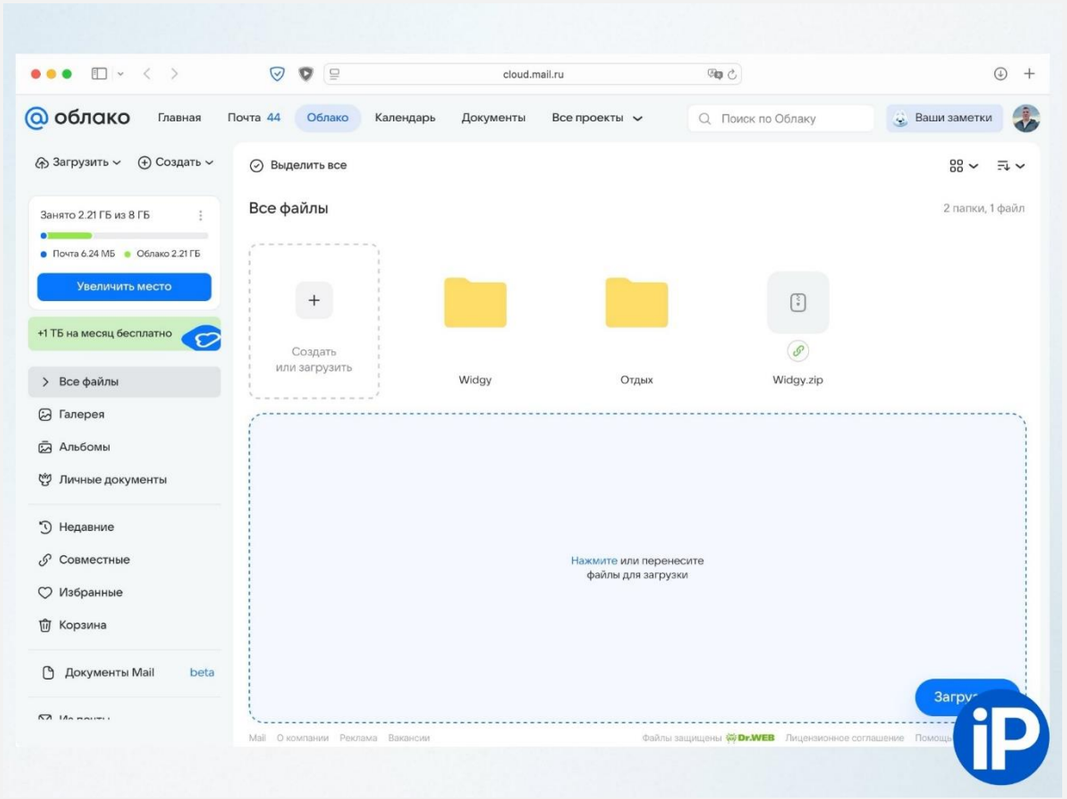
«Яндекс Диск» — облачный сервис, принадлежащий компании Яндекс, входит в экосистему сервисов «Яндекс 360». Позволяет пользователям хранить данные на серверах в «облаке» и передавать их другим пользователям в интернете.

Платформы: веб-версия, десктопный клиент для Windows, macOS и Linux, мобильная версия для iOS, Android и Windows Phone.

Безопасность

- Автоматически проверяет файлы встроенным антивирусом, проверяет даже содержимое заархивированных файлов (ZIP или RAR).
- Можно контролировать, кто сможет получить доступ к данным на «Диске» — например, предоставлять доступ только отдельным пользователям или по прямой ссылке.

2.Облако Mail



«Облако Mail» (ранее «Облако Mail.ru») — облачное хранилище данных российской компании VK. Позволяет хранить музыку, видео, изображения и другие файлы в облаке, синхронизировать данные на компьютерах, смартфонах или планшетах, а также делиться ими с другими пользователями интернета.

Адрес: cloud.mail.ru.

Платформы: веб-версия, приложения для Windows, macOS, iOS, Android.

Одной из уникальных функций сервиса стало приложение Disk-O. Он умеет собирать информацию на разных облаках с ее последующей синхронизацией в своем хранилище. Также можно создавать резервные копии.

Безопасность

- Распределённое хранение — файл загружается только один раз, а хранится в нескольких копиях на нескольких серверах, расположенных в России.
- Проверка файлов на вирусы — заражённые файлы блокируются и становятся недоступны для загрузки в хранилище.
- Двухфакторная аутентификация — вход в аккаунт в два этапа: сначала вводится обычный пароль, а потом одноразовый код из СМС или специального приложения.

3.СберДиск

«СберДиск» — российское облачное хранилище данных, разработанное Сбербанком. Подходит для хранения личных файлов (фотографий, документов, видео) и обмена ими с другими пользователями.

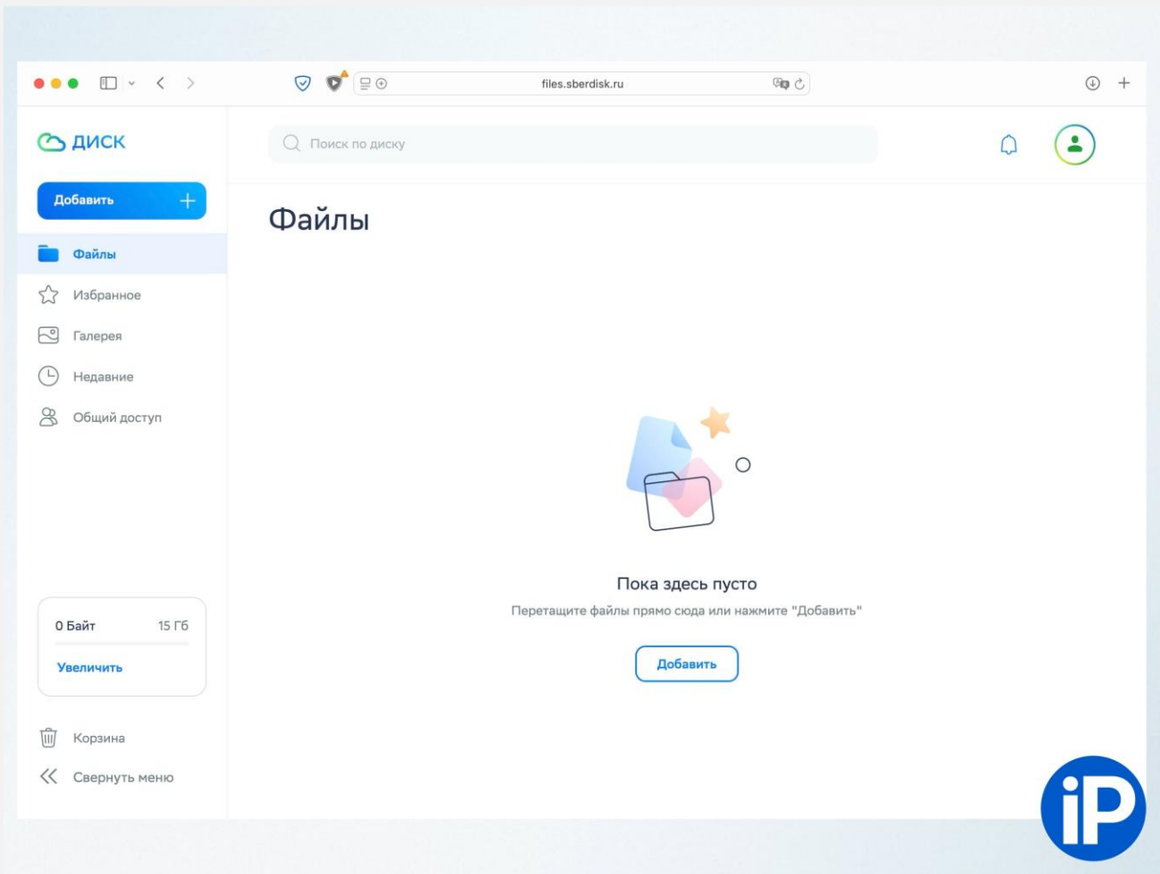
Сайт: sberdisk.ru.

Платформы: веб-версия, приложения для iOS и Android.

Чтобы начать пользоваться сервисом, необходимо зарегистрироваться в «СберID» по номеру телефона.

Безопасность

- Шифрование данных на стороне сервера, что обеспечивает защиту от хакерских атак и утечки данных.
- Многофакторная авторизация — совместное использование нескольких факторов снижает риск утечки данных (помимо пароля, применяются карты, сканеры отпечатков пальцев и другое).
- Резервное копирование данных в несколько независимых мест, что делает практически невозможным их потерю или повреждение.
- Соответствие федеральному закону №152-ФЗ — сбор персональных данных, их обработка и защита соответствуют этому закону.

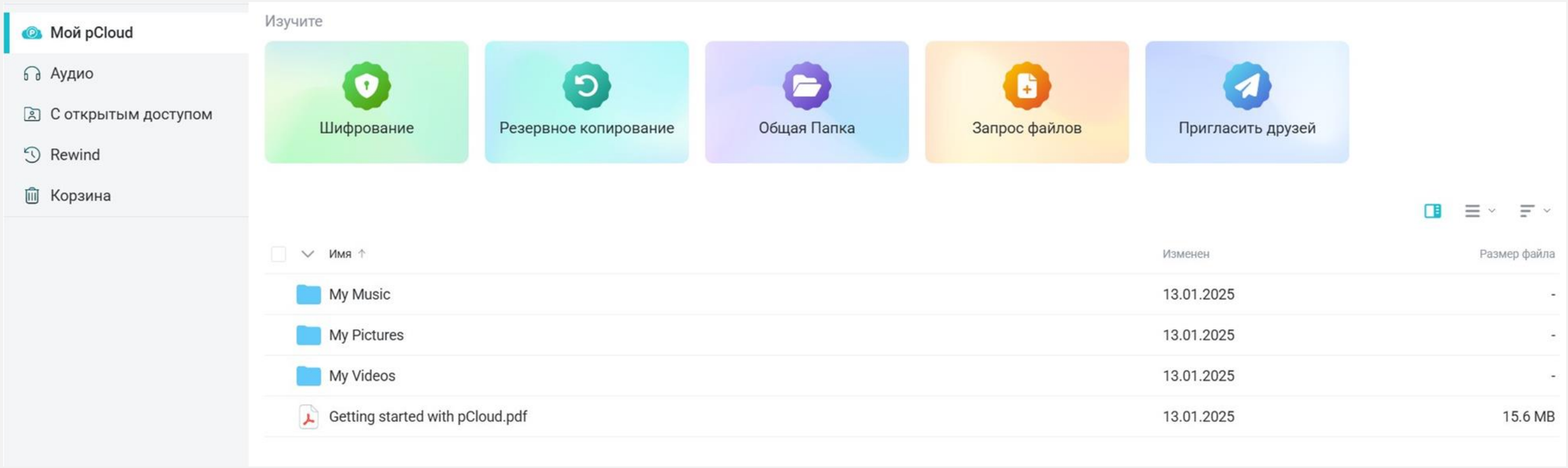


4.iCloud

iCloud — облачное хранилище данных, разработанное компанией Apple. Предназначено для хранения и синхронизации данных между устройствами Apple, такими как iPhone, iPad, Mac и другие.

Безопасность

- Данные в iCloud защищены шифрованием как при передаче, так и в хранении. Некоторые меры безопасности:
- Двухфакторная аутентификация — при входе с нового устройства система запрашивает дополнительное подтверждение через доверенное устройство или SMS-код.
- Контроль доступа приложений — в настройках iCloud можно отключить ненужные разрешения.
- Управление резервными копиями — нужно настроить автоматическое резервное копирование важной информации и периодически проверять актуальность сохранённых копий.



5.Google Диск

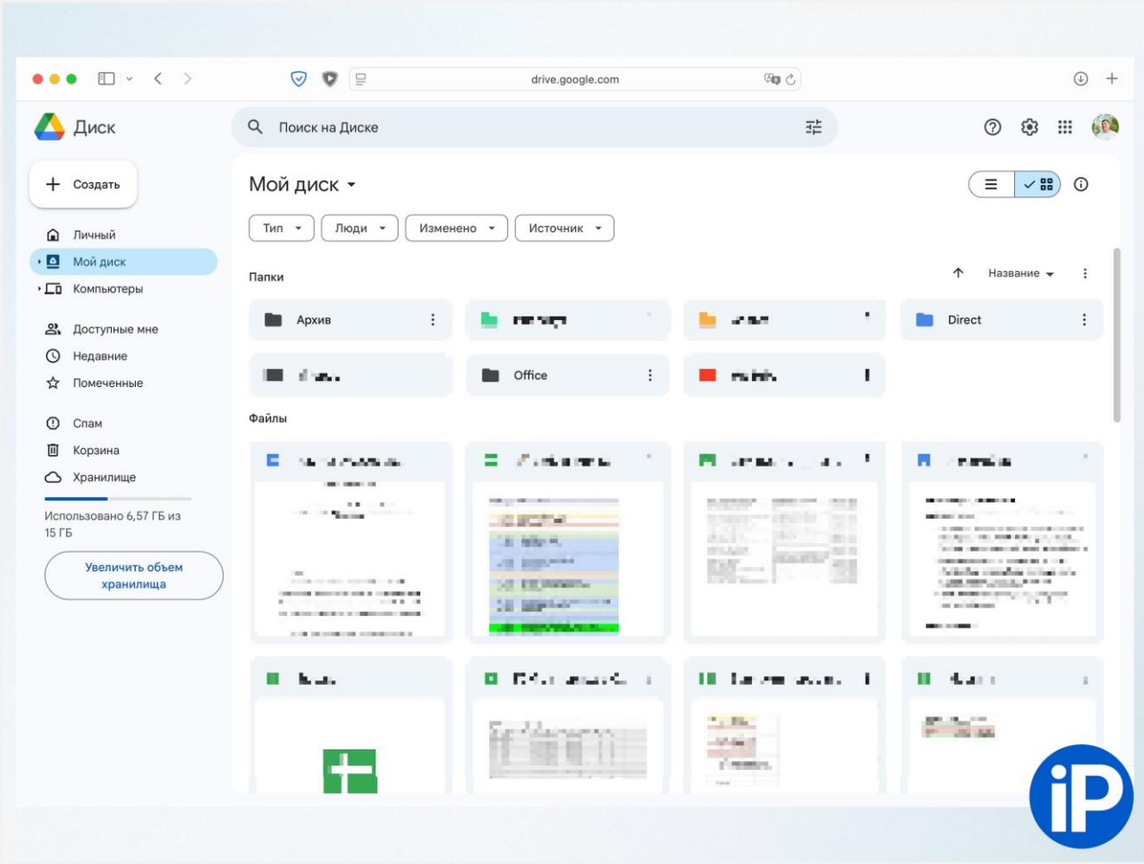
Google Drive («Google Диск») — облачное хранилище от компании Google, позволяющее пользователям сохранять файлы, управлять и делиться ими онлайн. Сервис был запущен в 2012 году.

Интегрирован с другими сервисами Google, такими как Google Docs («Документы»), Sheets («Таблицы»), Slides («Презентации») и Forms («Формы»).

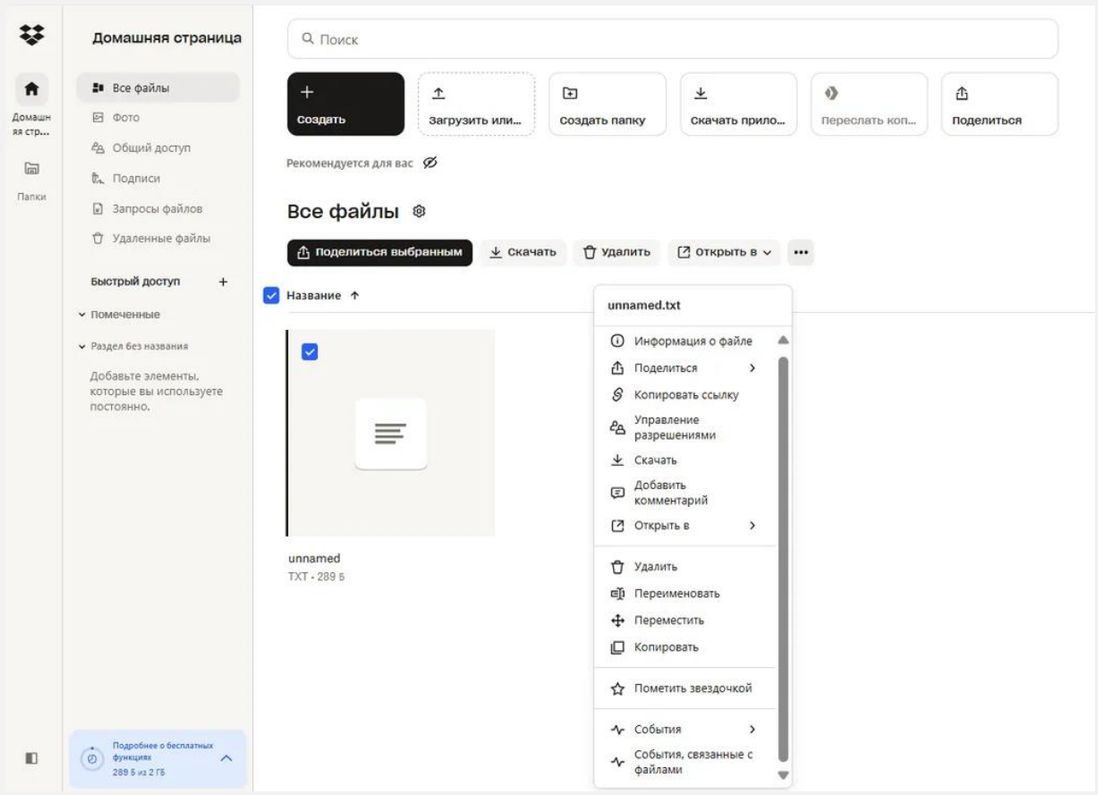
Файлы, размещённые в Google Drive, защищены современными протоколами безопасности. Некоторые меры безопасности:

Безопасность

- Шифрование — файлы шифруются с использованием расширенных стандартов шифрования AES-128 или AES-256.
- Двухфакторная аутентификация (2FA) — даже если злоумышленник узнает пароль, ему понадобится подтвердить вход с помощью SMS-кода или приложения-аутентификатора.



6.Dropbox



Dropbox — облачный сервис для хранения и обмена файлами, созданный в 2007 году Дрю Хьюстоном и Арашем Фердоуси. Это виртуальный диск, который синхронизируется между всеми устройствами пользователя через интернет-соединение.

Это один из наиболее популярных облачных сервисов для хранения информации. Здесь пользователи могут не только размещать файлы, но и редактировать фото, видео, файлы в формате PDF, синхронизировать пароли и подписывать документы ЭЦП.

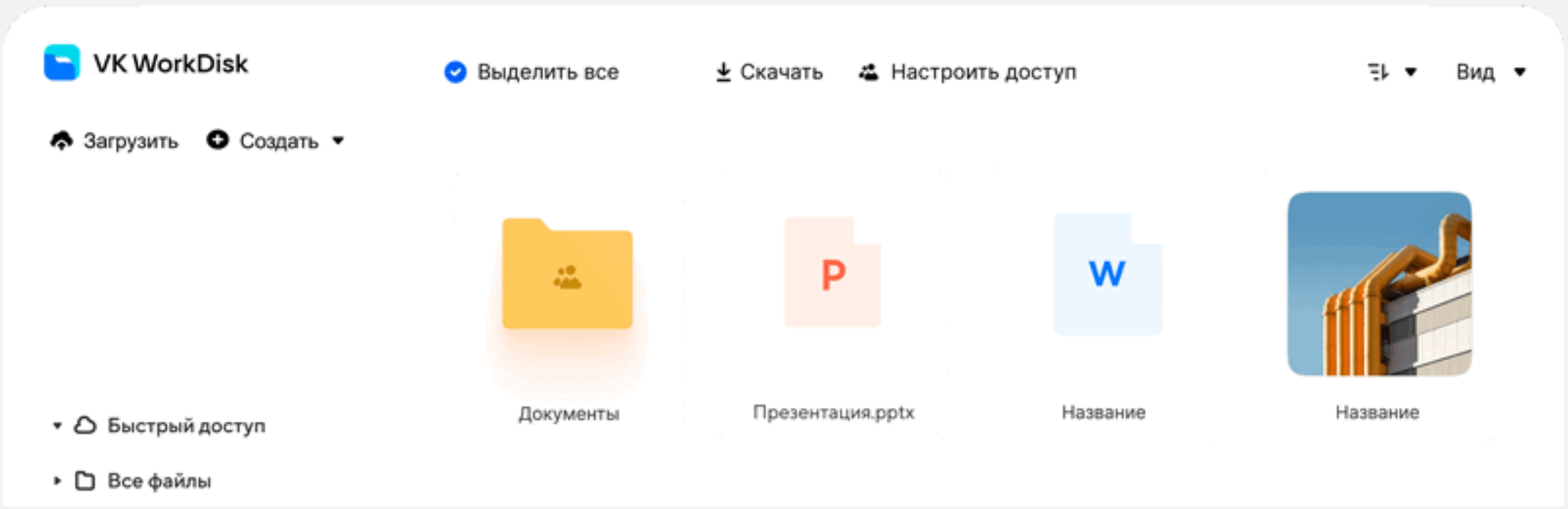
Максимально допустимый размер загружаемого файла ограничивается только размером самого хранилища, но при этом не может быть больше 2 Тб для приложения или 350 Гб для сайта.

7.VK WorkDisk

VK WorkDisk — облачное хранилище данных для корпоративного использования, разработанное компанией VK. Входит в цифровую экосистему VK WorkSpace.

Безопасность

- Шифрование данных при передаче и хранении.
- Многофакторная авторизация — совместное использование нескольких факторов снижает риск утечки данных (помимо пароля, применяются карты, сканеры отпечатков пальцев и другое).
- Резервное копирование в нескольких местах — это делает практически невозможным потерю или повреждение данных.



ПРАВИЛА

Использовать одну основную версию документа — создать главный файл и передать ссылку на него сотрудникам.

Вводить систему именования файлов — это поможет избежать путаницы и найти нужный файл.

Регулярно архивировать важные версии — сохранять старые версии документа в отдельной папке, чтобы они не мешали текущей работе, но при этом были доступны для обращения в будущем.

Настроить оповещения о изменениях — это поможет держать команду в курсе всех правок и изменений.

БЕЗОПАСНОСТЬ

Использовать шифрование — это защищает данные от несанкционированного доступа.

Ограничивать доступ к информации — например, давать каждому сотруднику минимальные права, необходимые для выполнения его обязанностей.

Создавать резервные копии — это поможет защитить данные от потери, если облачный сервис выйдет из строя по причине сбоя в системе, атаки вирусов или неправильной работы программного обеспечения.