

Наизусть:

1. Типы скачков напряжения и мощности

Brownout	Prolonged low voltage
Sag/Dip	Momentary low voltage
Fault	Momentary power loss
Blackout	Complete loss of power
Surge	Prolonged high-voltage
Noise	Steady interfering line disturbance
Transient noise	Short duration line disturbance
Spike	momentary high voltage
Inrush	current is initial surge of power at the beginning

2. Типы orange книг (red, blue и проч )

Red book	Trusted Network Interpretation book
Orange Book	Trusted Computer System Evaluation Criteria
Green Book	Password Management
Yellow Book	TCSEC in Specific Environments
Tan Book	Audit
Brown Book	Facility management

3. Типы TSCEC(B1 - , C2 - )

Степени доверия:

A	Verified Protection	configuration management
B3	Security domain MAC	TCB; security administrator and auditing; configuration management
B2	Structured protection MAC	addresses covert channels and trusted facility management; configuration management
B1	Labeled Security MAC	labels for AC
C2	Controlled Access DAC	
C1	Discretionary DAC	
D	Minimal	system tested and failed

4. ITSEC separates these two attributes and rates them separately. Functionality is rated from F1 to F10 and assurance is rated from E0 (D) to E6 (A1)

5. OSI

7	Application	HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP,		
---	-------------	------------------------------------------------------------	--	--

		NNTP, S-RPC, and SET, S-HTTP, SOCKs		
6	Presentation	encryption protocols, such as RSA and DES, and format types, such as ASCII, EBCDIC, TIFF, JPEG, MPEG, and MIDI		
5	Session	TLS, NFS, SQL, and RPC		
4	Transport	SSL, SPX, TCP, and UDP, SSH2, SKIP		End-to-end
3	Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPsec, IPX, NAT, and SKIP	Router	packet filtering firewalls
2	Data Link	SLIP, PPP, ARP, RARP, L2F, L2TP, PPTP, FDDI, ISDN, MAC	Bridge	Address the physical locations and/or devices on the network
1	Physical	EIA/TIA-232, EIA/TIA-449, X.21, HSSI, SONET, V.24, and V.35	Repeaters and Hubs	

6.

Bella-LaPadula

Simple Security Rule	No read up
The * properties or Confinement(ограничение) property	No Write down
Strong star or <i>Tranquillity</i> property	На этом же уровне. For a subject to be able to read and write to an object, the subject's clearance and the object's classification must be equal.

Biba

*-integrity axiom	no write up
Simple integrity axiom	no read down

7. Типы контроля

Physical control	guards and building security, biometric access restrictions, protection of cables, file backups
Administrative control	policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation.
Logical or technical control	Restrict access to systems and the protection of information — Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols (Kerberos, IPsec)

8.

Application control type	Accuracy	Security	Consistency
--------------------------	----------	----------	-------------

Preventive	Data checks, forms, custom screens, validity checks	Firewalls, sensitivity labels, encryption, passwords, test environments	Data dictionary, programming standards
Detective	Hash controls, cyclic redundancy checks	IDS and audit trails	Comparison controls, relationship tests
Corrective	Backups, checkpoint restarts	Emergency response and reference monitor	Program comments and database controls

9. Operational controls: are people, they are most often procedures. Backup and recovery, contingency planning and operations procedures are operational controls.

10.

Security Modes of Operation:

1. Dedicated: Each subject must have clearance for ALL information on system and valid need to know for ALL information.

2. System high: Each subject must have clearance for ALL information on system and valid need to know SOME of the information —All users may not have need to know —

3. Compartmented: Each subject must have clearance for MOST RESTRICTED information on system and valid need to know THAT information.

4. Multilevel: Some subjects do not have clearance for ALL information — Each subject has a need to know ALL information to which they will have access.

11.

Multicast	a source packet is copied and sent to specific multiple destinations on the network
Unicast	sends a packet from a single source to a single destination
Broadcast	a packet is copied and then sent to all the stations on a network

12.

Specification	Cable Type	Max Length
10BaseT	UTP	100 meters
10Base2	Thin Coax (Thinnet)	185 meters
10Base5	Thick Coax (Thicknet)	500 meters
10BaseF	Fiber	2000 meters

UTP Category Characteristics Usage

Category 1	Voice-grade telephone cable	Not recommended for network use, but modems can communicate over it
Category 2	Data transmission up to 4 Mbps	Used in mainframe and minicomputer terminal

		connections, but not recommended for highspeed networking
Category 3	10 Mbps for Ethernet and 4 Mbps for Token Ring	Used in 10Base-T network installations
Category 4	16 Mbps	Used usually in Token Ring networks
Category 5	100 Mbps for 100Base-TX and CDDI networks; has high twisting, and thus low crosstalk	Used in 100Base-TX, CDDI, Ethernet, and ATM installations; most widely used for new network installations
Category 6	155	Used in new network installations requiring high-speed transmission
Category 7	1 Gbps	Used in new network installations requiring higher-speed transmission

### 13. Normalizing data in Databases:

1. Eliminating any repeating groups by putting them into separate tables.
2. Eliminating redundant data (occurring in more than one table).
3. Eliminating attributes in a table that are not dependent on the primary key of that table.

### 14. RAID

0	Data striped over several drives	Striping. It lessens the fault tolerance of the disk system. One-for-one disk to disk ratio	hardware-level parity – faster
1	Data is written to two drives at once	Mirroring of drives. Первый, кто обеспечивает redundancy (избыточность) и parity (четность)	hardware-level parity – faster. Very expensive, resulting in the highest cost per megabyte of data capacity
2	Data striping over all drives at the bit level	Hamming code parity	
3	Data striping over all drives and parity data held on one drive	Byte-level parity	
4	Same as level 3 except parity is created at the block level instead of the byte level	Block-level parity	
5	Data is written in disk sector units to all drives	Interleave parity	
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives	Second parity data (or double parity)	
7	RAID 5 + single virtual disk in the hardware		5+virtual disk
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures	Striping and mirroring	0+1

1. Mean-time-between failure (MTBF) is the average length of time the hardware is functional without failure. Mean-time-to-repair is the amount of time it takes to repair and resume normal operation after a failure has occurred. Having a higher MTBF and a lower MTTR will increase the reliability of a piece of equipment, thus the system's overall reliability.

#### 15. Backup

Incremental backups	backups store only those files that have been modified since the time of the most recent full or incremental backup. Некоторые файлы после Любого бэкапа
Differential backups	store all files that have been modified since the time of the most recent full backup. Все файлы после Полного бэкапа
Full backup	Delete archive bit

#### 16. Алгоритмы

	Алгоритм	Блоки, Длина ключа	Кругов
	DES	56 bit key, + 8 parity bits=64	16
	3DES	56+56+56= 168	48
	IDEA	128	8
	Blowfish	64,448	
	Skipjack	80 bit key, 64 bit block key size	
	RSA	512,768,1024	
	AES Rjandal	128,192,256	10,12,14
	SHA-1	SHA-256, SHA-384, SHA-512 supports AES — HAVAL	
	MD5	128 bit digest of input message, uses blocks of 512	4

#### 10.

Red Box	Simulate tone
Black Box	Line voltage
Blue Box	Voltage manipulate

#### 11.

Acceptance - is the verification that performance and security requirements have been met.
Accreditation - An accreditation is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.
Certification - is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended.

12.

1. Legal evidence

- a. Best evidence — original or primary evidence rather than a copy of duplicate of the evidence
- b. Secondary evidence — a copy of evidence or oral description of its contents; not as reliable as best evidence
- c. Direct evidence — proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses
- d. Conclusive (Окончательное) evidence — incontrovertible неопровержимое; overrides all other evidence
- e. Opinions — two types: Expert — may offer an opinion based on personal expertise and facts, Non-expert — may testify only as to facts
- f. Circumstantial (косвенное) evidence — inference выведение of information from other, immediate, relevant facts
- g. Corroborative (подтверждающее evidence) — supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence
- h. Hearsay (на слухах) evidence (3rdparty) — oral or written evidence that is presented in court that is second hand and has no firsthand proof of accuracy or reliability

(i) Обычно не допустимое в суде

(ii) Computer generated records and other business records are in hearsay category

(iii) Certain exceptions to hearsay rule (1) Made during the regular conduct of business and authenticated by witnesses familiar with their use (2) Relied upon in the regular course of business (3) Made by a person with knowledge of records (4) Made by a person with information transmitted by a person with knowledge (5) Made at or near the time of occurrence of the act being investigated (6) In the custody of the witness on a regular basis

2. Standards for evidence

- a. Relevant — must be related to the crime
- b. Legally Permissible — evidence was obtained in a lawful manner
- c. Reliability — evidence has not been tampered не фальсифицированное with or modified
- d. Sufficient достаточное — must be persuasive enough to convince a reasonable person of the validity of the findings. должно быть убедительный достаточно, чтобы убеждать разумного человека в достоверности сведений
- e. Identification — evidence is properly identified without changing or damaging the evidence
- f. Preservation — evidence is not subject to damage or destruction

3. Evidence life cycle: collection and identification; analysis; storage, protection, transportation; presentation in court; and return to victim/owner

1973	U.S. Code of Fair Information Practices applies to personal record-keeping.
1974	U.S. Privacy Act provides for the protection of information about private individuals that is held in federal databases
1977	U.S. Foreign Corrupt Practices Act imposes civil and criminal penalties if publicly held organizations fail to maintain adequate controls over their information. Organizations must take reasonable steps to ensure not only the integrity of their data, but also the system controls the organization put in place.
1980	Organization for Economic Cooperation and Development (OECD) Guidelines— provides for data collection limitations, the quality of the data, specifications of the purpose for data collection, limitations on data use, information security safeguards, openness, participation by the individual on whom the data is collected, and accountability of the data controller
1986	US Electronic Communications Privacy Act— prohibits eavesdropping or interception of message contents without distinguishing between private or public systems
1987	Federal Computer Security Act: first to require government agencies to do security training and adopt security plan
1996	Health Insurance and Portability Accountability Act (HIPAA) (Kennedy-Kassenbaum Act) — addresses the issues of personal health care information privacy and health plan portability in the United States
1999	Gramm Leach Bliley (GLB) Act— requires financial institutions to develop privacy notices and give their customers the option to prohibit the banks from sharing their information with nonaffiliated third parties