

Сигурност и архивиране на данни

Защита на информацията и възстановяване в Windows

Сигурността на информацията е важна част от работата с компютърните системи. При използване на операционната система могат да възникнат загуба на данни, повреда на системни файлове, неотризиран достъп или заразяване със зловреден софтуер. Средството за защита се избира според конкретния риск.

В този урок ще създавате и проверявате резервно копие, ще разграничавате средствата за възстановяване и ще проверявате настройките за достъп и мрежова защита. Ще обяснявате необходимите действия на друг потребител.

1 Архивиране на данните

Архивирането за резервно съхранение (backup) е създаване на отделно копие на информацията. Целта е данните да могат да се възстановят при случайно изтриване, повреда на носител, софтуерен проблем, кражба или атака. То се извършва предварително и редовно.

Думата „**архив**“ се използва и за файл като ZIP или 7z, който обединява файлове и може да намали обема им чрез компресиране. Компресирането само по себе си не създава защита от загуба. ZIP файл, съхранен единствено на същия диск като оригиналите, може да се загуби заедно с тях.

Как се организира резервното съхранение

- Определят се важните файлове, мястото за копието, периодичността и срокът за пазене на старите версии.
- Използва се отделен носител или подходяща услуга: външен диск, мрежово хранилище или облачно резервно съхранение. Папка на същия физически диск не защитава от повредата му.
- Копието се защитава с права за достъп; при чувствителни данни се използва криптиране. Част от копията се пазят отделно или изключени от компютъра, за да не се засегнат от същата атака.
- Проверява се възстановяването на файл, а не само наличието на папка с копия. Записват се датата, обхватът и резултатът от проверката.

Синхронизацията поддържа еднакви файлове на различни места и може да пренесе изтриване или повредена версия. При облачна услуга се проверяват историята на версиите, кошчето и срокът за възстановяване. Резервното съхранение изисква възстановима предишна версия.

Копие на файлове и системен образ

Резервното копие на данни съдържа избраните потребителски файлове. Системният образ (system image) е копие на избраните системни дялове и може да включва ОС, приложения, настройки и данни. Възстановяването му може да замени текущото съдържание с това към датата на образа. Обхватът се проверява преди използване.

2 Средства за архивиране и възстановяване

System Restore

System Restore (Възстановяване на системата) връща системни файлове, системния регистър и настройки към състояние от по-ранна точка за възстановяване (restore point). Това може да помогне след проблемна инсталация, актуализация или промяна на драйвер.

Точките могат да се създават автоматично при определени системни промени или ръчно, когато защитата на системата е включена. Възстановяването не е предназначено за изтрити лични документи; може да премахне приложения или драйвери, инсталирани след избраната точка. Личните файлове не се възстановяват чрез този инструмент.

За преглед потърсете **Create a restore point** → **System Protection**. Проверете защитата за системния дял и наличните точки. Ръчна точка се създава с Create и описателно име. При липса на права или изключена защита се обръщате към администратора. В учебната задача не се извършва връщане на системата.

File History

File History (История на файловете) пази версии на потребителски файлове на външен диск или мрежово местоположение. Проверява се дали нужната папка е включена в обхвата. Служи за възстановяване на файл или негова предишна версия; не представлява образ на цялата ОС.

Достъпът в Windows 10 и 11 може да се намери чрез търсене на **File History** или **Control Panel** → **System and Security** → **File History**. Избират се устройство и включване на функцията. За възстановяване се използва Restore personal files или наличните предишни версии; избира се дата и файл. За учебна проверка се възстановява в друга папка.

Backup and Restore

Backup and Restore (Windows 7) е по-стар инструмент, който в някои версии на Windows дава възможност за резервни копия и системен образ чрез Create a system image. Наименованието е запазено и в по-нови версии. Функцията за системен образ е наследена и вече не се развива; наличието и подходящото решение се проверяват за конкретната система.

Съвременното приложение Windows Backup е отделно средство, свързано с личен Microsoft акаунт, OneDrive и запазване на определени настройки. То не трябва да се приема за пълен локален системен образ.

Нужда	Подходящо средство
Връщане след проблемен драйвер	System Restore при налична подходяща точка.
Възстановяване на личен документ	Резервно копие или File History при налична версия.
Възстановяване на системни дялове	Предварително създаден подходящ системен образ.

3 Потребителски акаунти и права

Потребителският акаунт определя самоличността на потребителя в системата и участва в определянето на достъпа до ресурси. Начинът на влизане и нивото на правата са различни характеристики.

Начин на влизане	Особености
Локален акаунт	Създава се за конкретния компютър. Самото влизане в него не изисква интернет или облачна синхронизация.
Microsoft акаунт	Личен онлайн акаунт за услуги на Microsoft и възможна синхронизация. Обхватът зависи от услугата и настройките.
Служебен или учебен акаунт	Управлява се от организация. Достъпът и настройките могат да са зададени централизирано.

Нива на достъп

- **Standard User** (стандартен потребител) използва приложенията и променя разрешените лични настройки. Системни промени могат да изискват администраторско удостоверяване.
- **Administrator** (администратор) може да извършва административни промени, например управление на акаунти и системни настройки. Това не означава автоматично неограничен достъп до всеки защитен или криптиран файл.

Локален и Microsoft акаунт могат да имат стандартни или административни права. За ежедневна работа се използват само необходимите права. За споделена папка в мрежата могат да са разрешени четене или промяна; наличието на мрежова връзка не дава автоматично достъп.

4 User Account Control

User Account Control (UAC) е механизъм за контрол при действия, изискващи повишени права. Обикновено и при административен акаунт приложенията работят с ограничени права, докато не бъде разрешено конкретно повишаване.

При административна промяна UAC може да поиска потвърждение от администратор или негови данни за удостоверяване при стандартен потребител. Поведението зависи и от политиките на организацията. Преди разрешаване се проверяват програмата, издателят и причината за искането; неочаквана заявка се отказва и се проверява.

Настройките се намират чрез **Change User Account Control settings**. Четирите нива са: винаги уведомявай; уведомявай при промени от приложения с потъмняване на екрана; същото без потъмняване; никога не уведомявай. Последното намалява защитата. В задачата се разглежда текущото ниво, без да се понижава.

UAC не е антивирусна програма и не гарантира, че разрешеното приложение е безопасно. Не създава резервно копие и не заменя добрата преценка на потребителя.

5 Защитна стена и други средства за защита

Защитната стена (Firewall) е съвкупност от технически и/или програмни средства за контрол на мрежовия трафик и заявките за услуги. Windows Defender Firewall прилага правила за входящи и изходящи връзки. Разрешаването или блокирането зависи от правилата и активния мрежов профил.

Мрежов профил	Предназначение
Domain network	Мрежа, в която компютърът е удостоверен към домейн на организацията; правилата често се управляват централизирано.
Private network	Доверена мрежа, например домашна. Откриване и споделяне се разрешават според настройките.
Public network	Недоверена мрежа, например обществен Wi-Fi. Подходяща е по-ограничена достъпност за други устройства.

Private не означава „без риск“, а **Public** не означава „достъп до интернет за всеки“. Профилът определя прилаганите правила. Достъпът до интернет и откриваемостта от други устройства са различни неща.

Отворете **Windows Security** → **Firewall & network protection**. В Allow an app through firewall се виждат разрешените изключения за приложения и профили. Този списък не показва всички текущи интернет връзки и не е пълна справка за изходящия трафик; допълнителните правила са в Advanced settings. Не изключвайте цялата защитна стена заради проблем с една програма.

Ограничаването на достъп до определени сайтове може да се реализира с подходящо мрежово филтриране, специализирана защитна стена, DNS или прокси услуга. Обикновеният списък с разрешени приложения в Windows Firewall не е списък с уеб адреси.

Избор според риска

Проблем или риск	Основно средство
Загуба или изтриване на данни	Резервни копия с проверено възстановяване.
Чуждо прочитане на външен диск	Криптиране на данните и защита на ключа.
Неоторизиран достъп до акаунт	Уникална силна парола и двуфакторна автентикация.
Зловреден софтуер	Антивирусна защита, актуализации и проверка на източниците.
Нежелани мрежови връзки	Защитна стена и подходящи правила.
Автоматично стартиране на приложения	Task Manager → Startup apps.

Криптирането прави съдържанието нечетимо без необходимия ключ. То защитава поверителността, но не възстановява загубен носител. **Двуфакторната автентикация** използва два различни вида фактори, например парола и код от приложение на телефон. Две последователни пароли не са два различни фактора.

При проблем с акаунт се проверяват активните сесии, сменя се компрометираната парола и се включва допълнително удостоверяване. Съчетаването на мерки намалява риска; не гарантира абсолютна сигурност.

6 Практически задачи

Задача 1 Точки за възстановяване

Отворете **System Protection** и проверете състоянието на защитата и наличните точки. При разрешение създайте точка с име „Преди учебна промяна“. Запишете датата и обхвата. Обяснете защо тази точка не възстановява изтрит личен документ. Не изпълнявайте System Restore.

Задача 2 Акаунт и UAC

Проверете типа на своя акаунт и текущото ниво на UAC. Разграничете начина на влизане от административните права. Обяснете как стандартен потребител реагира на заявка за административна промяна. Не записвайте пароли и не понижавайте защитата.

Задача 4 Windows Firewall

Проверете активния профил и състоянието на защитната стена. В Allow an app through firewall намерете Google Chrome, ако е инсталиран и присъства в списъка, или друго посочено приложение. Запишете отметките за Private и Public и обяснете какво означават. Разгледайте Advanced settings чрез демонстрация; не променяйте правилата.

Задача 5 Указания за друг потребител

Напишете кратки указания за резервно копиране и възстановяване на учебна папка. Посочете целта, версията на Windows, необходимите права, избраното място, последователността, проверката и реакцията при липса на носител или отказан достъп. Съученик изпълнява указанията и отбелязва дали възстановеният файл е правилен.

Задача 6 Казус за училищен проект

Част от файловете са изтрити по погрешка и има съмнение за чужд достъп до облачния акаунт. Предложете действия за възстановяване и за защита на акаунта. Обяснете защо само Firewall или компресиране не решава и двата проблема.