



Сохранность личной информации

6 ГЛАВА

Несем устройство в ремонт

Если ваш компьютер или телефон сломался, единственный выход — нести его в мастерскую. Но перед этим нужно обратить внимание на два момента:

1. Насколько профессиональны мастера, которым вы отдаете устройство для ремонта.
2. Необходимо установить защиту данных, которые находятся на компьютере или смартфоне.

Не идите в первый попавшийся или самый разрекламированный сервисный центр. Поинтересуйтесь рекомендациями ваших знакомых. Возможно, кто-то уже пользовался услугами по ремонту.

Если вы ищете ремонтную мастерскую через интернет, почитайте отзывы о данной компании и только потом принимайте решение.

Когда будете сдавать устройство в ремонт, вам должны выдать квитанцию приема-выдачи оборудования.

В квитанции должны быть:

- дата;
- ФИО и подпись ваша и приемщика;
- подробное описание неисправности;
- описание технического и визуального состояния устройства;
- указание модели, серийного номера, IMEI.

Некоторые специалисты рекомендуют сделать фотографии вашего устройства на момент сдачи в ремонт.



После диагностики обычно озвучивают точную сумму ремонта. Если же после диагностики вам снова называют приблизительную стоимость и приблизительный срок ремонта, примерный срок гарантии, то, возможно, это сигнал поискать другую ремонтную мастерскую.

На что обратить внимание, если необходимо отнести устройство в ремонт:

1. Выбор ремонтной мастерской.
2. Защита конфиденциальной информации, которая есть на устройстве.

Варианты, как защитить свои данные при сдаче компьютера в ремонт:

1. Воспользоваться командой «Сделать резервную копию», а затем удалить все данные с компьютера.
2. Зашифровать жесткий диск.
3. Вручную скопировать приватные папки и файлы, затем удалить их с устройства.
4. Попросить в ремонтной мастерской при вас вытащить накопительный диск и забрать его.

Обязательно уточняйте: какие работы будут проведены, за какую сумму, в какие сроки и каков период гарантии.

Когда будете принимать устройство, обязательно проверьте его работу и осмотрите визуально. И только после этого принимайте и подписывайте акт выполненных работ.

Если неисправность устройства не ограничивает вам доступ к личным данным, то стоит провести ревизию. Внимательно посмотрите, что нужно обязательно удалить (при этом не забыть сохранить эту информацию на флеш-накопителе), а что можно оставить.

Есть несколько вариантов:

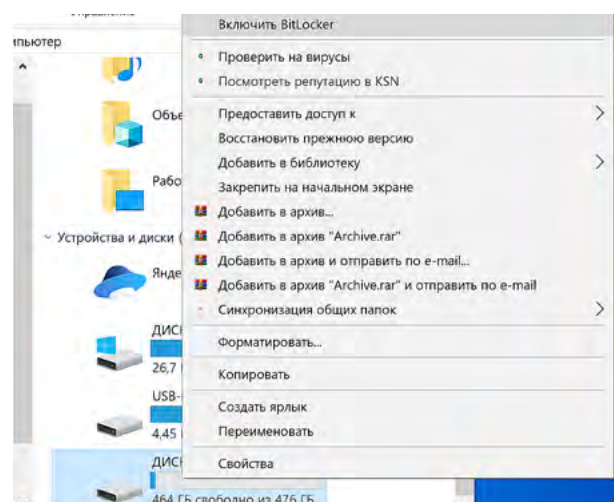
- воспользоваться командой «Сделать резервную копию» и так перенести данные на флешку, а затем удалить все с компьютера (в смартфоне это процесс проще);
- вручную перенести нужные данные на внешний накопитель (флешку) и затем удалить файлы и папки, которые скопировали;
- зашифровать жесткий диск;
- попросить при вас вытащить из компьютера SSD-накопитель (диск внутри компьютера, на котором хранится информация) и забрать его с собой.

Шифрование жесткого диска

Один из вариантов решения для защиты своих данных — шифрование жесткого диска. В Windows есть технология **BitLocker**. Программа уже встроена в операционную систему и проста в использовании:

- перейдите в «Пуск»;
- затем зайдите в раздел «Проводник»;
- выберите «Этот компьютер» или «Мой компьютер»;
- выберите диск, который намерены зашифровать, например, диск D;
- наведите на диск курсор и нажмите правую кнопку мыши;
- в выпавшем меню кликните по команде «Включить BitLocker» 6.1.

6.1

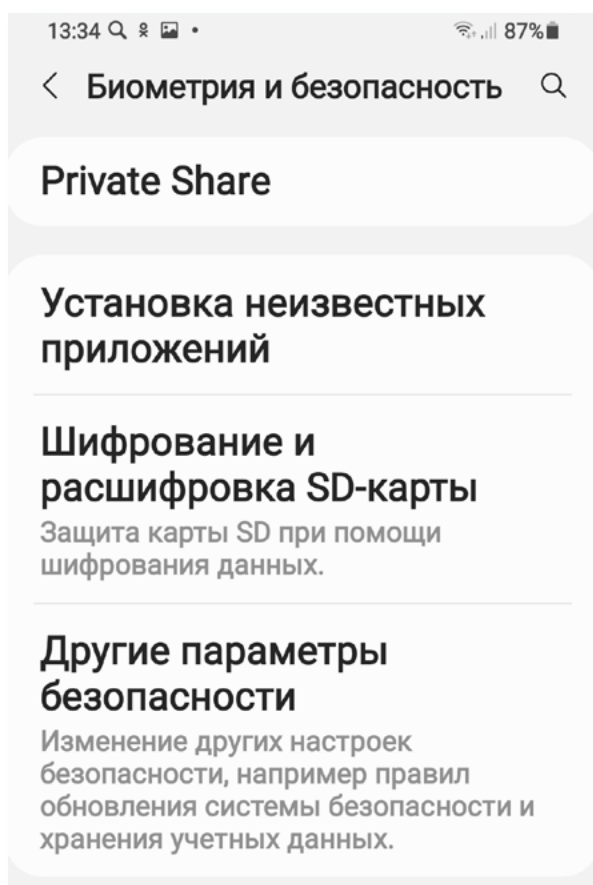


Далее понадобится придумать надежный пароль. Обязательно запишите его. Теперь при каждом входе на диск компьютер будет спрашивать пароль.

В операционной системе **Альт (Alt Linux)** также можно зашифровать папки. Для этого нужно:

- открыть **«Точка входа»** (значок папки на нижней панели);
- выбрать **«Рабочий стол»**;
- далее выбрать нужную папку в списке, навести на нее курсор и нажать правую кнопку мыши;
- в меню выбрать **«Свойства»**;
- далее — вкладку **«Публикация»**;
- нажать **«Создать пароль Samba»**;
- придумать и ввести пароль;
- подтвердить действие.

В смартфоне также есть возможность шифрования данных. На некоторых моделях таким образом можно зашифровать доступ ко всем данным смартфона, а на других — только доступ к SD-карте. Для подключения шифрования в операционной системе Android в **«Настройках»** нужно перейти в раздел **«Биометрия и безопасность»** и выбрать пункт **«Шифрование и расшифровка SD-карты»** (в нашем примере) 6.2.



6.2

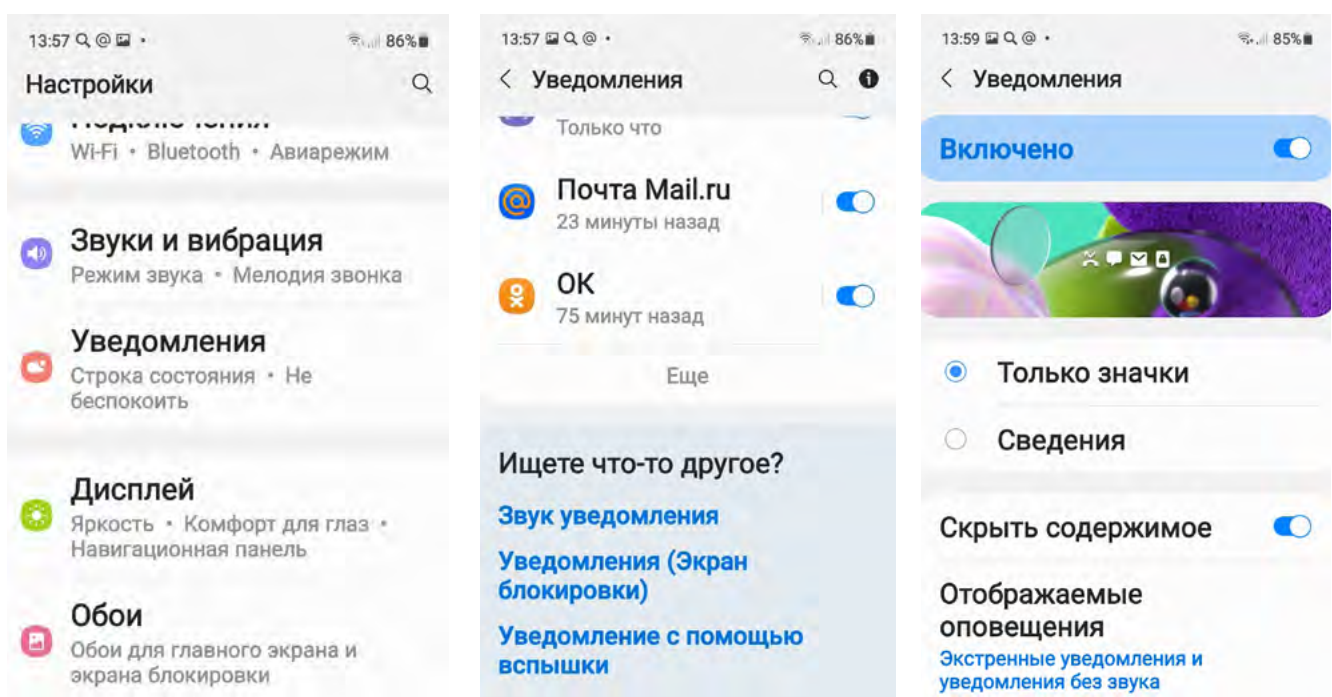
В различных моделях и версиях смартфонов раздел может называться по-разному. Может быть просто **«Безопасность»**, например.

Принцип тот же, что и в компьютере. Нужно будет подтвердить ваше намерение зашифровать данные и придумать надежный пароль. Теперь каждый раз, чтобы получить доступ к информации на SD-карте, нужно будет вводить пароль. Есть и программы, которые позволяют зашифровать данные на смартфоне.

Будет полезным поставить вход по биометрии, по отпечатку пальца (Touch ID). В этом случае при блокировке экрана все данные в смартфоне также находятся в зашифрованном виде. При этом на главном экране могут отображаться уведомления. Их необходимо отключить.

Для этого перейдите в «**Настройки**», выберите пункт «**Уведомления**», внизу кликните по строке «**Уведомления (Экран блокировки)**». Выключите показ уведомлений (передвиньте влево ползунок около надписи «**Включено**») 6.3.

6.3



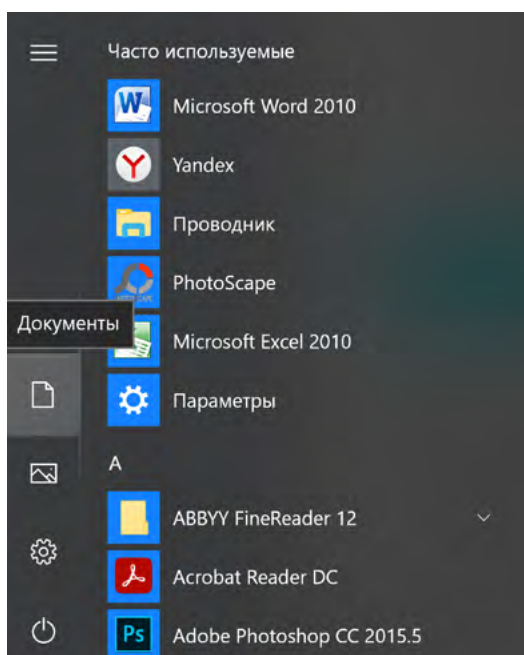
Копирование и удаление важной информации вручную

Но, конечно, шифрование дисков и данных — это возможность сохранить информацию для более продвинутых пользователей.

А вот один из самых простых способов защиты данных — провести ревизию содержимого вашего компьютера и выбрать файлы, которые нужно скопировать на внешний накопитель (флешку), а с компьютера удалить:

- нажмите «**Точка входа**» (в ОС Альт), «**Пуск**» (в Windows);
- затем выберите «**Рабочий стол**» (в ОС Альт), «**Компьютер**» (в Windows 7), «**Проводник**» или «**Документы**» (в Windows 10) 6.4;

6.4



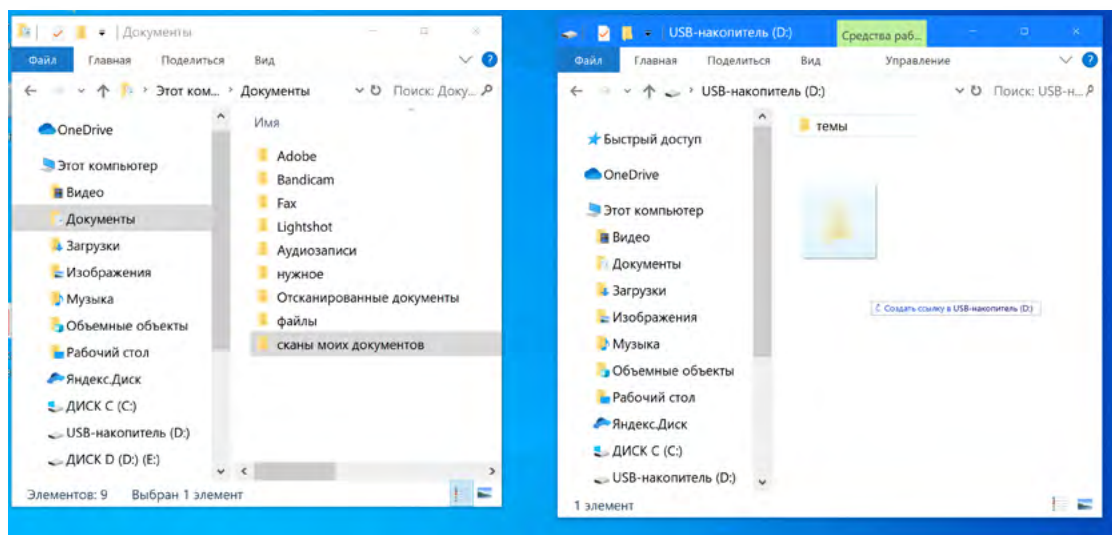
- в меню слева можно перейти в папки, которые есть на компьютере, и выбрать, какие вы будете удалять, а какие оставлять. Обратите внимание на папки или файлы, где есть записанные пароли от разных интернет-ресурсов (помните, что храниться на компьютере такая информация может только в зашифрованном виде).

Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность»

Проверьте, не хранятся ли на компьютере ваши личные данные (сканы паспортов, других документов, где есть данные вашего СНИЛС, ИНН, адреса электронной почты). Примите во внимание потенциально компрометирующие вас файлы, если таковые есть.

Вставьте внешний накопительный USB-диск (флешку). Откройте его на компьютере и скопируйте сюда файлы и папки, которые не должны попасть в поле зрения посторонних. Можно просто открыть два окна и мышкой перетащить файлы из одного в другое 6.5.

6.5



После того, как вы скопировали нужные данные на флешку, можно удалить папки и файлы с компьютера.

Также в браузере стоит полностью очистить историю вместе с куки-файлами и данными форм сайтов. Для этого в настройках браузера нужно перейти в историю просмотров.

Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность»

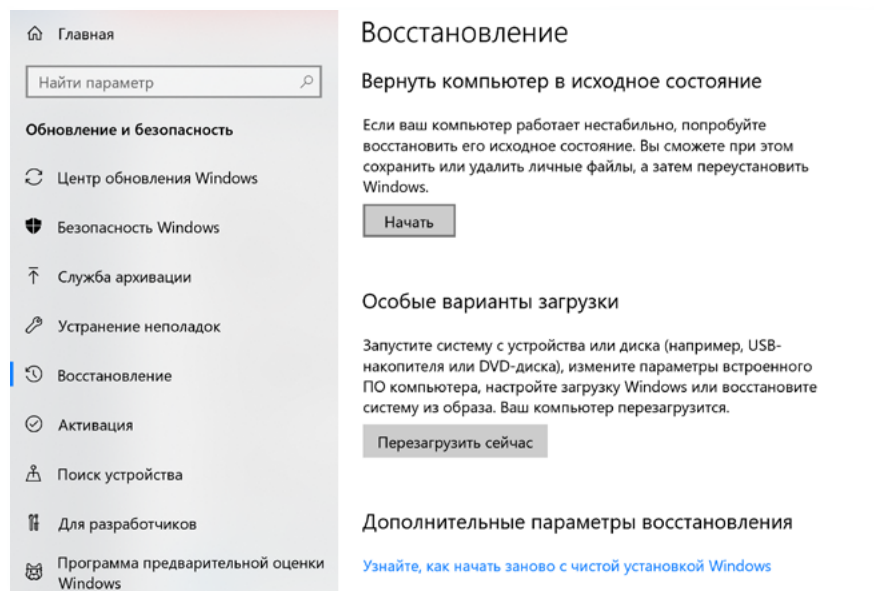
Для списка паролей в браузере лучше включить функцию **«Мастер-пароль»**. Выйдите из электронной почты, аккаунтов социальных сетей, браузера, личного кабинета на Госуслугах и других сайтах, где вы проводите оплату. При этом позаботьтесь о сохранении логинов и паролей. Лучший вариант — менеджер паролей.

Можно вообще полностью удалить все ваши данные с компьютера и вернуть его к заводским настройкам. Такой вариант может понадобиться, если вы решили продать устройство.

Чтобы удалить всю информацию на Windows 10:

- нажмите **«Пуск»**;
- выберите **«Параметры»**;
- затем блок **«Обновление и безопасность»**;
- в левом меню выберите **«Восстановление»**;
- в блоке **«Вернуть компьютер в исходное состояние»**;
- нажмите **«Начать»** 6.6;

6.6



- далее нужно будет выбрать удаление всех файлов и папок и возвращение к исходным заводским настройкам.

! При возврате к заводским настройкам будут удалены все программы, которые были установлены пользователем на компьютер, останутся только предустановленные.

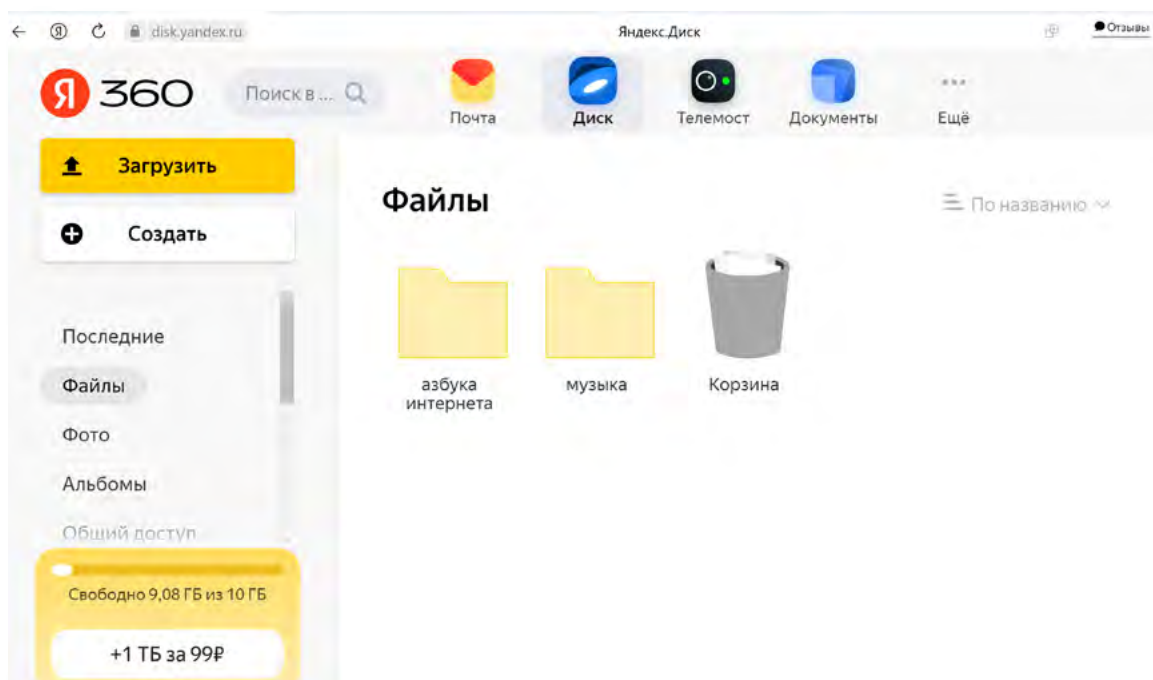
Резервное копирование и облачные сервисы для сохранения ваших данных

Можно также воспользоваться встроенными в операционную систему программами и провести резервное копирование всей информации на устройстве.

При этом скопировать данные можно на внешний накопитель с большим объемом памяти (от 128 ГБ и более), так как на устройстве хранится немало данных. Например, те же фотографии и видео могут занимать большой объем памяти.

Но сейчас все чаще для резервного копирования используют **облачные хранилища**. Это удаленные архивы информации, которые хранятся в сети интернет постоянно. Доступ к тем или иным хранилищам предоставляют различные интернет-ресурсы.

Такие облачные хранилища сегодня есть практически при каждом почтовом сервисе и поисковой системе (**Яндекс Диск** у Яндекс Почты [6.7.](#), **Облако Мэйл** у Мэйл Почты, **Гугл Диск** у Гугл Почты и т.д.), у операционных систем Windows — **OneDrive** (Вандрайв), у iOS (операционной системы устройств Apple) — **iCloud** (Айклауд), у Самсунг — **Samsung Cloud** (Самсунг Клауд).



6.7

Это удобно, ведь для регистрации в электронной почте, смартфоне или на компьютере вам предлагается авторизоваться. Практически тут же вы получаете доступ к облачному хранилищу и можете зайти в него с любого устройства в любое время. Вы можете что-то сохранить на компьютере в облаке, а потом посмотреть эти файлы уже с планшета или смартфона.

Например, у Айфона по умолчанию стоит резервное копирование. Оно позволяет, например, не переносить контакты и всю информацию вручную с одного смартфона на другой, если вы решили поменять модель смартфона.

Резервное копирование на компьютере в операционной системе Windows или в ОС Альт выполнить несколько сложнее, чем на смартфоне или планшете. Здесь понадобятся навыки продвинутого пользователя.

Можно попросить сделать резервную копию и затем полностью очистить компьютер при вас в мастерской. Для этого стоит принести с собой внешний диск. Лучше, если он будет объемом от 128 ГБ до 1 ТБ — чем больше, тем лучше. Больше шансов, что вся резервная копия на нем уместится. И затем также в мастерской, принимая устройство после ремонта, можно попросить при вас восстановить данные. Возможно, что услуга будет платной.

На смартфоне или планшете сделать резервную копию возможно и пользователю, имеющему только базовые навыки работы на устройстве.

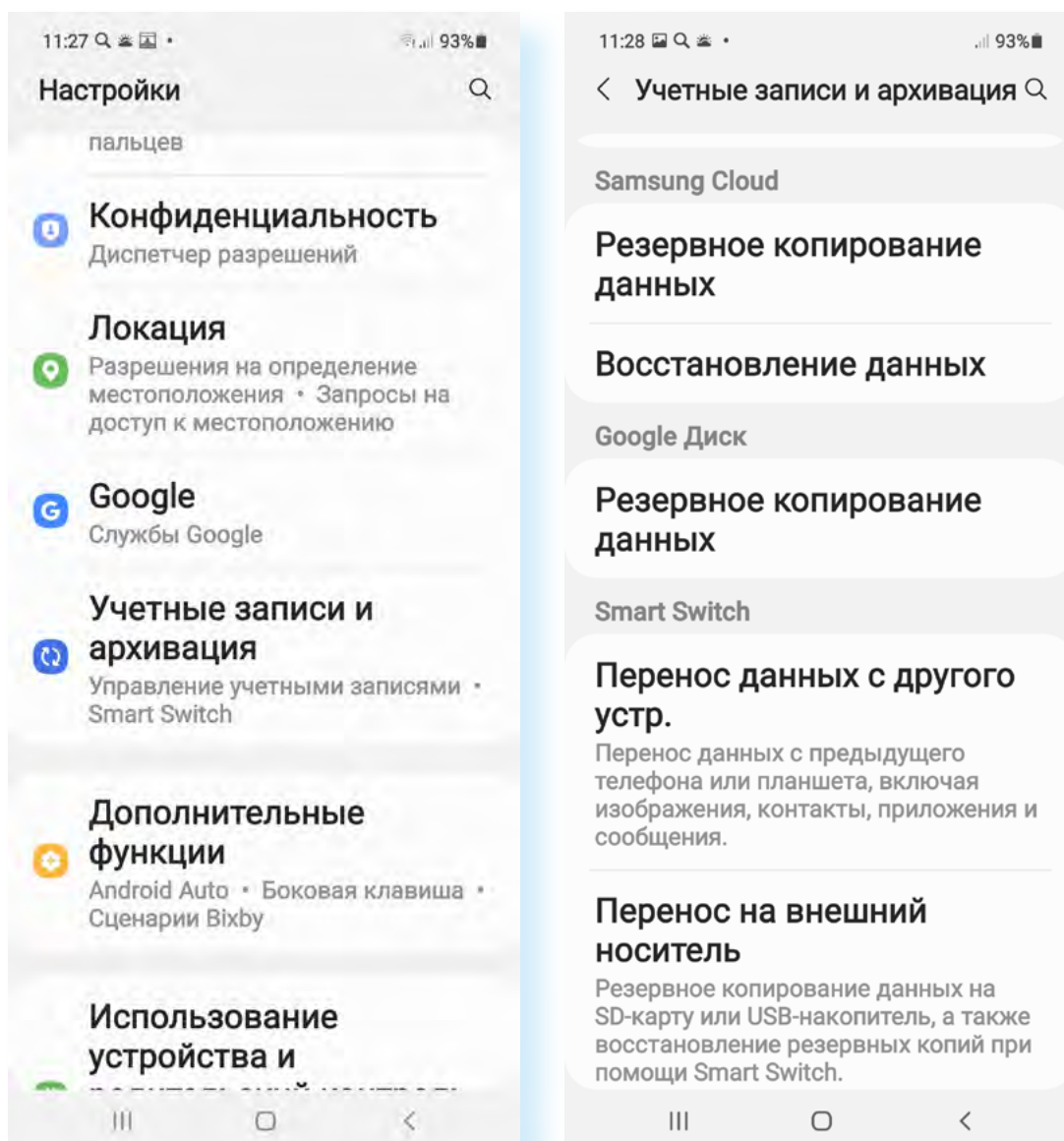
Принцип такой же: создаете резервную копию, а затем удаляете всю информацию с устройства. Именно на мобильных устройствах это нужно сделать обязательно. На смартфоне, как правило, установлены разные приложения — личные кабинеты в банках, социальных сетях, Госуслугах и прочее. Бывают случаи, что, отдавая смартфон в ремонт, обратно пользователь получает телефон с основательно подчищенными банковскими счетами и, возможно, даже с новыми кредитами, оформленными онлайн от вашего имени. А если еще в смартфоне активирован и бесконтактный модуль оплаты и система финансовых расчетов (например, **Mir Pay**), то риски попасть в неприятную ситуацию увеличиваются.


Подробнее о системе финансовых расчетов в главе 5 «Финансовые расчеты через приложения» модуля 8 «Работа с мобильными приложениями» расширенного курса «Азбука интернета»

Чтобы сделать резервную копию на смартфоне:

- откройте приложение **«Настройки»**;
- перейдите в раздел **«Учетные записи и архивация»** (на различных моделях смартфонов раздел может иметь другие названия);
- далее нужно выбрать, куда поместить резервную копию. В нашем варианте предлагаются облачные хранилища **Samsung Cloud** и **Google Диск** или перенос информации на внешний носитель **6.8**.

6.8

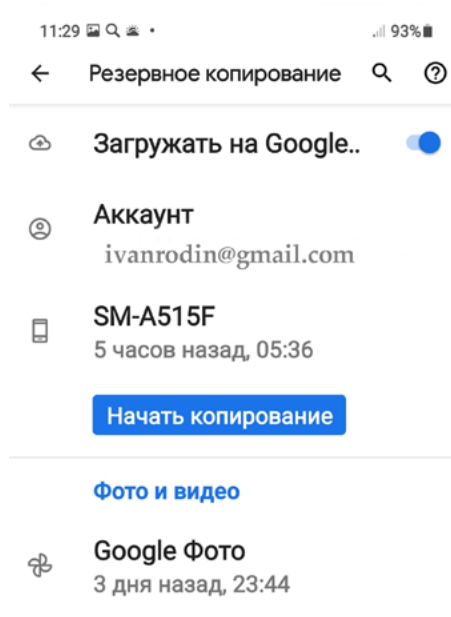


В том случае, если вы приняли решение сделать резервную копию на внешнем накопителе (флешке), ее нужно будет подключить к устройству. 

Обычно смартфоны с операционной системой Андроид привязаны к **Google Диску**, поэтому резервное копирование можно сделать в это облачное хранилище. Нажмите в блоке **Google Диск** пункт «**Резервное копирование данных**». Здесь обозначен ваш аккаунт на Google (адрес электронной почты), логин и пароль от которого также будут являться данными для входа в облачное хранилище **Google Диск**.

Для того, чтобы создать резервную копию, нужно нажать «**Начать копирование**» [6.9](#).

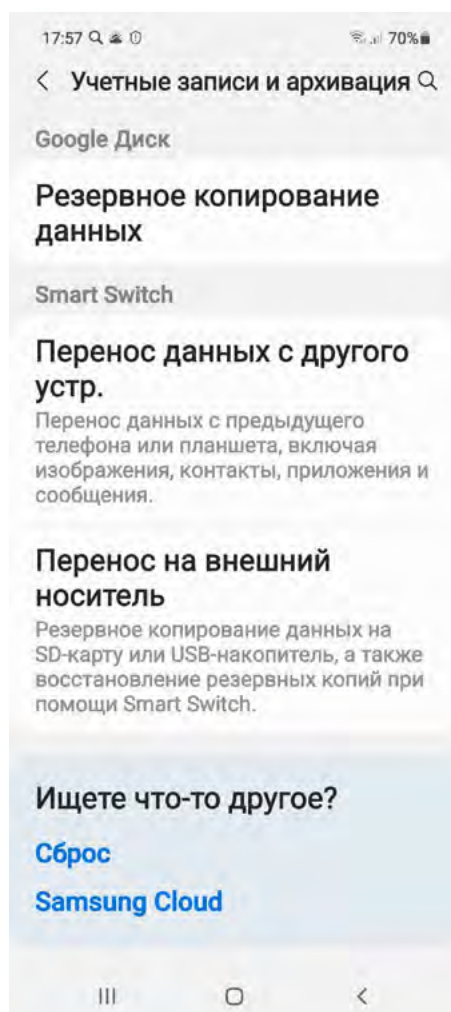
6.9



Это займет какое-то время. Дождитесь завершения процесса.

После этого можно провести сброс всех параметров. Перейдите в «Настройки», в раздел «Учетные записи и архивация». Внизу найдите пункт «Сброс» 6.10.

6.10



Далее нужно выбрать «Сброс всех параметров» или «Сброс данных».

На следующей странице можно посмотреть, какие данные будут стерты, и нажать команду на сброс всех настроек.

Чтобы затем восстановить данные на устройстве, при авторизации нужно ввести логин и пароль вашей учетной записи, в которой вы проводили резервное копирование данных.

В целом, функция резервного копирования данных будет полезна не только при ремонте, а еще, например, в случае потери устройства. Зайдя в аккаунт Google, можно удаленно стереть данные с потерянного устройства и восстановить все данные на новом смартфоне.

Что делать, если взломали ваш аккаунт

Сегодня почти у каждого человека есть аккаунты в социальных сетях, зарегистрированы электронные почтовые ящики, есть личные кабинеты в интернет-магазинах. И, как следствие, есть вероятность, что вашу почту или аккаунт в социальных сетях взломают. Как понять, что это случилось? Например, вы не можете войти в свою учетную запись, потому что изменился пароль.

Главное в этой ситуации — оценить, какие данные могут попасть в руки мошенников, и постараться минимизировать потери. Безусловно, нужно предупредить друзей и знакомых, что у вас взломали почту или страничку в соцсети, и что не нужно отвечать на письма и сообщения, которые могут в этот момент приходить якобы от вас.

Обязательно нужно постараться восстановить контроль над учетной записью.

Первым делом попробуйте воспользоваться сервисом восстановления пароля. Есть шанс, что мошенники не успели отвязать от аккаунта вашу почту или номер мобильного телефона.

Если не получается это сделать, обратитесь в службу поддержки, разъясните ситуацию.

Если мошенники смогли добраться до аккаунта в какой-то платежной системе или интернет-банкинге, звоните в банк и просите заблокировать вашу карту или аккаунт.

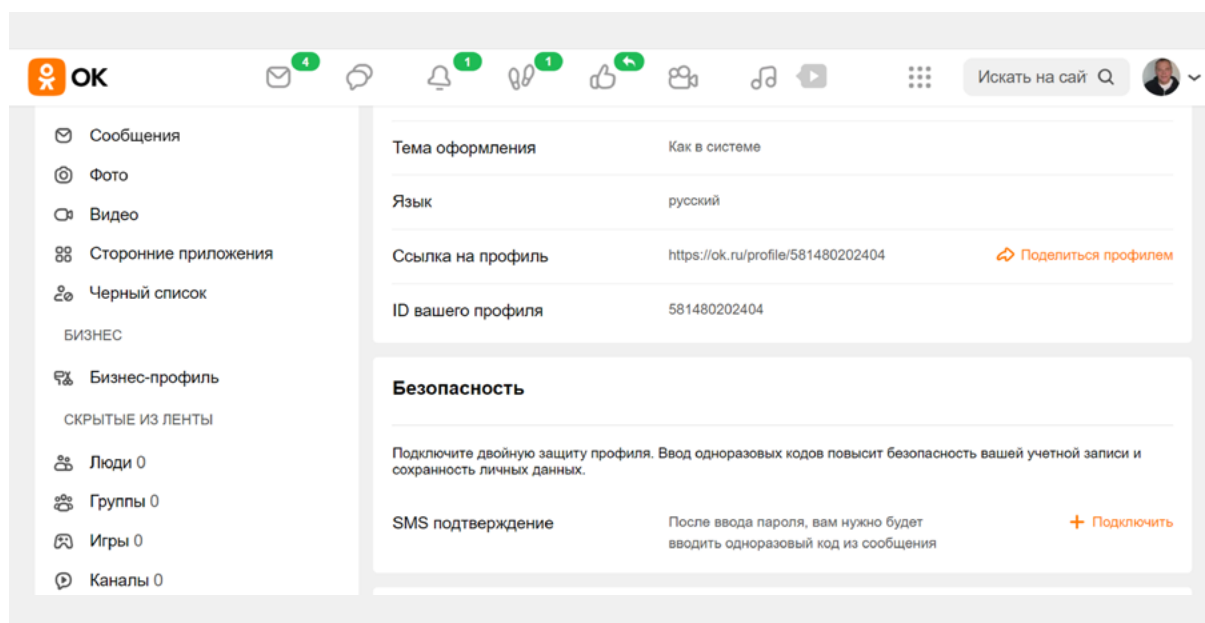
Если взломали электронный почтовый адрес, постарайтесь вспомнить, где еще вы его вводили для регистрации — ведь ссылки для восстановления пароля на таких сервисах будут приходить именно на эту почту. Зайдите во все сервисы и постарайтесь изменить электронную почту или отвязать от учетной записи взломанный адрес.

Поменяйте пароли в тех сервисах, где вы использовали тот же пароль, что и от взломанного аккаунта. А еще лучше сразу настройте **двухфакторную аутентификацию** — подтверждение входа в учетную запись двумя разными способами (например, ввод логина и пароля и кода проверки, который приходит на мобильный телефон или электронную почту).

Подробнее в главе 5 «Система надежных паролей» модуля 10 «Кибербезопасность» расширенного курса «Азбука интернета».

Если вам удалось восстановить доступ к взломанному аккаунту, сразу поменяйте пароль, ответьте на контрольные вопросы и настройте двухфакторную аутентификацию. Например, вот так выглядит страница настройки дополнительной защиты аккаунта в **Одноклассниках 6.11**.

6.11



Для того, чтобы настроить доступ к взломанному аккаунту в соцсети, нужно:

1. Нажать на значок профиля вверху справа.
2. В открывшемся меню зайти в «Изменить настройки».
3. Выбрать слева «Основное».
4. В блоке «Безопасность» нажать «Подключить».
5. Следовать инструкции на экране.

Если настроить ее, то при каждом входе в профиль на ваш мобильный телефон, связанный с учетной записью в **Одноклассниках**, будет приходить sms-сообщение с кодом. Только после ввода данного кода вы сможете войти на свою страницу.

Чтобы настроить данную опцию в соцсети, нужно:

1. Нажать на значок профиля вверху справа.
2. В открывшемся меню зайти в «Изменить настройки».
3. Выбрать слева «Основное».
4. В блоке «Безопасность» нажать «Подключить».
5. Следовать инструкции на экране.

Многие сервисы информируют о подозрительной активности в вашем аккаунте. Если вы увидели такое письмо, никогда не переходите по указанной в нем ссылке. Это может быть и письмо от мошенников. Зайдите в аккаунт, набрав адрес в строке браузера, и, как минимум, поменяйте пароль и настройте сервисы безопасности. Также можете проверить историю входов. Такую функцию предоставляют сегодня многие порталы. Если увидите, что в ваш аккаунт зашли с незнакомого устройства, нажмите команду «**Выйти из всех устройств**».

Например, на **Госуслугах**, чтобы увидеть историю входов в ваш аккаунт, нужно:

- вверху справа нажать значок профиля;
- нажать пункт «Профиль»;
- слева выбрать раздел «Безопасность»;
- справа на странице вкладку «Действия в системе» 6.12.

The screenshot shows the 'Госуслуги' (Gosuslugi) website interface. The user is logged in as 'Гражданин РФ'. The navigation menu includes 'Услуги', 'Документы', 'Заявления', 'Платежи', and 'Помощь'. The main content area is titled 'Действия в системе' (System Actions). It features a section for logging out on other devices with a 'Выйти' button. Below this is a filter section with 'Период' (Month) and 'Действие' (All) dropdowns, and a 'Скачать' button. A table lists system actions with columns for Date, Action, Status, IP, and Device.

Дата	Действие	Статус	IP	Устройство
20.10.23 16:19:47	Вход в систему Портал государственных услуг Российской Федерации Авторизация по номеру телефона. Личный кабинет физического лица	Успешно		Windows, Яндекс.Браузер

Бывают случаи, когда вам приходит сообщение от мошенников, в котором они сообщают, что заразили ваш компьютер вирусом и полностью отслеживают все ваши перемещения, более того, записали на веб-камеру компромат или скопировали переписку и, угрожая опубликовать данные, требуют выкуп.

Скорее всего, никто ничего не взламывал, а это просто вымогатели рассылают письма всем подряд из какой-нибудь купленной базы адресов. Нужно проверить компьютер на вирусы любой антивирусной программой-сканером. Проверку на вирусы часто предлагают установить бесплатно. На всякий случай поменяйте пароль доступа к электронной почте и включите двухфакторную аутентификацию.

Контрольные вопросы

1. Что делать, если ваш аккаунт взломали?
2. Как на мобильном телефоне сделать резервную копию устройства?
3. Где могут храниться резервные копии информации с устройства?
4. Зачем нужна система резервного копирования?
5. Как вручную можно почистить компьютер?
6. Можно ли зашифровать папку или файл на компьютере?
7. Что нужно учесть при необходимости сдать компьютерное устройство в ремонт?