Belarusian State Technological University
Department of Information Systems and Technology

Pavel Urbanovich

INFORMATION PROTECTION.

Part 1: INTRODUCTION TO THE SUBJECT AREA

pav.urb@yandex.by, p.urbanovich@belstu.by

Literature

- **Vasant Rawalv, Ashok Fichadia,** *Risks, Controls and Security - Concepts and Applications*, John Wiley, 2007
- **C.Pfleeger, S. Pfleeger**, *Security in Computing*, Prentice Hall,2007
- **J. Pieprzyk, T. Harjono, J. Seberry**, *Fundamentals of Computer Security, Springer-Verlag, 2003*
- ***B. Schneier***, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996
- ***Howard M., LeBlanc D.*** *Writing Secure Code, 2nd Edition*, Microsoft Corporation, 2003

Literature (in Russian)

- ***Urbanovich, P. P.*** *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii : ucheb.-metod. posobiye dlya stud. / P.P. Urbanovich. - Minsk: BGTU, 2016. - 220 s.*
- ***Shneier, B.*** *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty naya yazyke Si/ B. Shnayyer. – M.: Izdatel'stvo TRIUMF, 2003.*
- ***Kharin, YU. S.*** *Matematicheskiye osnovy kriptologii / YU. S. Kharin, V. I. Bernik, G. V. Matveyev. – Mn.: BGU, 1999.*
- ***Urbanovich, P. P.*** *Informatsionnaya bezopasnost' i nadezhnost' sistem: ucheb.-metod. posobiye / P. P. Urbanovich, D. M. Romanenko, Ye. V. Romantsevich. – Mn.: BGTU, 2007*
- ***Howard, M.*** *Zashchishchennyy kod / M. Howard,, D. Leblank. – M.: Izdatel'skiy dom «Russkaya redaktsiya», 2005*
- **Urbanovich, P. P.** Zashchita informatsii i nadezhnost' informatsionnykh sistem: pos. dlya stud. vuzov spets. 1-40 05 01-03 «Informatsionnyye sistemy i tekhnologii (izdatel'sko-poligraficheskiy kompleks)» / P. P. Urbanovich, D. V. Shiman.- Minsk : BGTU, 2014. - 91 s.

Information protection (I. security) - definition

- **Information (Data) protection** is a set of **actions** taken to safeguard information or data stored in computer memory, in particular in databases.
- It is also the **process** of safeguarding important information from corruption and/or loss.

Assets of computer systems

Hardware

Software

Data

Communication facilities and networks

Basic definitions

The development of information technology has led to dynamic development of communication processes:

- *collection and storage*,
- t*ransformation*,
- *analysis and presentation*,
- *exchange and transmission of information* (*data*, *knowledge*).

Def. 1 Informatics

(computer science, computing science, information technology, informatics)

A discipline that has developed concepts, methods and techniques for building complex systems for:

- collection and storage,
- processing analysis and representation,
- transfer,

of information in a symbolic form.

Def. 2 Telecommunications

- the field of science and technology dealing with distance information transmission.

Def. 3 Information technology

- this is the combination of IT applications with communication techniques.

Hierarchy of cognitive concepts

The most important terms of the information society are: ***data*****,** ***information*** *and* ***knowledge***

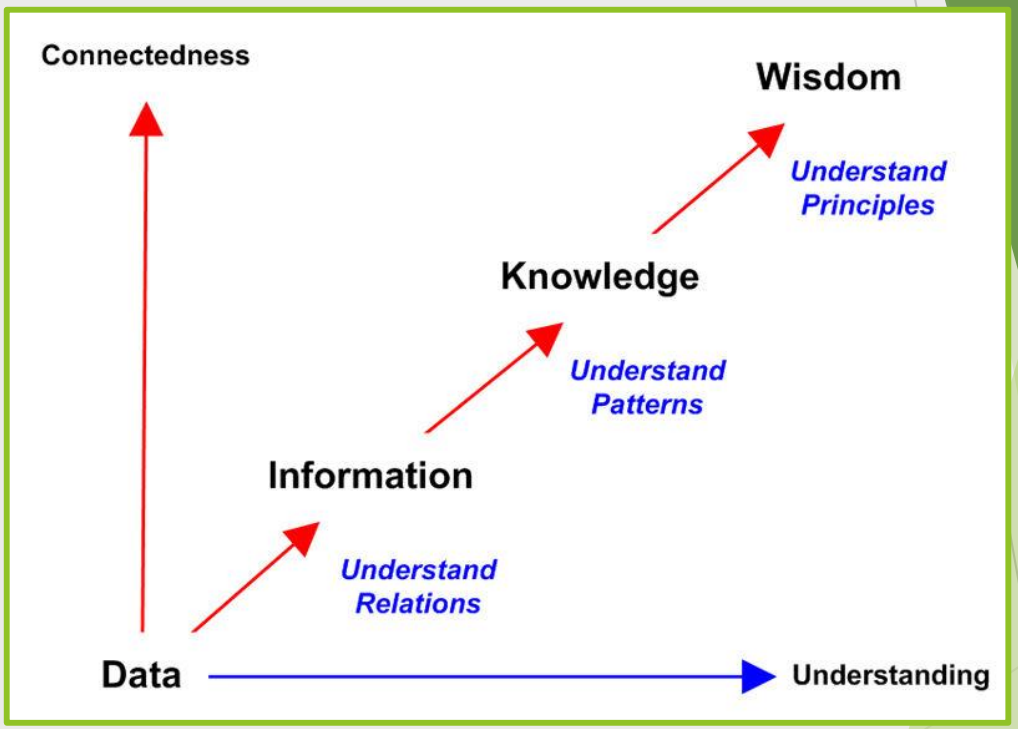
Hierarchy of terms

You can meet the term **DIKW** - short for the first letters of each component:

- **Data,**
- **Information,**
- **Knowledge,**
- **Wisdom.**

The cognitive chain

Data-Information-Knowledge-Wisdom – shows how each of the next links depends on the others



The chain is used in:

- the knowledge management process,
- and supports the way to create a value hierarchy.

Information and Data

Def. 4. Data (or datum – a single unit of data)

- this is fixed information about events and phenomena that are stored on certain media.

Data can take different forms:

- characters,
- speech,
- graphs.

- Different **data** may represent the same information.
- **Data** as a general concept refers to the fact that some existing information or knowledge is *represented* or *coded* in some form suitable for better usage or processing.
- **Data** - this is a untested fact, number and event from which information can be elaborated.
- **Data in IS - representation of information stored in a certain area of computer memory.**

Thus:

- The raw data is not of much practical importance.
- Data is therefore a concept narrower than information.
- The information appears as a result of data processing in solving specific problems.

Def.5 Information

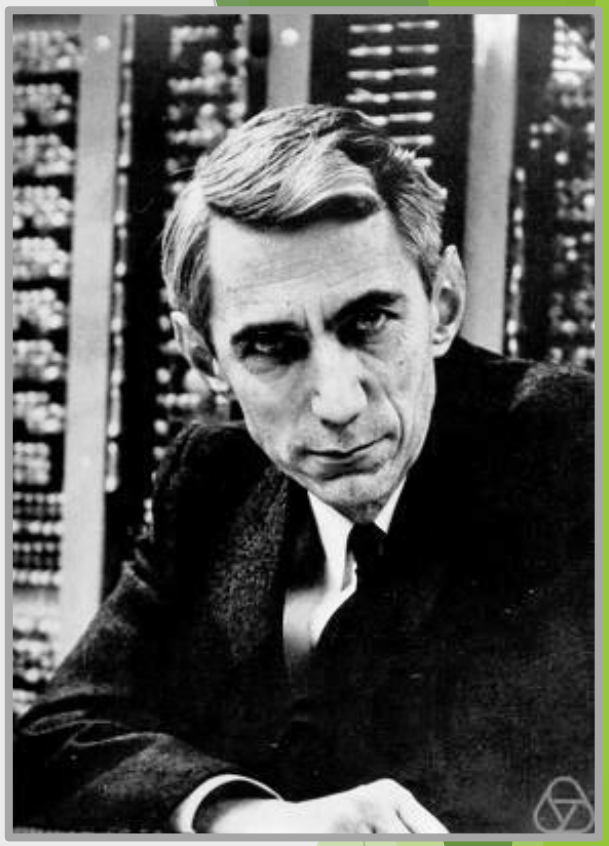
- is the content of the message in order:

-collection and storage,

-processing analysis and representation,

-exchange or transmission of data.

- The concept of data in the context of computing has its roots in the work of **Claude Shannon**, an American mathematician known as the **father of information theory**.
- He ushered in binary digital concepts based on applying two-value Boolean logic to electronic circuits.



Claude Elwood Shannon *(April 30, 1916-February 24, 2001) was an American mathematician, electrical engineer, and cryptographer.*

Shannon, C.E. "A Mathematical Theory of Communication." *The Bell System Technical J.* **27**, 379-423 and 623-656, July and Oct.1948
http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

Selected definitions of data and information from the literature

Authors	Definitions of data	Definitions of information
Avison and Fitzgerald (1995)	Data represents unstructured facts	Information has a meaning... It comes from the selection of data, their summaries and presentations in a way they are useful to the recipient
Clare and Loucopoulos (1987)	Facts gathered from observations or records regarding phenomena, objects or people	Requirements for making decisions. Information is a product of significant data processing
Galland (1982)	Facts, concepts or results in a form that can be communicated and interpreted	Information is what arises as a result of certain human thought activities (observations, analyzes) successfully applied to data to reveal their essence or meaning
Hicks (1993, 3rd Ed)	Reprezentacja faktów, koncepcji lub instrukcji w sposób sformalizowany, umożliwiający komunikowanie, interpretację lub przetwarzanie przez ludzi lub urządzenia automatyczne	Representation of facts, concepts or instructions in a formalized way that allows communication, interpretation or processing by people or automated devices
Knight and Silk (1990)	Numbers representing observable objects or issues (facts)	Meaning for people related to observed objects and phenomena
Laudon and Laudon (1991)	Raw facts that can be shaped and formed to create information	Data that has been shaped or formed by humans into an important and useful form

Important concepts with respect to information protection

CIA

Confidentiality

- Confidentiality - is to ensure that information processed in the system can be read only by authorized persons.
- Assets are only available for authorized parties.

-Include *confidentiality* and *privacy*-

Let ***X*** be a set of entities and let ***I*** be some information. ***I*** has the confidentiality property with respect to ***X*** if no member of ***X*** can obtain information about ***I***.

Example:

- ***X*** = set of students,
- ***I*** = final exam answer key,
- ***I*** is confidential with respect to ***X*** if students cannot obtain final exam answer key.

Integrity

- Integrity - is to ensure that data stored in the system and transmitted information can only be modified by authorized persons.
- Assets can be changed only by authorized parties in authorized ways.

  – Covers protect against unauthorized *modification*, *deletion* or *insertion* data reuse of others' messages and so on -

Let ***X*** be a set of entities and *let **I*** be some information or a resource. ***I*** has the integrity property with respect to ***X*** if all members of ***X*** trust ***I***.

Types of integrity:

- trust ***I***, its conveyance and protection (*data integrity*),
- if ***I*** is information about origin of something or an identity, then members of ***X*** trust that the information is correct and unchanged (*origin integrity, authentication*),
- if ***I*** is a resource, integrity means that the resource functions as it should (*assurance*).

Availability

- Availability - provides the ability of authorized users to use the system resources at any time.
- Assets are available for authorized parties when desired.

–Covers timely responses, fair service, maintaining the necessary capacity, orderly crash... -

Let ***X*** be a set of entities and let ***I*** be some information or a resource. ***I*** has the availability property with respect to ***X*** if all members of ***X*** can access ***I***.

Types of availability:

- traditional: $x \in X$ gets access or not,
- quality of service: promised a level of access (for example, a specific level of bandwidth) and not meet it, even though some access is achieved.

Confidentiality + Integrity + Availability

- A security policy considers all relevant aspects of confidentiality, integrity and availability.

Confidentiality Policy:

- the policy identifies those states in which information leaks to those not authorised to receive it,
- the policy must also handle dynamic changes of authorisation.

Integrity Policy:

- the policy identifies authorised ways in which information may be altered and entities authorised to alter it.

Availability Policy:

- the policy describes what services must be provided, including parameters, required quality of service etc.

- Resistance - consists in ensuring the blocking and neutralization of various intrusions (attacks) and interferences in the IS.

- Accountability - consists in preventing both the sender and receiver of the message from denying the message.

- Authenticity - consists in correctly determining of the origin of the message, ensuring the authenticity of the source.

- Reliability - is to ensure the correct operation of the system.

Personal Data

Def. 6 Personal data

means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

- In accordance with **UK's ICO**

  (https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/)

- **Personal data** is "…any set of information relating to individuals… specific information relating to a particular individual is readily **accessible**".

"**Accessible record**" means:

• a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual;

• an educational record that consists of information about a pupil, which is held by a local education authority or special school; or

• an accessible public record that consists of information held by a local authority for housing or social services purposes.

Personal Data: Examples

- **Personal data:**
- What are the types of personal data?
- How can you use them (for example) in health care, in education etc.?
- Who can see them?
- How can you guarantee the confidentiality of this data (in most situations)?

- **Company's data:**
- The financial data,
- Patents,
- Internal product information,
- Personal information about staff files for clients, partners, etc.
- Information on the technical aspects of business.

Who and how can use the information?

The important things for a person, a company or an institution, **to be protected.**

- Examples:
- Staff Address book,
- Patient records,
- Tax Information,
- Character Sheets,
- Criminal records,
- Keys for net-banking.

Sensitive Personal Data

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Criminal records,
- Serious social problems,
- Civil registration (CPR) numbers

Data protection and computer security

DP and **IP** - protection of data (information) and information systems from:

- ***interference***, the result of which can be:
  - destruction of data,
  - modification of data,
  - block access to data for legitimate users.
- ***unauthorized access***, which can be:
  - data usage,
  - disclosure of data,-modification of data,-destruction of data,
  - data theft.

Computer security is a field of technology known as information (data) protection used in computers.

Interference and obstacles

- **Sources of interference:**

-cosmos,

-telecommunication, power engineering, machinery and tools.

- **Intentional sources:**

-normal provided by the constructors, the work of the device is a source of interfering signals of other devices (radar, telecommunication transmitters, industrial transmitters, etc.)

- **Non-intentional sources:**

-disturbance signals are the result of transient states, failures or non-ideal functioning of equipment or systems or installations (sparking commutations, non-ideal connectors, transient states, switching phenomena, short circuits in electrical circuits).

Protection methods : in the simplest case:

-shielding equipment and transmission channels,

-use of UPS,

-CRC - Cyclic Redundancy Check (Code).

Def.7 Unauthorized Access

Viewing private accounts, messages, files or resources when one has not been given permission from the owner to do so. Viewing confidential information without permission or qualifications can result in legal action.

Protection methods: Computer systems use a variety of mechanisms to block UA.

Def.8 Destruction of data

Complete, irretrievable data loss, preventing them from being repaired.

Protection methods: The only possibility of effective protection is regular creation **Backup copy**.

Def.9 Modification or corruption of data

Occurrence of errors in the data, which prevent their proper use.

Protection methods: Computer systems use a number of mechanisms to guarantee data integrity, cryptography, steganography, hashings, redundant codes, passwords

and more.

Def.10 Data theft

Means that data is in unauthorized hands. A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Then: **a threat can be blocked by checking a vulnerability.**

Protection methods: cryptography, digital signatures, steganography, authorization.

Typical threats in IT Systems

Hardware-related:
- Fire, water, dust, smoke, chemicals...
- Theft, vandalism, physical destruction.
- Listening, electromagnetic emission.

LiveWare-related:
- Social engineering, phishing.

Software-related:
- Unauthorized modification, deletion, use of the wrong version.
- Viruses, worms, Trojan horses, logic bombs.
- Theft, unauthorized copying.

Data-related:
- Theft, unwanted disclosure.
- "Masquerading„ unauthorized access.

Social engineering

Attempts to use various psychological conditions in humans to get hold of confidential information.

Attack

Def.11 An attack

is a attempts to exploit a vulnerability; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

An attacker must have "MOM"

- Method: The necessary skills to carry out the attack.
- Opportunity: Time and access to carry out the attack.
- Motive: A motive for carrying out the attack.

The motivations can be quite different!

- revenge,
- entertainment,
- prestige,
- „Because it was there",
- political/religious.

Phishing

- Phishing attacks use unsolicited emails or scams coming from spoofed email addresses in addition to fake websites controlled by the attacker, but which mimics the login page of some banking, gaming or similar site.
- Very often, the email are “targeted” (spear-phishing) toward specific users and leverage social engineering, to make the scam more reliable.

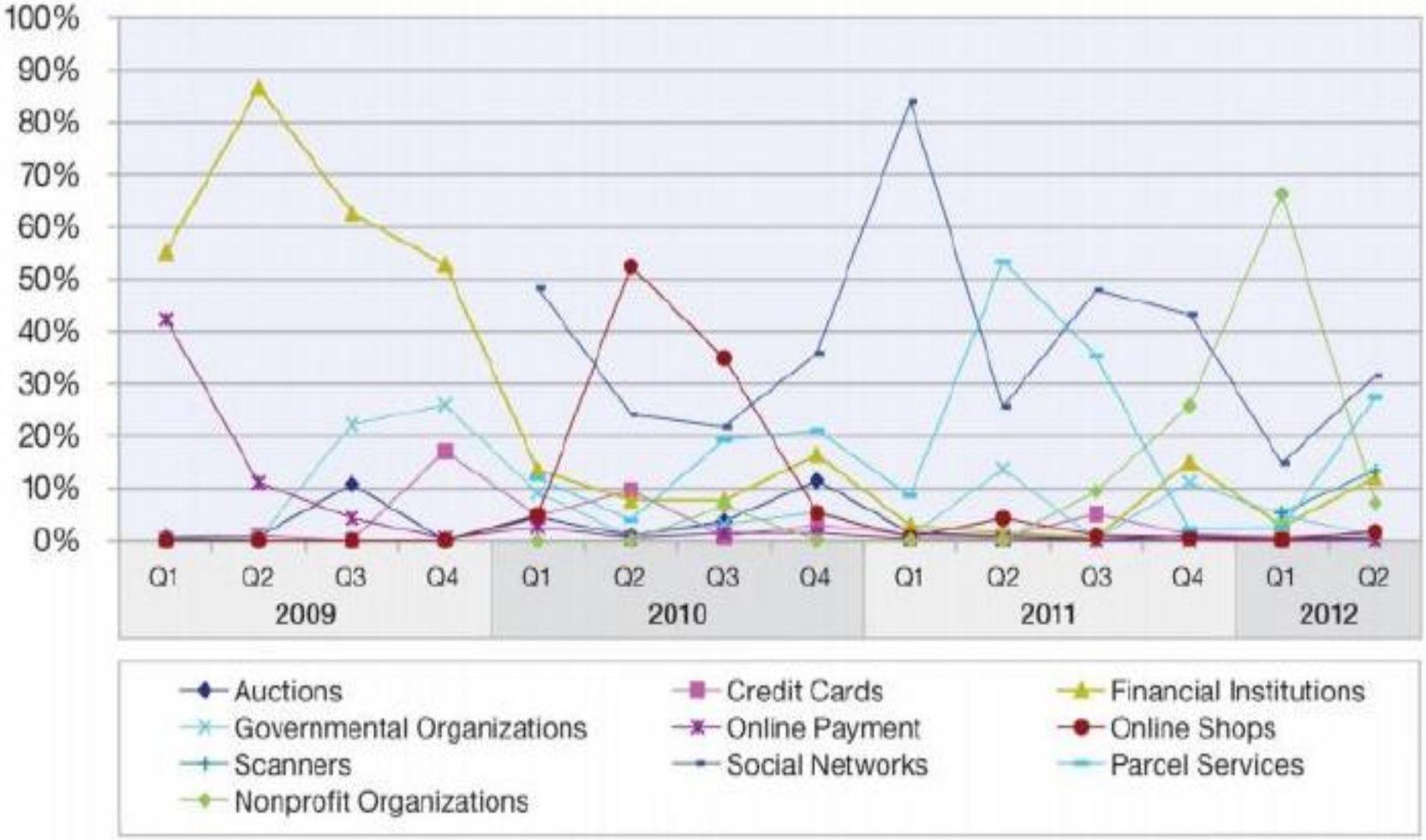
Phishing utilizes different techniques to get people to provide personal (often confidential) data (information).

Among others:

- **Name dropping:** A message refers to an important person, as you may know.
- **Short time**: Something terrible will happen unless you respond rather quickly.
- **Plausible reasons**: eg. That you have to do as the man says in order to avoid a security breach!
- **Asking for sympathy**: Of course you would like to help!
- **False address**: "From" field may look as if the mail comes from a colleague or friend (... but what about the "Reply-to"?).

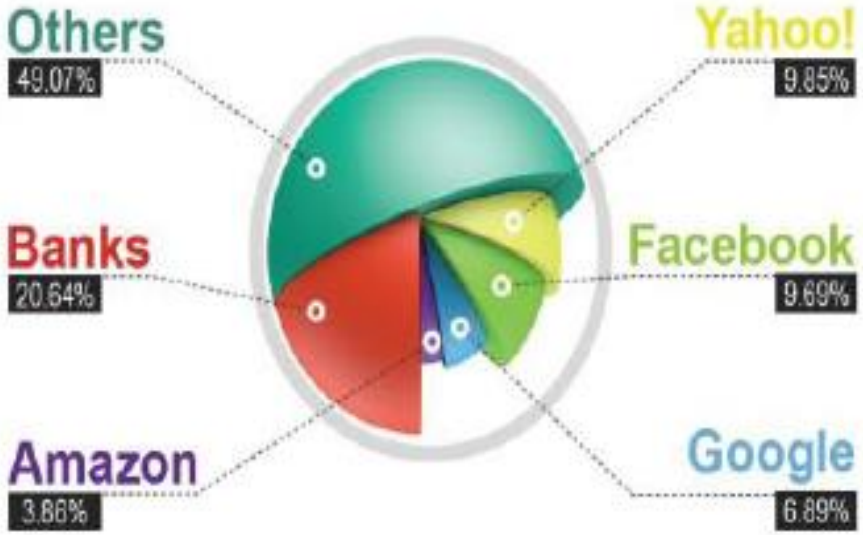
Scam/Phishing Targets by Industry

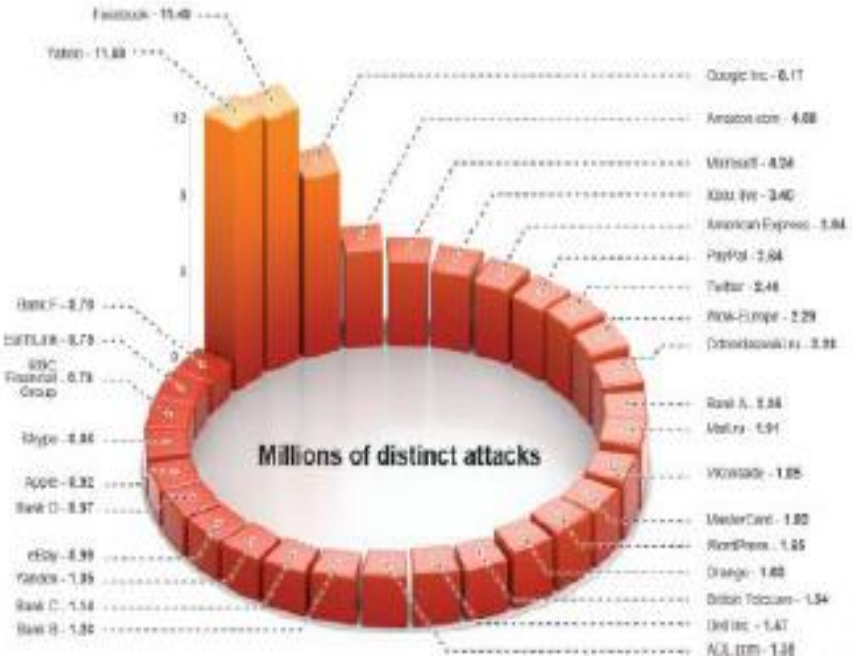
2009 Q1 to 2012 Q2



Source: IBM X-Force® Research and Development

Phishing 2013 for Kaspersky Lab





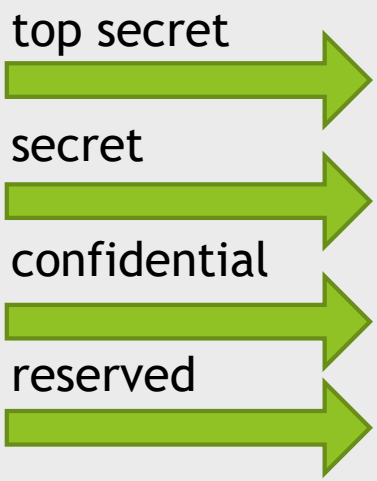
Source: https://www.kaspersky.ru/internet-security

Classified information

Def.12 Classified information

is information (data) to which access needs to meet certain conditions.

In the Act of 5 August 2010 on the protection of classified information, it will renounce the division of state secrets and official secrecy while leaving the current classification of the most classified:



Computer crimes

- break into the computer system
- unauthorized retrieval of information
- destruction of data and programs
- sabotage (paralyzing work) of the system
- computer piracy
- software theft,
- computer fraud and computer forgery
- computer espionage
- access unauthorized to the data in order
  - use of data,
  - disclosure of data,
  - data modification,
  - data destruction,
  - data theft.

- The international criminal police "Interpol" uses the classification of computer crimes by the codifier of the international criminal police of the Interpol General Secretariat(1991).

•All codes characterizing computer crimes have an identifier starting with the letter **Q**.

- **QA - Unauthorized access and interception:**
- QAH - computer gates,
- QAI – interception,
- QAT - theft of time,
- QAZ - other types of unauthorized access and interception;
- **QD - Use of destructive software(malware):**
- QDL - a logical bomb,
- QDT - a Trojan horse,
- QDV - a computer virus,
- QDW - a computer worm,
- QDZ - other types;

- **QF - Computer fraud:**
- QFC - fraud with ATMs,
- QFF - computer fake,
- QFG - fraud with slot machines,
- QFM - manipulations with the input programs,
- QFP - fraud with payment means,
- QFT - telephone fraud,
- QFZ - other computer frauds;
- **QR - Illegal copying (piracy):**
- QRG - computer games,
- QRS - other software,
- QRT - topography of semiconductor products,
- QRZ - other illegal copying;

- **QS - Computer sabotage:**
- QSH - with hardware,
- QSS - with software,
- QSZ - other kinds of sabotage;
- **QZ - Other computer crimes:**
- QZB - using computer bulletin boards,
- QZE - theft of information constituting a trade secret,
- QZS - transmission of confidential information,
- QZZ - other computer crimes;

CyberCrime

- Problem of jurisdiction

- Laws are mostly national, cyber crime is typically transnational.

- International treaties/conventions may codify crime in several countries

- Where is crime committed?

- How to investigate?

- Collecting evidence requires collaboration among law enforcement agencies.

- Extradition agreements between nation

- How to punish criminals?

Fragments of the Belarusian Criminal Codex

- Статья 349. Несанкционированный доступ к компьютерной информации. Наказание: штраф, арест, ограничение или лишение свободы на срок до 2 лет. Если действия, предусмотренные статьей, повлекли тяжкие последствия – возможно ограничение свободы на срок до 5 лет или лишением свободы на срок до 7 лет.
- Статья 350. Модификация компьютерной информации. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.
- Статья 351. Компьютерный саботаж – умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок 3-10 лет.
- Статья 352. Неправомерное завладение компьютерной информацией наказывается общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением или лишением свободы на срок до 2 лет.
- Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети наказывается штрафом, или арестом на срок 3-6 месяцев, или ограничением свободы на срок до 2 лет.
- Статья 354. Разработка, использование либо распространение вредоносных программ. Наказание: штраф, арест, ограничение свободы на срок до 2 лет, лишение свободы до 10 лет.
- Статья 355. Нарушение правил эксплуатации компьютерной системы или сети. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы на срок до 2 лет, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.

https://www.lawtrend.org/publications-interview-programmnye-intervyu-kommentarii-i-publikatsii-ekspertov-prosvetitelskogo-uchrezhdeniya-tsentr-pravovoj-transformatsii/kozluk/aleksej-kozlyuk-zakonodatelstvo-belarusi-o-prestupleniyah-v-sfere-vysokih-tehnologij

Data Center

Def.13. Data center (or datacenter) is a facility composed of networked computers and storage that businesses or other organizations use to organize, process, store and disseminate large amounts of data.

- **DC** - general term referring to modern technology for:
  -collection,
  -storage and processing large amounts of data as well,
  -presentations these data in the user's desired appearance.
- **CD** - is a specialized building for hosting server and network devices and connecting subscribers to Internet channels.

The term "**data center**" has emerged in the 90s with the emergence of client-server architecture. At that time this term was applied to specially designed Server rooms.

- Data centers can be defined by various levels of reliability or resilience, sometimes referred to as **data center tiers**.
- In 2005, the American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA) published standard ANSI/TIA-942, „Telecommunications Infrastructure Standard for Data Centers", which defined four tiers of data center design and implementation guidelines.
- Each subsequent tier is intended to provide more **resilience** (the ability of a substance or object to spring back into shape), **security** and **reliability** than the previous tier.

For example: a tier 1 data center is little more than a server room, while a tier 4 data center offers redundant subsystems and high security.

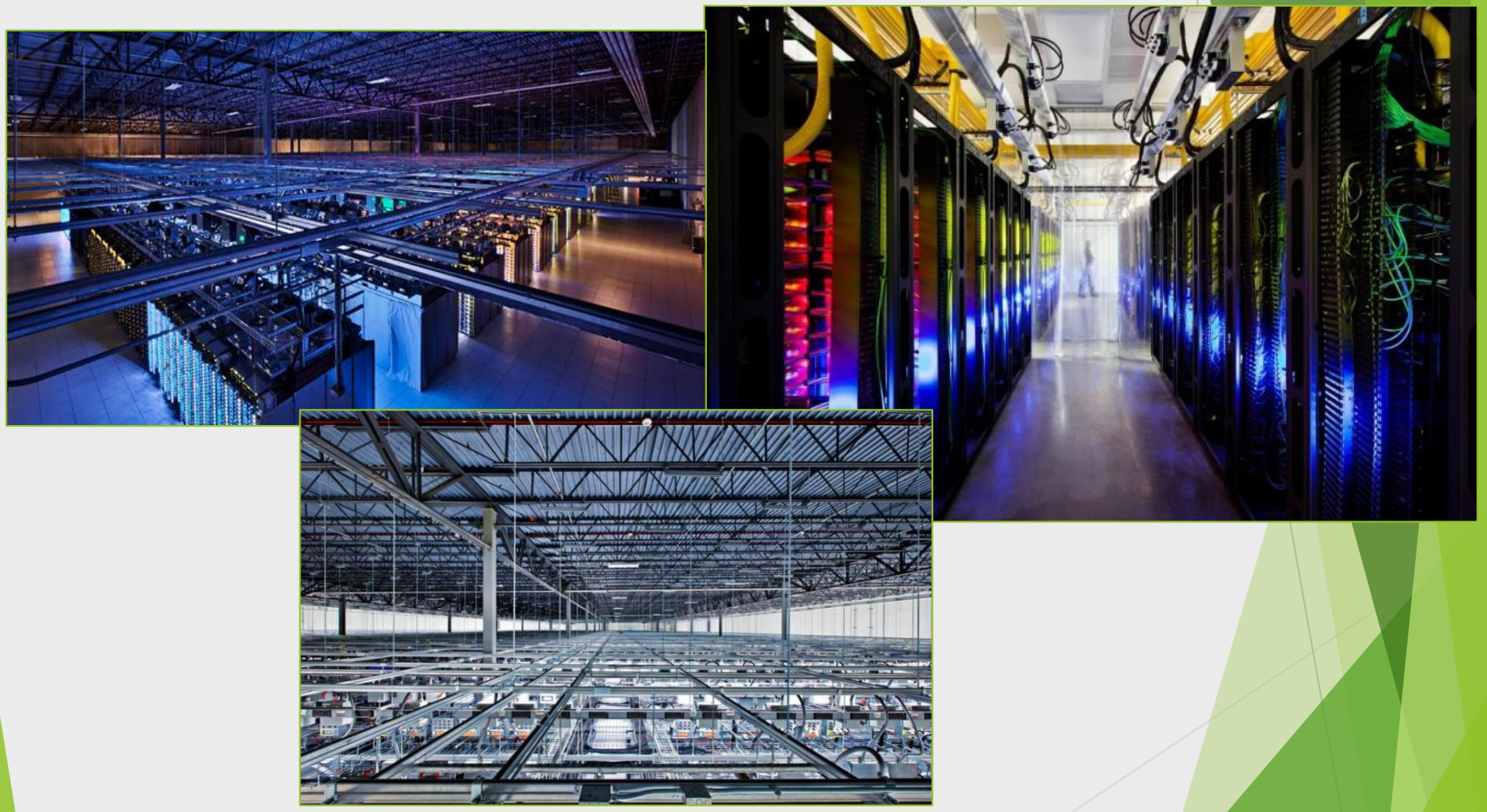
Data Center Tiers

- Tier 1 – basic data center
  - no redundancy
- Tier 2 – redundant components
  - single distribution path with redundant components
- Tier 3 – concurrently maintainable
  - multiple distribution paths with only one active
- Tier 4 – fault tolerant
  - multiple active distribution paths

TIA-942 Spaces

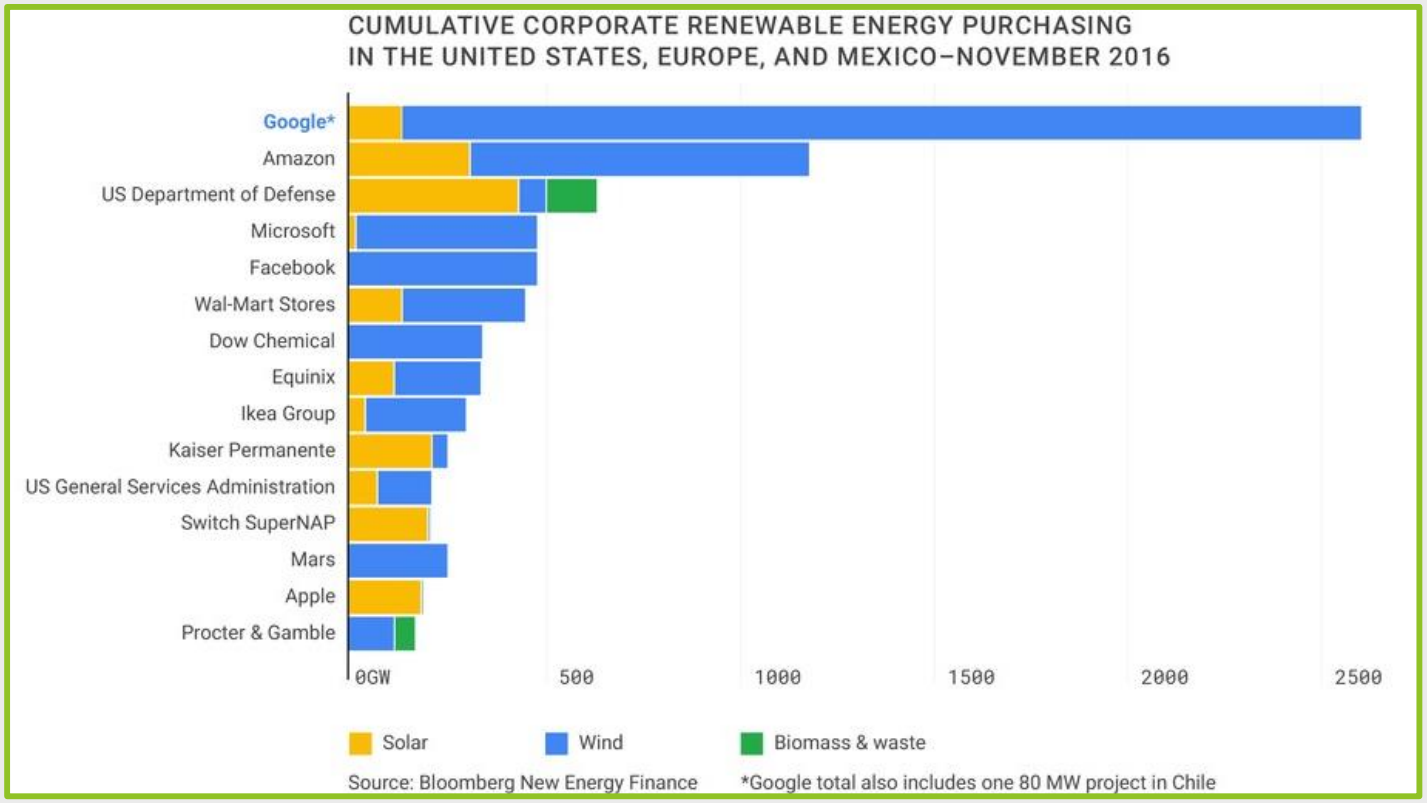
- Etrance Room (ER) – location of interface with campus and carrier entrance facilities.
- Main Distribution Area (MDA) – location of main cross-connect (MC).
- Horizontal Distribution Area (HDA) – location of horizontal cross-connect (HC).
- Zone Distribution Area (ZDA) – location of zone outlet (ZO) or consolidation point (CP).
- Equipment Distribution Area (EDA) – location of equipment cabinets and racks.

DC Google



Source: https://yandex.by/images/search?text=google%20data%20center&stype=image&lr=157&source=wiz

Google is the world's largest corporate buyer or renewable energy, totaling over 3.0GW.



The failed hard drives are destroyed on the spot - Google claims that this is part of their privacy policy.

Source: https://yandex.by/images/search?text=google%20data%20center&stype=image&lr=157&source=wiz

References:

1. Урбанович, П. П. Информационная безопасность и надежность систем : учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. - Минск : БГТУ, 2007. - 87 с. (URL: http://elib.belstu.by/handle/123456789/2937)

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ.. - Минск : БГТУ, 2016. - 220 с. (URL: http://elib.belstu.by/handle/123456789/23763)

3. Урбанович, П. П. Защита информации и надежность информационных систем : пос. для студ. вузов спец. 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)» / П. П. Урбанович, Д. В. Шиман.- Минск : БГТУ, 2014. - 91 с. (URL: https://elib.belstu.by/handle/123456789/23761)

4. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. - Lublin: Wydawnictwo KUL, 2004. - 150 p. (URL: https://elib.belstu.by/handle/123456789/27516)

5. Makas, S. B. License Protection of a Component of Web-Applications on .Net Framework / S. B. Makas, P. P. Urbanovich // New Electrical and Electronic Technologies and their Industrial Implementation: proc. of the 5-th Intern. Conf., Zakopane, Poland.- Lublin. 2007. - P. 99 (https://elib.belstu.by/handle/123456789/25895)

6. Ahmad Almulhem. Security Policie, [Electronic Resource], URL: http://www.ccse.kfupm.edu.sa/~ahmadsm/coe449-072/policy.pdf

7. [Electronic Resource], URL: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx

8. [Electronic Resource], URL: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

9. Confidentiality, Integrity, and Availability (CIA triad), [Electronic Resource], URL: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

10. MIT Open Cource Ware: Introduction to Computational Thinking and Data Science, [Electronic Resource], URL: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-0002-introduction-to-computational-thinking-and-data-science-fall-2016/

11. Guide to Data Protection, [Electronic Resource], URL: https://ico.org.uk/for-organisations/guide-to-data-protection/

12. Vasant Rawalv, Ashok Fichadia, Risks, Controls and Security - Concepts and Applications, John Wiley, 2007

13. C.Pfleeger, S. Pfleeger, Security in Computing, Prentice Hall,2007

14. J. Pieprzyk, T. Harjono, J. Seberry, Fundamentals of Computer Security, Springer-Verlag, 2003

15. B. Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996

16. Howard M., LeBlanc D. Writing Secure Code, 2nd Edition, Microsoft Corporation, 2003