

<https://itkvariat.by/news/1173-kolichestvo-unikalnyh-kiberatak-snizilos-vpervye-za-neskolko-let.html>

*«Эксперты Positive Technologies проанализировали актуальные киберугрозы III квартала 2021 года и зафиксировали снижение числа уникальных кибератак, рост доли атак на частных лиц, а также увеличение количества атак на организации с использованием ВПО для удаленного управления.»*

**ВЫВОД???**

<https://habr.com/ru/company/pt/blog/598845/>

*«За всеми этими кажущимися отстраненными страшилками о гигантских утечках, зашифрованных или взломанных на продажу данных, вымогательском ПО и кибершпионаже стоят вполне понятные каждому обывателю словосочетания:*

- нехватка топлива,*
- отмена авиарейсов,*
- приостановка производства,*
- перебои с поставками продовольствия,*
- неработающие АЭС,*
- срыв плановых операций.*

*А ещё десятки миллионов долларов, потерянных частными компаниями по всему миру, и уничтоженные репутации.»*

**ВЫВОД???**

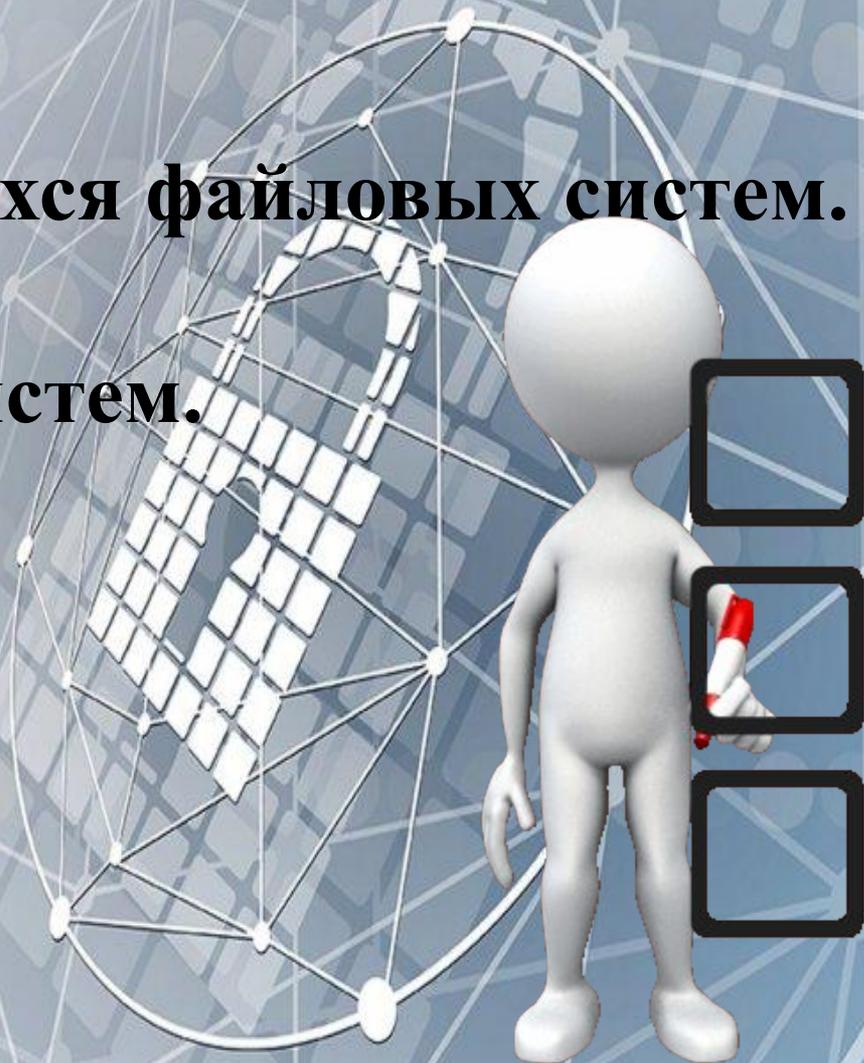
ЛЕКЦИЯ:

# РАБОТА С ФАЙЛОВОЙ СИСТЕМОЙ В ОПЕРАЦИОННЫХ СИСТЕМАХ



# ВОПРОСЫ:

1. Обзор часто встречающихся файловых систем.
2. Уязвимости файловых систем.



# 1. Обзор часто встречающихся файловых систем.



**ВОПРОС:**

**Что такое «ФАЙЛОВАЯ СИСТЕМА»?**





**Case 2017 года**

Пользователи ПК со стажем могут помнить ошибки операционных систем Windows 95 и 98. Определённые имена файлов были способны привести к аварийному завершению работы ОС. Злоумышленники могли использовать это для атак на персональные компьютеры.

Как выяснилось, схожий баг присутствует и в более современных операционных системах Windows 7, Windows 8.1 и Windows Vista. Речь идет об уязвимости в файловой системе NTFS, позволяющей злоумышленникам вызвать зависание или аварийное завершение работы.

Причина возникновения проблемы кроется в файле \$MFT. Этот файл является самым важным в разделе диска, поскольку отслеживает все файлы на томе, их физическое местоположение на жестком диске, логическое расположение внутри папок и всевозможные метаданные. Пользователи не могут открыть файл, поскольку это может привести к разрушению всех данных.

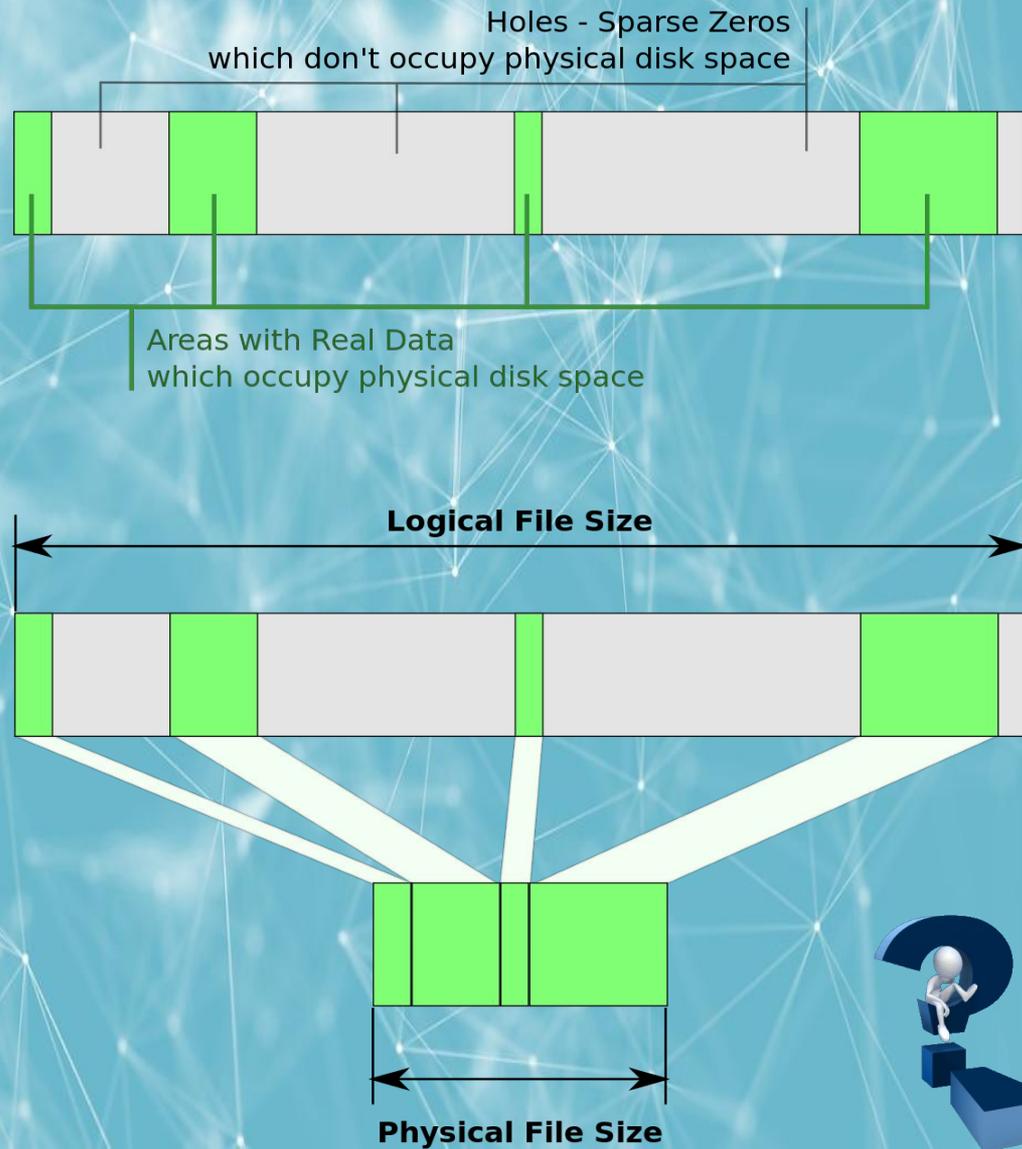
Если использовать имя файла \$MFT в качестве имени директории (C:\\$MFT\foo), можно вызвать зависание или аварийное завершение работы Windows. Если система зависла, единственный способ решить проблему — перезагрузить компьютер. Баг работает в браузерах Internet Explorer и Firefox, но не работает в Chrome.



# Что такое «разреженный файл»?

**Разрежённый файл (англ. sparse file)** — файл, в котором последовательности нулевых байтов [1] заменены на информацию об этих последовательностях (список дыр).

**Дыра (англ. hole)** — последовательность нулевых байт внутри файла, не записанная на диск. Информация о дырах (смещение от начала файла в байтах и количество байт) хранится в метаданных ФС.



## Case 2018 года

Разработчик софта Майк Бомбич обнаружил уязвимость файловой системы APFS, которая при определенных условиях может привести к потере данных MacOS. Она связана с тем, как операционная система обрабатывает разреженные файлы в формате APFS.

По словам Бомбича, на данный момент в яблочной настольной системе есть две проблемы. Первая заключается в том, что macOS не совсем корректно рассчитывает свободное пространство на диске. А вторая – в том, что система не сообщает пользователям о возможных ошибках при переполненном диске и продолжает операцию. Однако после перезагрузки компьютера получить доступ к таким данным уже не получится. При этом проблемы затрагивают только разреженные образы дисков, отформатированные в формате файловой системы APFS, представленной в macOS High Sierra в марте 2017 года.

Разреженный образ диска - тип файла образа диска, который может увеличиваться в ходе того, как пользователь добавляет в него все больше данных. Разреженные образы дисков могут работать только до уровня, на котором может использоваться базовый носитель, и они будут показывать доступное значение свободного места в зависимости от свободного места, которое осталось на жестком диске.

Как пояснил Бомбич, операционная система не только не предупреждает пользователей о заполнении жесткого диска, но и отображает ложную информацию. В частности, в течение короткого периода после выполнения операции записи macOS может получить доступ к файлу и даже показать файл с надлежащей контрольной суммой. Таким образом пользователь может думать, что операция копирования или перемещения пошла успешно. При этом после перезагрузки системы все артефакты скопированных файлов удаляются из памяти ОС, а сами файлы становятся поврежденными и недоступными.



## Case 2020 года

В августе 2020 года, октябре 2020 года и, наконец, на этой неделе, исследователь из InfoSec Йонас Л привлек внимание к уязвимости NTFS Windows 10, которая до сих пор не исправлена.

Эксплуатацию уязвимости можно выполнить с помощью однострочной команды, после чего мгновенно происходит повреждение NTFS. Система предлагает перезагрузить компьютер, чтобы восстановить поврежденные записи на диске.

Диск можно повредить, если определенным образом попытаться получить доступ к атрибуту \$i30 NTFS в папке.

Выполнение приведенной ниже команды на работающей системе приведет к повреждению диска и, возможно, сделает его недоступным.

Приводим пример команды, которая приводит к повреждению диска: Атрибут индекса NTFS или строка «\$i30» представляет собой список файлов и подпапок каталога. В некоторых случаях индекс NTFS может включать удаленные файлы или каталоги, что удобно при восстановлении объектов во время экспертизы.

После запуска команды в командной строке и нажатия Enter пользователь Windows 10 получит ошибку «Файл или папка повреждены. Чтение невозможно».

Windows немедленно выведет уведомление с предложением перезагрузить компьютер и восстановить поврежденный том диска. После повреждения дисков Windows 10 начнет генерировать ошибки в журнале событий, указывая, что основная таблица файлов (MFT) для конкретного диска содержит поврежденную запись.

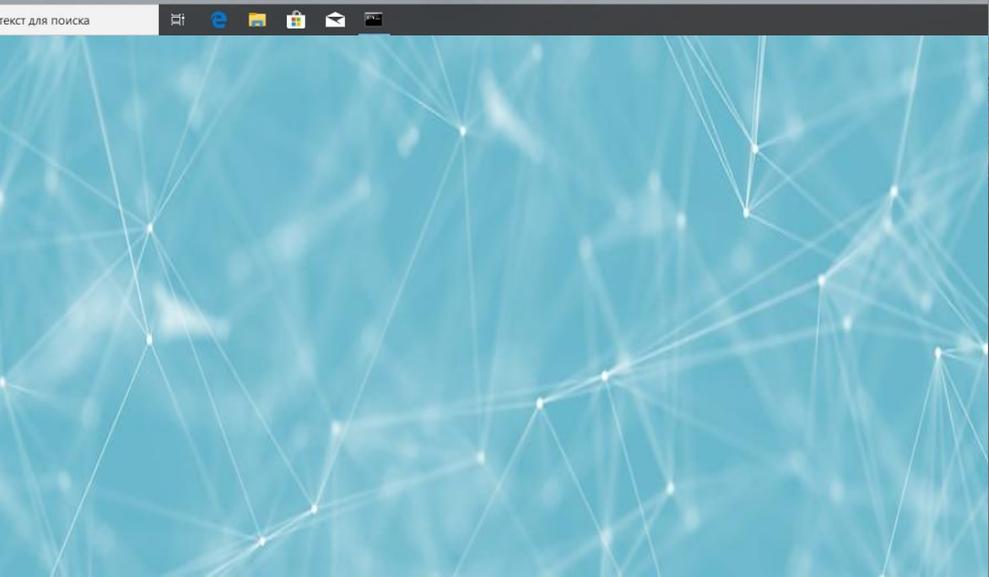


```
Командная строка
Microsoft Windows [Version 10.0.18363.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\military>cd C:\$130$bitmap
Файл или папка повреждены. Чтение невозможно.

C:\Users\military>
```

 **Перезагрузите, чтобы устранить ошибки диска**  
Щелкните, чтобы перезагрузить компьютер  
Центр безопасности и обслуживания



```
Командная строка
Microsoft Windows [Version 10.0.18363.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\military>cd C:\$130$bitmap
Файл или папка повреждены. Чтение невозможно.

C:\Users\military>
```

**Центр безопасности и обслуживания**

**Перезагрузите свой ПК, чтобы исправить ошибки на диске**

Перед перезагрузкой сохраните все открытые файлы и закройте все приложения.



# Классификация файловых систем

## По структуре

Одноуровневые (в настоящее время не применяются)

Иерархические

Однокорневые (применяются в unix-подобных ОС)

Многокорневые (применяются в ОС Windows и Linux-подобных ОС)

## По назначению

Для носителей с произвольным доступом (NTFS, FAT32, ext2 и т.д.)

Для носителей с последовательным доступом (QIC и т.д.)

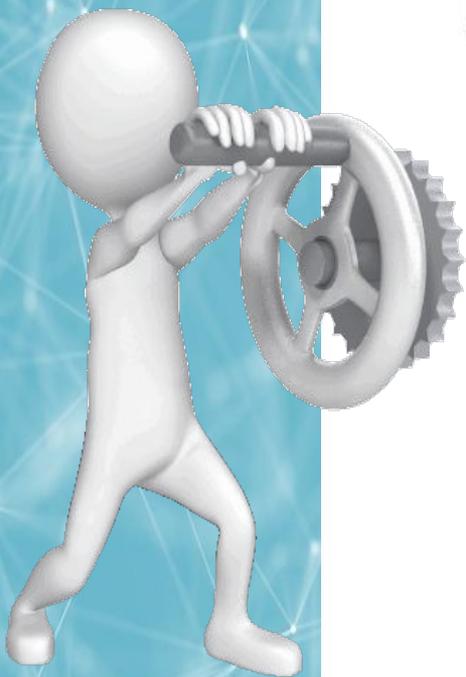
Для оптических носителей (ISO9660, UDF, HFS)

Виртуальные файловые системы (AEFS и т.д.)

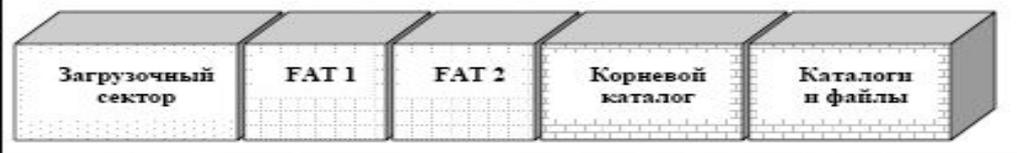
Сетевые файловые системы (NFS, CIFS, SSHFS, GmailFS)

Для флэш-памяти (YAFFS, exFAT и т.д.)

VMware VMFS (кластерная файловая система, для хранения других файловых систем)



**FAT** является наиболее упрощенным из файловых систем, поддерживаемых Windows. Файловая система FAT характеризуется таблицей распределения файлов (FAT), которая на самом деле является таблицей, которая находится в самом "верху" тома. Чтобы защитить том, в случае повреждения одной из них хранятся две копии FAT. Кроме того, таблицы FAT и корневой каталог должны храниться в фиксированном расположении, чтобы правильно располагать файлы загрузки системы.



Диск, отформатированный с помощью FAT, выделяется в кластерах, размер которых определяется размером тома. Когда создается файл, в каталоге создается запись и устанавливается первый номер кластера, содержащий данные. Эта запись в таблице FAT указывает на то, что это последний кластер файла, или указывает на следующий кластер. В структуре каталогов FAT нет организации, и файлам предоставляется первое открытое расположение на диске.

### **Достоинства:**

1. *Высокая скорость работы;*
2. *Низкое требование к объему оперативной памяти;*
3. *Эффективная работа с файлами средних и малых размеров;*
4. *Более низкий износ дисков, вследствие меньшего количества передвижений головок чтения/записи.*

### **Недостатки:**

1. *Низкая защита от сбоев системы;*
2. *Не эффективная работа с файлами больших размеров;*
3. *Ограничение по максимальному объему раздела и файла (4 гигабайта);*
4. *Снижение быстродействия при фрагментации;*
5. *Снижение быстродействия при работе с каталогами, содержащими большое количество файлов.*

**NTFS** (аббревиатура от англ. new technology file system — «файловая система новой технологии») — стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft.

NTFS поддерживает хранение метаданных. С целью улучшения производительности, надёжности и эффективности использования дискового пространства для хранения информации о файлах в NTFS используются специализированные структуры данных. Информация о файлах хранится в главной файловой таблице — Master File Table (MFT). NTFS поддерживает разграничение доступа к данным для различных пользователей и групп пользователей (списки контроля доступа — англ. access control lists, ACL), а также позволяет назначать дисковые квоты (ограничения на максимальный объём дискового пространства, занимаемый файлами тех или иных пользователей). Для повышения надёжности файловой системы в NTFS используется система журналирования USN. Для NTFS размер кластера по умолчанию составляет от 512 байт до 64 КБ в зависимости от размера тома и версии ОС.

### **Достоинства:**

1. Быстрая скорость доступа к файлам малого размера;
2. Размер дискового пространства на сегодняшний день практически не ограничен;
3. Фрагментация файлов не влияет на саму файловую систему;
4. Высокая надёжность сохранения данных и собственно самой файловой структуры;
5. Высокая производительность при работе с файлами большого размера.

Зона MFT

Загрузочная запись
Файлы
\$Mft
Зарезервированное место под \$Mft
Файлы

### **Недостатки:**

1. Более высокие требования к объёму оперативной памяти по сравнению с FAT 32;
2. Работа с каталогами средних размеров затруднена из-за их фрагментации;
3. Более низкая скорость работы по сравнению с FAT 32.

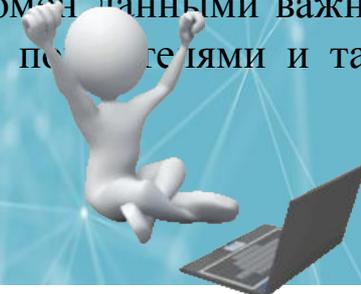
**ExFAT** — это аббревиатура, означающая «Расширенная таблица распределения файлов». Максимальный размер кластера ExFAT составляет 32 мегабайта. Максимальное же количество файлов, которое может быть сохранено в папке — 2 796 202. В случае с FAT32 — предшественником exFAT — верхний предел был ограничен 65 534 файлами.

ExFAT крайне полезен при работе с различными операционными системами. Причиной тому является прекрасное взаимодействие и совместимость с Mac, Windows и Linux. Кроме того, поддерживаются все носители информации — от жестких дисков до USB-накопителей и SD-карт. ExFAT элементарно решает все проблемы, при хранении огромных файлов на различных платформах.

### **Недостатки:**

При работе с интенсивными, ресурсозатратными приложениями exFAT часто может столкнуться с теми или иными проблемами. Причем, независимо от операционной системы на которой используется данный формат. Жесткий диск иногда может не отображаться в списке подключенных устройств и, иногда, для правильной передачи данных может понадобиться несколько попыток. Поскольку ExFAT не является избыточным носителем для хранения основных данных, носители с файловой системой exFAT всегда следует извлекать с особой осторожностью. В противном случае данные могут быть потеряны или повреждены. И восстановить их после этого довольно сложно.

Отсутствие поддержки сжатия также делает exFAT неподходящим выбором для определенных приложений. Поэтому, если вы работаете только с Windows и не считаете межплатформенный обмен данными важным для своей работы, NTFS остается лучшим вариантом. Тем более что со скоростными приложениями и так все в порядке.



Файловая система	Win XP	Win 7/8/10	macOS (до 10.6.4)	macOS (10.6.5 и новее)	Ubuntu Linux	PlayStation 4	Xbox 360 / One
<b>NTFS</b>	Да	Да	Только для чтения	Только для чтения	Да	Нет	Нет/Да
<b>FAT32</b>	Да	Да	Да	Да	Да	Да	Да/Да
<b>exFAT</b>	Да	Да	Нет	Да	Да (с пакетами ExFAT)	Да (с MBR, а не GUID)	Нет/Да
<b>HFS+</b>	Нет	(только для чтения с Boot Camp)	Да	Да	Да	Нет	Да
<b>APFS</b>	Нет	Нет	Нет	Да (macOS 10.13 или выше)	Нет	Нет	Нет
<b>EXT 2, 3, 4</b>	Нет	Да (со сторонним ПО)	Нет	Нет	Да	Нет	Да

Файловая система	Размер файла	Ограничение размера тома
<b>NTFS</b>	Больше, чем коммерчески доступные диски	16 ЭБ
<b>FAT32</b>	Менее 4 ГБ	Менее 8 ТБ
<b>EXFAT</b>	Больше, чем коммерчески доступные диски	64 ЗБ
<b>HFS +</b>	Больше, чем коммерчески доступные диски	8 ЭБ
<b>APFS</b>	Больше, чем коммерчески доступные диски	16 ЭБ
<b>EXT 2, 3</b>	16 ГБ (до 2 ТБ на некоторых системах)	32 ТБ
<b>EXT 4</b>	1 ЭБ	16 ТБ

*Кластерные файловые системы включают поддержку распределенных хранилищ, расширяемость и модульность.*

К ним относятся:

**ZFS** – «Zettabyte File System» разработана для распределенных хранилищ Sun Solaris OS;

**Apple Xsan** – эволюция компании Apple в CentraVision и более поздних разработках StorNext;

**VMFS** - разработана компанией VMware для VMware ESX Server;

**GFS** – Red Hat Linux именуется как «глобальная файловая система» для Linux;

**JFS1** – оригинальный (устаревший) дизайн файловой системы IBM JFS, используемой в старых системах хранения AIX.



**ZFS** — это copy-on-write файловая система, она никогда не перезаписывает данные. Мы всегда оперируем новым блоком, для обеспечения консистентности данных не нужен журнал, как в большинстве других файловых системах

Copy-on-write дает следующее преимущество: старые данные не меняются, можно не вести журнал и восстановить данные, записанные ранее. Мы не боимся повреждения данных, так как их нельзя повредить, новый вариант блока запишется в новое место, не затирая старый.

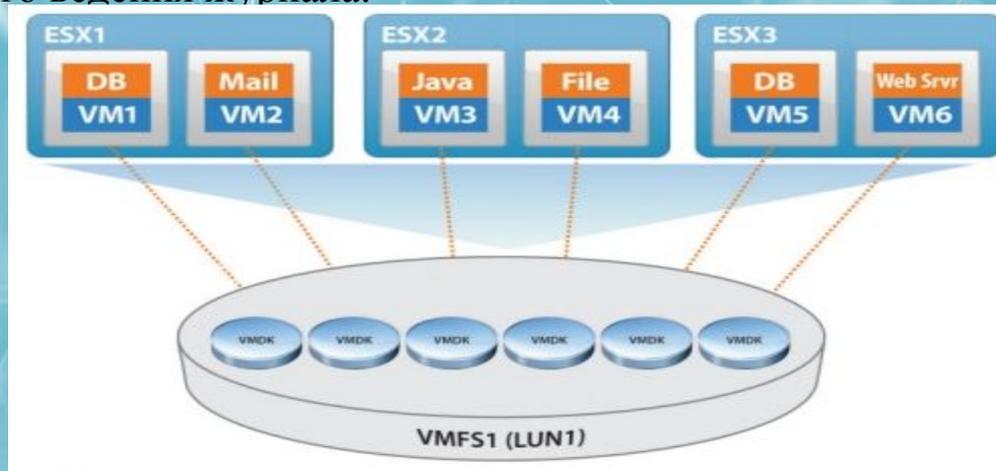
Сам copy-on-write процесс не гарантирует консистентность данных, но если рассматривать ZFS, то в основе его работы лежит дерево Меркла, или Хэш-дерево. У ZFS всегда консистентное состояние за счет того, что он использует атомарные транзакции. Есть дерево блоков, для каждого из них с самого нижнего блока подсчитывается хеш-сумма и так доходит до самого верхнего блока. Хеш-сумма верхнего блока (uberblock) позволяет валидировать состояние всей файловой системы на момент транзакции.



**VMware VMFS (Virtual Machine File System)** - кластерная файловая система VMware, Inc., используемая основным пакетом виртуализации серверов компании, vSphere. Он был разработан для хранения образов дисков виртуальных машин, включая snapshots. Несколько серверов могут считывать/записывать одни и те же файлы одновременно, в то время как отдельные файлы виртуальных машин являются загруженными. Объемы VMFS могут быть логически "выращены" (не активно увеличены в размере) путем нескольких объемов VMFS вместе.

### Особенности:

- Возможность обеспечения одновременного доступа к нескольким серверам ESXi за счет реализации файловых io. Резервирование SCSI реализуются только при обновлении метаданных логического номера (LUN) (например, изменение имени файла, изменение размера файла и т. д.);
- Возможность добавления или удаления сервера ESXi с тома VMware VMFS без прерывания работы других серверов ESXi;
- Благодаря ESX/ESXi4 тома VMFS также можно расширить с помощью расширения логических устройств;
- Возможность восстановления виртуальных машин быстрее и надежнее в случае сбоя сервера с помощью функции распределенного ведения журнала.



## 2. Уязвимости файловых систем.



**Уязвимость** — это недостаток в программном обеспечении, оборудовании или процедуре, который может предоставить атакующему возможность доступа к компьютеру или сети и получения несанкционированного доступа к информационным ресурсам.

***CVE (англ. Common Vulnerabilities and Exposures)*** — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида ***CVE-год-номер***, описание и ряд общедоступных ссылок с описанием.



**MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)** — это структурированный список известных поведений злоумышленников, разделенный на тактики и методы, и выраженный в виде таблиц (матриц). Матрицы для различных ситуаций и типов злоумышленников публикуются на сайте MITRE.

**Инцидент ИБ** — любое непредвиденное или нежелательное событие, которое может нарушить деятельность системы или ИБ.



## «Природа» возникновения уязвимостей в ФС:

- неправильная настройка файловой системы;
- «ошибка» в реализации файловой системы.



# Уязвимости файловых систем виртуализации (кластерных систем виртуализации):

- **обмен файлами между хостовой и гостевой ОС** (скомпрометированный гость может получить доступ к узлу файловой системы, изменить каталоги хостовой ОС);
- **гипервизор** - как единая точка входа в инфраструктуру;
- **связь разделов дисков VM на уровне вычислителей** (разделы на VM делят ресурсы памяти, процессора и пропускную способность, соответственно, если определенный раздел потребляет слишком много одного из вышеуказанных ресурсов, к примеру, из-за вируса, на других разделах может появиться ошибка);
- **легкий доступ к виртуальным дискам** (виртуальные диски обычно хранятся на хосте, как незащищенные файлы и получить к ним доступ очень просто — не нужно ничего взламывать).

## *Работа по локализации уязвимостей файловых систем:*

- правильная настройка контролируемого оборудования:
  - ◆ настройка разрешений файловой системы;
  - ◆ резервирование место под данные пользователя root;
  - ◆ настройка проверки файловой системы;
  - ◆ другие...
- мониторинг состояния контролируемого оборудования:
  - ◆ использование систем мониторинга;
  - ◆ использование специализированных утилит;
  - ◆ **взаимодействие с CERT.RU.**
- мониторинг существования известных уязвимостей:
  - ◆ мониторинг уязвимостей на официальных сайтах вендоров;
  - ◆ мониторинг специализированных публичных ресурсов.

# Мониторинг состояния контролируемого оборудования:

- ◆ использование систем мониторинга:
- ◆ FileMon;
- ◆ SecureTower;
- ◆ Решения Лаборатории Касперского;
- ◆ Inotify-tools;
- ◆ Zabbix;
- ◆ и другие решения.

# • Мониторинг состояния контролируемого оборудования:

- ♦ использование специализированных утилит

## WINDOWS:

- ♦ **SFC** (проверка системных файлов) - SFC проверяет отсутствие важных файлов в вашей операционной системе Windows и восстанавливает их из кеша.

**CHKDSK** (проверка диска) - CHKDSK сканирует ваш диск на предмет сбойных секторов и пытается исправить ошибки в файловой системе.

- ♦ **DISM** (обслуживание образов развертывания и управление ими) - DISM напрямую обрабатывает неисправные образы Windows и восстанавливает их, загружая файлы замены с онлайн-серверов Windows.



# ♦ Мониторинг состояния контролируемого оборудования:

## ♦ использование специализированных утилит LINUX:

- ♦ **FSCK** - утилита для проверки и восстановления файловых систем Linux. Проверка файловых систем разных физических дисков выполняется параллельно, что позволяет значительно её ускорить.
- ♦ **DEBUGFS** - утилита входящая в состав пакета e2fsprogs и служит для интерактивного исследования и изменения состояния файловых систем типа ext2 и ext3.
- ♦ **DF** - утилита в UNIX и UNIX-подобных системах, показывает список всех файловых систем по именам устройств, сообщает их размер, занятое и свободное пространство и точки монтирования.
- ♦ **DU** - стандартная Unix-программа для оценки занимаемого файлового пространства. Показывает размер файлового пространства, занимаемого каждым файлом и каталогом в текущем каталоге.



```

root@pc:/home/user# fsck -help
fsck from util-linux 2.34
fsck.ext4: invalid option -- 'h'
Usage: fsck.ext4 [-panyrcdfktvDFV] [-b superblock] [-B blocksize]
               [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
               [-E extended-options] [-z undo_file] device

Emergency help:
-p           Automatic repair (no questions)
-n           Make no changes to the filesystem
-y           Assume "yes" to all questions
-c           Check for bad blocks and add them to the badblock list
-f           Force checking even if filesystem is marked clean
-v           Be verbose
-b superblock Use alternative superblock
-B blocksize Force blocksize when looking for superblock
-j external_journal Set location of the external journal
-l bad_blocks_file Add to badblocks list
-L bad_blocks_file Set badblocks list
-z undo_file Create an undo file
root@pc:/home/user#

```

```

user@pc:~$ du

```

```

16  ./config/dconf
3   ./config/evolution/sources
12  ./config/evolution
3   ./config/caja
16  ./config/ownCloud
4   ./config/celluloid/watch_later
4   ./config/celluloid/scripts
12  ./config/celluloid
3   ./config/google-chrome/Crowd Deny/2022.1.10.1202/_metadata
36  ./config/google-chrome/Crowd Deny/2022.1.10.1202
3   ./config/google-chrome/Crowd Deny/2022.1.24.1201/_metadata
36  ./config/google-chrome/Crowd Deny/2022.1.24.1201

```

```

root@pc:/home/user# df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	3,8G	0	3,8G	0%	/dev
tmpfs	785M	1,7M	783M	1%	/run
/dev/mapper/vgmint-root	227G	51G	165G	24%	/
tmpfs	3,9G	157M	3,7G	4%	/dev/shm
tmpfs	5,0M	4,0K	5,0M	1%	/run/lock
tmpfs	3,9G	0	3,9G	0%	/sys/fs/cgroup
/dev/loop1	56M	56M	0	100%	/snap/core18/2253
/dev/loop0	128K	128K	0	100%	/snap/bare/5
/dev/loop2	56M	56M	0	100%	/snap/core18/2284
/dev/loop3	165M	165M	0	100%	/snap/gnome-3-28-1804/161
/dev/loop4	44M	44M	0	100%	/snap/snapd/14295
/dev/loop5	66M	66M	0	100%	/snap/gtk-common-themes/1519
/dev/loop7	117M	117M	0	100%	/snap/drawio/142
/dev/loop6	44M	44M	0	100%	/snap/snapd/14549
/dev/loop8	117M	117M	0	100%	/snap/drawio/143
/dev/sda5	704M	209M	444M	32%	/boot
/dev/sda1	511M	4,0K	511M	1%	/boot/efi
tmpfs	785M	32K	785M	1%	/run/user/1000

```

root@pc:/home/user#

```



# Мониторинг существования известных уязвимостей:

- ◆ мониторинг уязвимостей на официальных сайтах вендоров;
- ◆ мониторинг специализированных публичных ресурсов:

<https://cve.mitre.org;>

<https://nvd.nist.gov;>

<https://cvedetails.com;>

<https://www.cve.org;>

[https://www.exploit-db.com.](https://www.exploit-db.com;)



# Взаимодействие с CERT.BY (PORTAL)

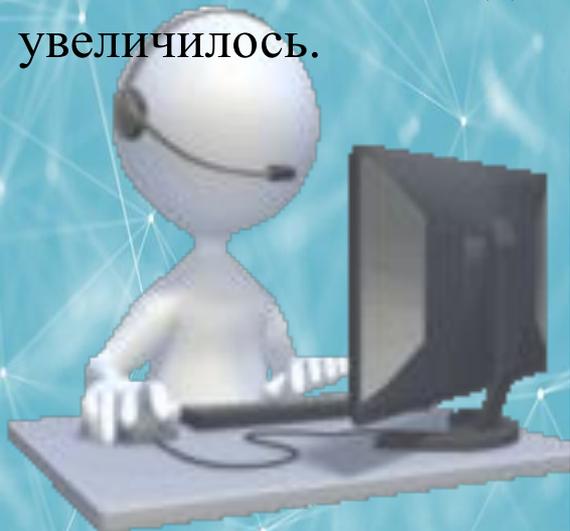
Отслеживается более **70 типов** событий информационной безопасности..

По состоянию на конец 2021 года — в системе **более 20 гос. органов и организаций** на автоматическое оповещение. Некоторые представляют секторальные центры компетенции.

Также **10 крупных провайдеров**.

Только в гос. органы и организации за прошлый год (2021) были отправлены уведомления более чем о **13000 событиях безопасности**.

С начала этого года число гос. органов, организаций и провайдеров еще увеличилось.



## Задачи CERT.BY



### Своевременное обнаружение

Своевременное обнаружение вирусных эпидемий в национальном сегменте сети Интернет



### Подготовка рекомендаций

Подготовка рекомендаций по выявлению и устранению проанализированных информационных угроз



### Анализ информационных угроз

Анализ выявленных информационных угроз на предмет функционала, методов распространения и управления, а также оценки потенциальных и реальных угроз



### Взаимодействие с международными командами

Взаимодействие с международными командами реагирования на компьютерные инциденты и с антивирусными компаниями



### Контроль модификаций

Контроль модификаций выявленных экземпляров информационных угроз

**СПАСИБО ЗА ВНИМАНИЕ!**

