Сигурност. Информационна и мрежова сигурност. Риск

проф. д-р инж. Венета Алексиева

Основни моменти

- Мрежова сигурност
- Информационна сигурност
- Стандарти по сигурност
- Политики за информационна сигурност
- Риск

Аспекти на сигурността

Баланс между 2 важни изисквания:

- Нуждата от отворени мрежи, които отговарят на изискванията на бизнеса
- Нуждата от защита на частната, индивидуална и фирмена информация относно стратегиите в бизнеса

Фактите

Нараства дела в световния търговски баланс на:

- Е-бизнес
- Е-търговия
- Internet приложения

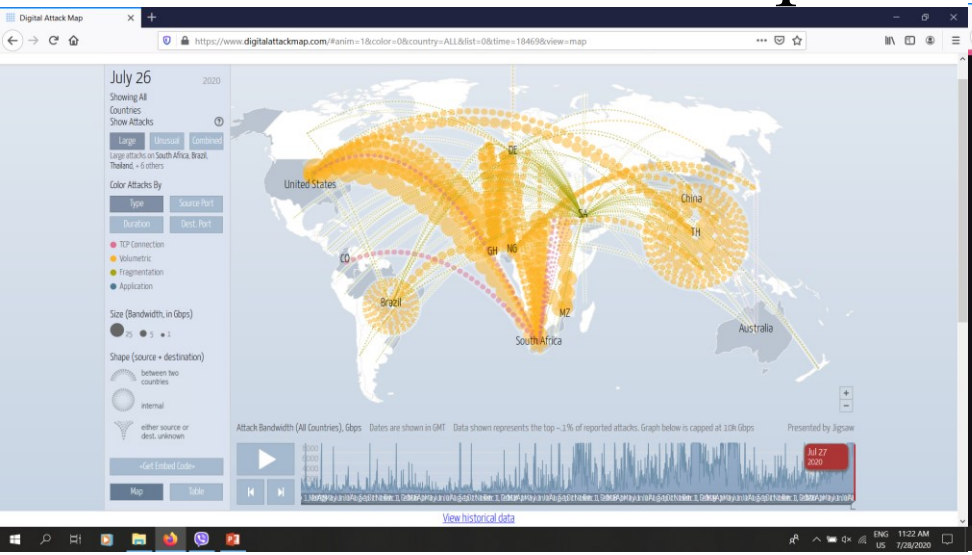
Безжичните мрежи нарастват по брой и се развиват ежедневно.

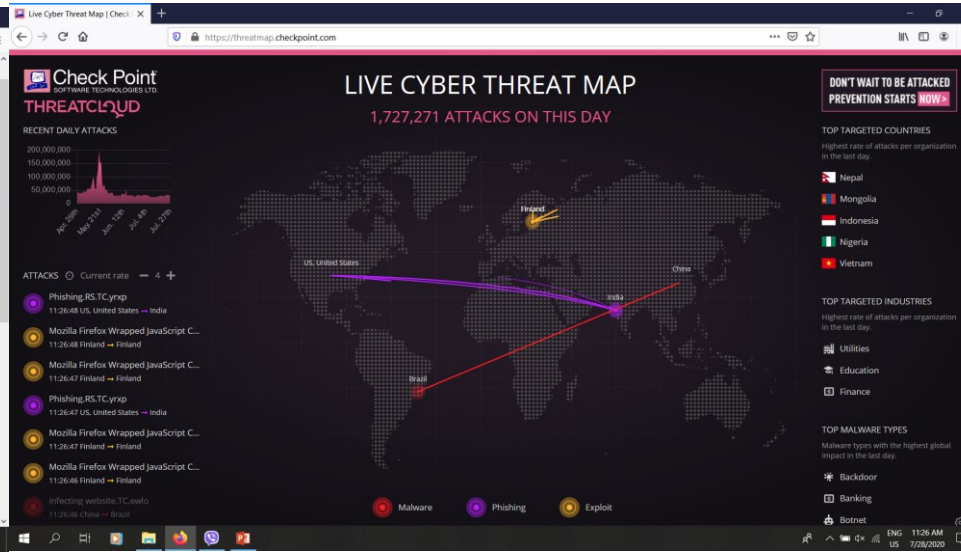
Фактите

Мрежите:

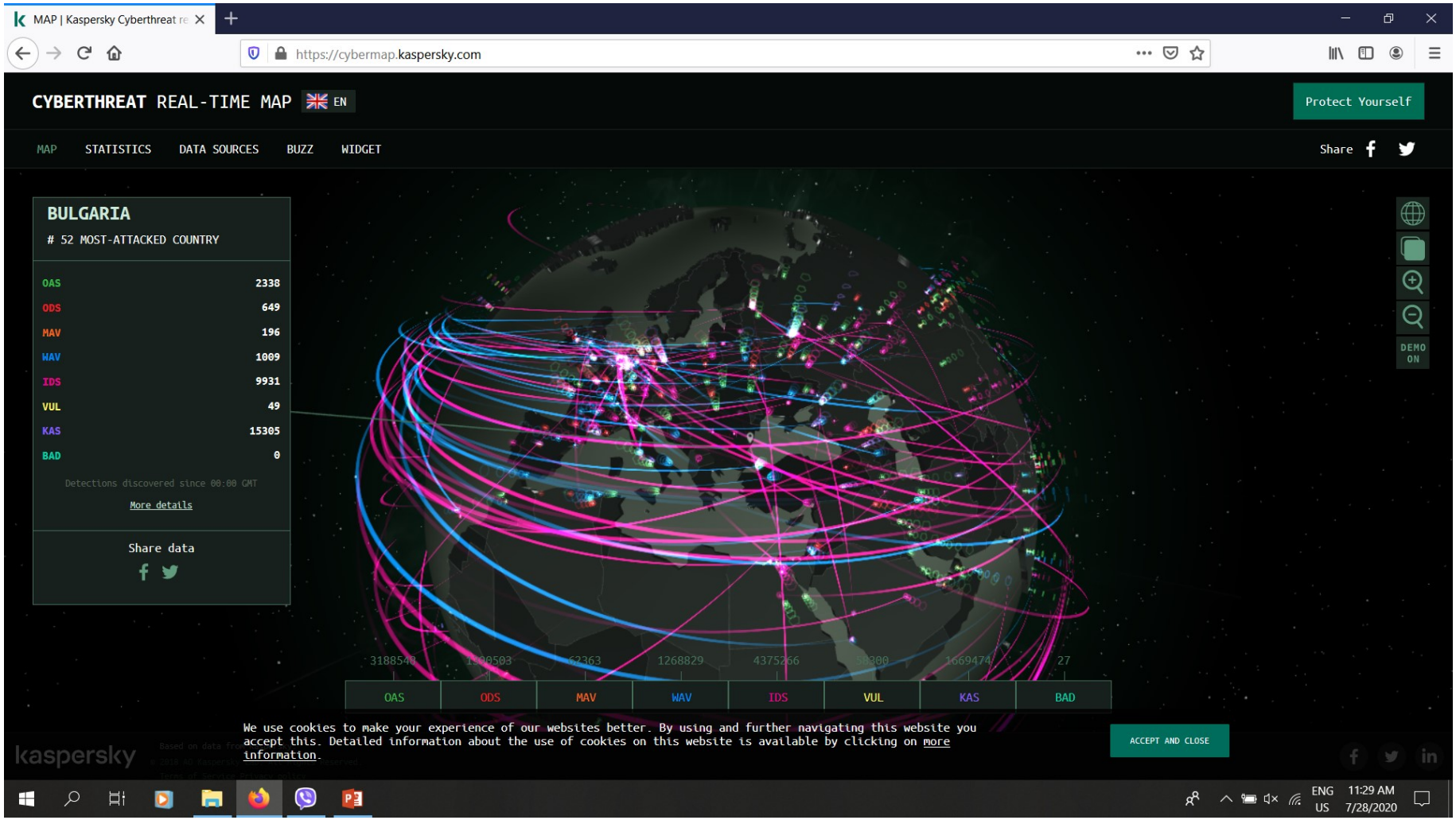
- се разрастват ежедневно,
- наблюдават се трудно,
- атакуват се все по-често.

Типовете атаки се развиват също ежедневно.



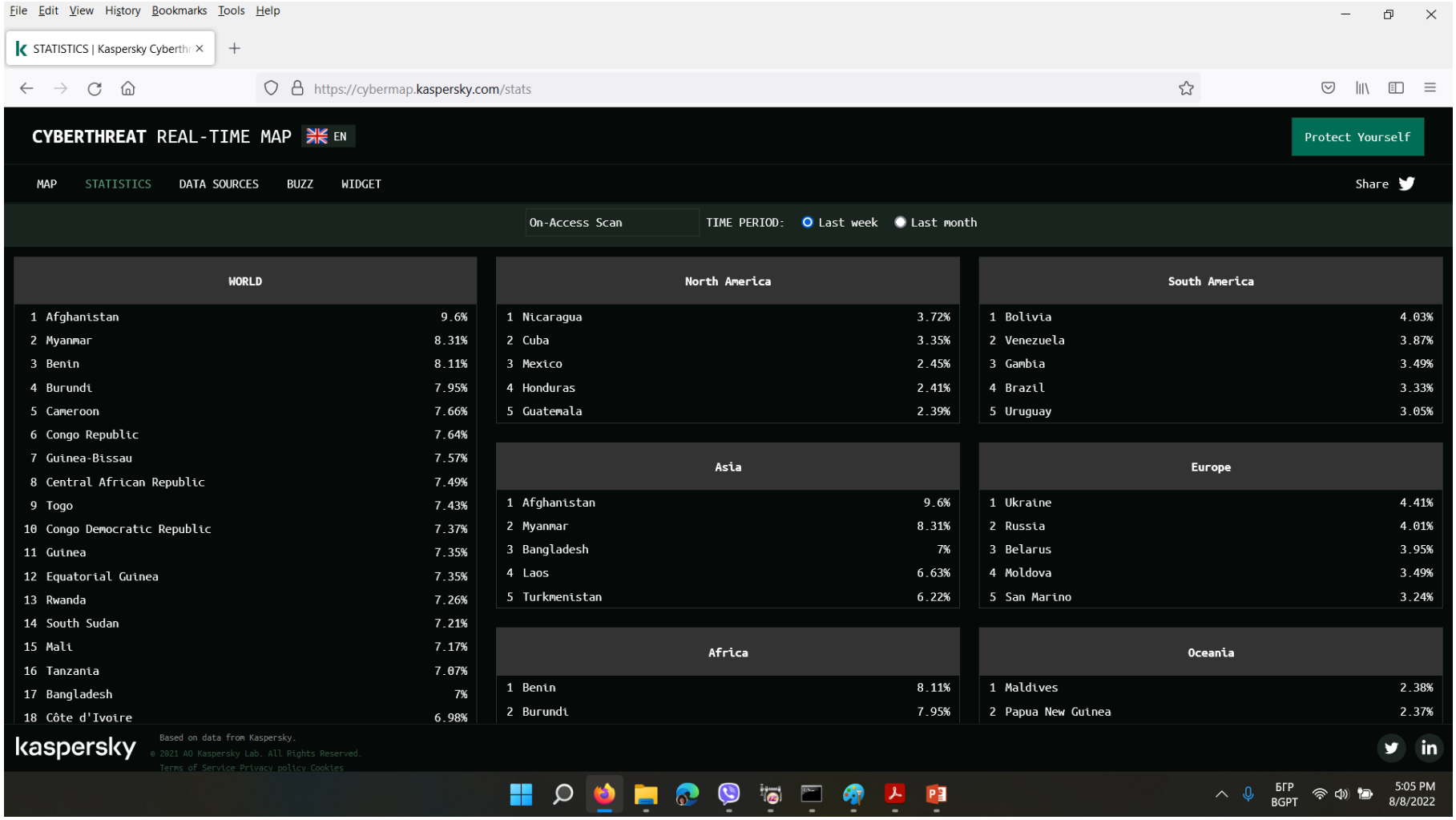


Мрежови атаки по тип атака 2020г



- През 2022г. България вече е на 56-то място

Мрежови атаки по държави 2022г



Фактите

Ако се прави компромис със сигурността, може:

- Да се загубят данни без да се знае чия е отговорността за това.
- Да бъде откраднатата информация без да се знае чия е отговорността за това.
- Могат да бъдат изтрити операционната система и конфигурационните файлове на мрежовите устройства и да се загуби свързаността в мрежата.

Организации за мрежова сигурност

Уязвимости

- Технологични
  - TCP/IP протоколи
  - Операционна система
  - Мрежово оборудване
- В конфигурирането
  - Правилно конфигуриране на компютрите
  - Правилно конфигуриране на мрежовите устройства
- В политиките за сигурност
  - Ако потребителите не следват правилата на политиките за сигурност

Класове физически заплахи

- Хардуерни
  - физически да се развалят сървъри, рутери, суичове, окабеляване, работни станции
- От обкръжението
  - Твърде високи или твърде ниски температури или твърде сухо или твърде влажно.
- Електрически
  - Пикове в напрежението, поднапрежение, шум в сигнала, загуба на захранване
- При експлоатация
  - лошо поведение на компонентите – електростатични разряди, липса на резервни части, лошо окабеляване, лошо означаване на етикетите на кабелите

Информационна сигурност ≠ Мрежова сигурност

Информационната сигурност е наука за осигуряване на:

- конфиденциалността,
- интегритета,
- достъпността (наличност) и
- невъзможността за отказ от авторство

на информацията.

Конфиденциалност

- Информацията, която се обменя между отделните потребители да остане лична – да не се вижда от останалите.
- Да се позволява достъп до информацията единствено на определените за това потребители.

- Достъпът да се дефинира като възможност за изпълнение на дейностите:
  - четене,
  - писане,
  - промяна,
  - копиране
  - преместване,
  - изтриване на информацията.

Интегритет

- Информацията трябва да бъде:
  - истинна,
  - актуална,
  - цялостна (в пълен обем).

- Постига се, когато обработката на информацията се извършва от определен потребител по определен начин.

Достъпност

- Възможността определените потребители за определените цели да работят с информацията.
- Услугите и ресурсите да бъдат налични по всяко време.

Невъзможност за отказ от авторство

- Невъзможността потребителят да отрече извършените от него действия с информацията.

Сигурност–Продуктивност

Сигурността се разглежда като обратно пропорционална на **продуктивността** защото:

- Мерките за защита ограничават функционалността на системата.
- По-голямата сигурност изисква повече средства.

Стандарти, касаещи защитата

- ISO 7498-2 SecurityArchitecture
  - OSI защитена архитектура
- ISO 9594-8
  - насоки за автентификация (X.509)
- ISO 10181
  - OSI насоки за защита на информацията
- ISO/IEC 27002
  - за управление на сигурността
- ISO/IEC 27004
  - за система от контроли и контролни механизми, използвани за осигуряване на ефективно функциониране на управлението на сигурността.

Стандарти по сигурност ISO/IEC 27002

ISO/IEC 27002 е практическо ръководство как да се постигне ефективна сигурност и се състои от 12 секции:

1. **Оценяване на риска**
2. **Политики за сигурност**
3. **Организация за информационна сигурност**
4. **Управление на активи**
5. **Сигурност на човешките ресурси**
6. **Сигурност на физическото обкръжение**
7. **Комуникационно и операционно управление**
8. **Контрол на достъпа**
9. **Придобиване, разработване и поддръжка на информационни системи**
10. **Управление на инцидентите в информационната сигурност**
11. **Управление на непрекъсваемостта на работа**
12. **Услужливост на системата**

Политики за информационна сигурност

Това е документ (или съвкупност от документи), който определя изискванията и целите при защитата на информацията, без да се навлиза в детайли, как те ще се постигат.

Създаване и управление на политиките за информационна сигурност

Необходимости:

- Какво да бъде защитено;
- От какво да бъде защитено;
- С какво да бъде защитено;
- Как да се работи с информационната система;
- Какви да са реакциите при инциденти и външни влияния.

Отговорности:

- Отговорности на управлението;
- Роля на специалистите;
- Подготовка на служителите.

Цели на политиките за сигурност

- Информират потребители и персонал за задълженията им и изискванията, които трябва да съблюдават за сигурността на информацията, с която боравят.
- Посочват конкретните механизми, с които ще се постигне тази сигурност.
- Осигуряват базови насоки за опазване, конфигуриране и защита на компютрите в мрежата.

Изисквания към политиките за информационна сигурност (ИС)

- Да са ориентирани към функционалността на организацията;
- Да са лесни за разбиране;
- Да са приложими и необходими;
- Да са адекватни;
- Да може да се контролира изпълнението им;
- Да са активни;
- Да са гъвкави;
- Да са кратки.

Общи политики за ИС

- Тестване на подсистемата за сигурност на системата;
- Документиране на изискванията;
- Наблюдение, контрол и възстановяване на системата;
- Анализ на процеса за влизане (логване) в системата;
- Въвеждане на отговорности на потребителя;
- Въвеждане на отговорности на организацията;
- Сигнализиране за нарушения в сигурността и определяне на източниците им;
- Запознаване с компютърните престъпления и анализа им.

Интернет политики за ИС

- Анализ на рисковете в Интернет;
- Въвеждане на отговорности на администратора;
- Въвеждане на отговорности на потребителя;
- Използване на VPN и тунели.

Политики за ИС на ел.поща

- Определяне на правила за работа с електронната поща;
- Администриране на електронната поща;
- Неизползване на стандартна електронна поща за класифицирана информация.

Политики за ИС срещу вреден софтуер (вируси, червеи, троянски коне и др.)

- Анализ на необходимостта за защита;
- Определяне на типа за защита (превантивна, при откриване, коригиране);
- Организиране на контрол на софтуера по минимум три начина;
- Въвличане на потребителя в борбата с вредния софтуер.

Политики за ИС за криптиране

- Използване на легални и оторизирани източници на криптоалгоритми;
- Осъществяване на управление на криптирането;
- Контрол на криптираните данни;
- Контрол при генерацията на ключовете;
- Осъществяване на управление на ключовете.

Политики за ИС за софтуер

- Контрол на процесите при разработване на софтуер;
- Разделяне на разработването на софтуера на части;
- Софтуера да се изработва от класифицирани специалисти;
- Извършване на тестване и създаване на документация на софтуера;
- Периодичен контрол и управление на конфигурирането.

Политики за ИС се описват в:

- Стандарти
- Директиви
- Процедури

Политики за ИС в стандарти

- Разработват се за осигуряване на съвместимост на подсистемите за информационна сигурност и определяне на единни правила за информационна сигурност.
- Ако организацията реши да приеме определен стандарт, той става задължителен при:
  - Изграждането,
  - Управлението,
  - Използването на подсистемата за информационна сигурност.

Политики за ИС в директиви

- Директивите са основни препоръки за информационна сигурност, обикновено базирани на стандарти и представляват ръководство за внедряване на стандарти.
- Има препоръки, които не са задължителни и могат да не се прилагат.

Политики за ИС в процедури

- Те са технически инструкции, които на ниско ниво осигуряват постигането на стратегическата цел, заложена в политиките за информационна сигурност.
- Те се базират на стандартите и директивите и внедряват политиките.
- Процедурите се изграждат от технически специалисти.

Области, обхванати от стандарти, директиви и процедури

- Отчетност на контрола;
- Физически контрол и контрол на околната среда;
- Административен контрол;
- Контрол на достъпа до информационната система;
- Контрол на оперирането с информационната система;
- Криптиране;
- Планиране на развитието на информационната система;
- Действие при инциденти.

Стандарт ISO/IEC 27004

- Ефективността на ИС, създадена и експлоатирана на база специфицираните в ISO 27001 изисквания и контроли за осигуряване на сигурността, се оценява по методика, предложена в ISO 27004
- ISO 27004 дава инструкции за разработване на Програма за измерване на информационната сигурност (ПИИС -Information Security Measurement Program):
  - да подпомага ръководството при идентифициране и оценка на несъответстващите и неефективни процеси по сигурността,
  - Да създава контроли за приоритизиране на действия, свързани с подобряване или промяна на тези процеси.
- ISO 27004 подпомага организацията да предостави доказателства за своите възможности за изпълнение на процесите „Преглед на управлението” и „Управление на риска за сигурността на информацията”.

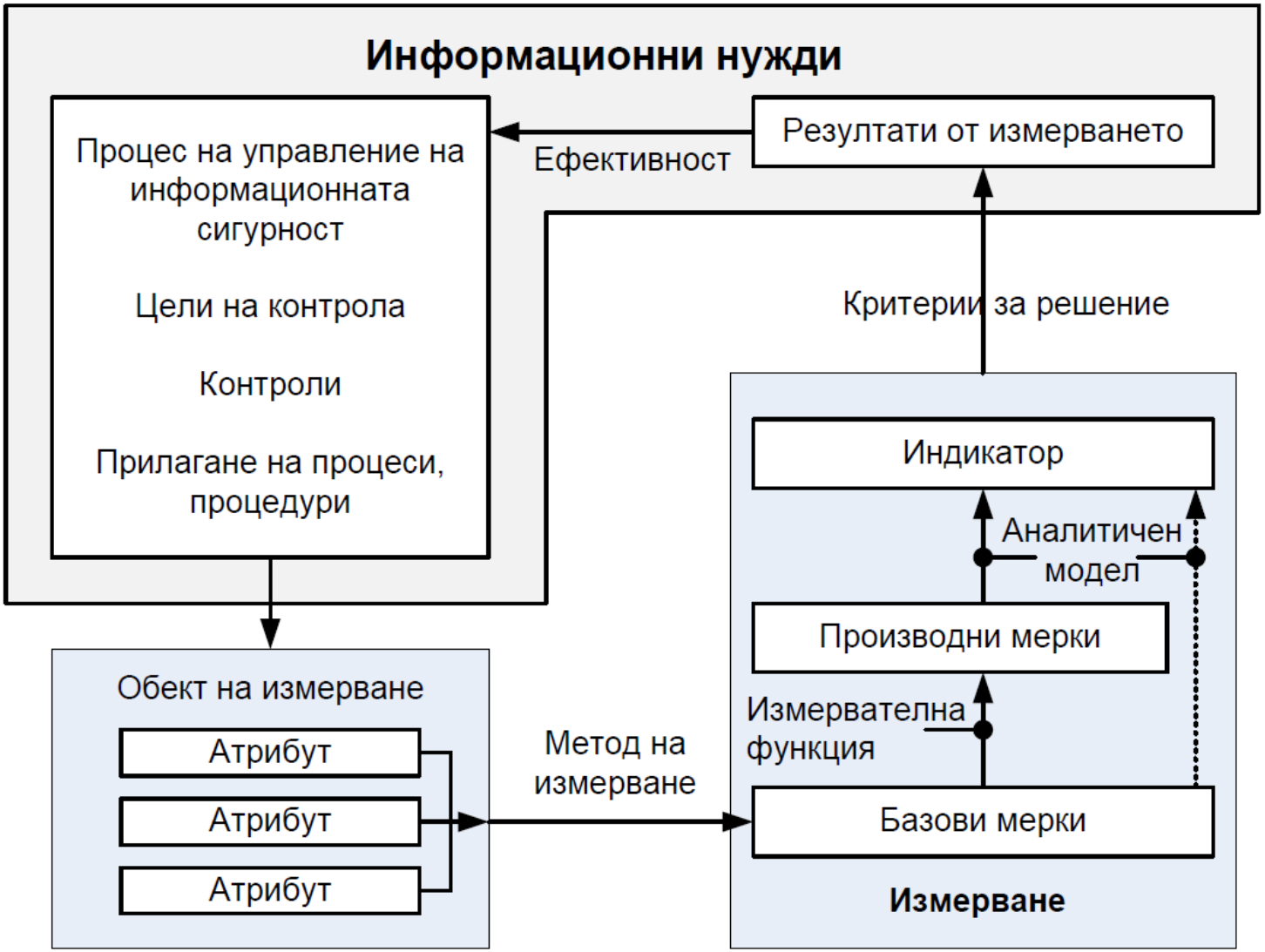
ISO/IEC 27004-предназначение

- ISO/IEC 27004 е практическо ръководство как да се създаде схема за подготовка и реализация на система за измерване на информационната сигурност:
- Дейности:
  - разработване на система от мерки (т.е. базови мерки, производни мерки и индикатори);
  - създаване и прилагане на ПИИС;
  - събиране и анализ на данните;
  - обработване на резултатите от измерванията;
  - разпространяване на обработените резултати от измерванията сред съответните заинтересовани страни;
  - използване на резултатите от измерванията като фактори, допринасящи за вземане на решения по отношение на СУИС;
  - използване на резултатите от измерванията за идентифициране на нуждите от подобрения на използваната СУИС, включително нейните обхват, политики, цели, процеси и процедури;
  - улесняване на постоянното подобряване на ПИИС.

ISO/IEC 27004 - обхват

- измервателни цели
  - ролята на информационната сигурност в поддържането на цялостната бизнес дейност на организацията ;
  - рисковете, пред които е изправена.
- измервателна структура
  - базирана на предложения в стандарта Модел за измерване на информационната сигурност (МИИС -Information Security Measurement Model);
  - осигурява обективни, повторяеми и полезни резултати.

Модел за измерване на информационната сигурност



Риск

- Рискът е възможността да се случи нещо вредно на изградената мрежа и предлаганите в нея услуги.
- Той е вероятностна величина и като такава стойността му е в диапазона [0,1].
- Граничните състояния са:
  - 0 - невъзможно е да се случи,
  - 1 - задължително се случва.

Основни типове риск

- Физическа повреда при бедствия и аварии;
- Рискове произтичащи от служителите:
  - измама,
  - саботаж,
  - неправилна употреба на информацията,
  - кражба,
  - нерегламентирано предоставяне на вътрешна информация,
  - тенденциозно разрушаване на данните;
- Вътрешни и външни атаки;
- Грешки в системния и приложен софтуер.

Анализ на риска

- Откриване и идентифициране на риска;
- Определяне на вероятността за случване на събитието;
- Определяне на възможната вреда.

Откриване и идентифициране на риска

- Прави се оценка до каква степен определени фактори влияят на ИС.
- На базата на откритите уязвимости на ИС се прави списък на рисковете.
- Един риск може да съответства на една или няколко уязвимости или на една уязвимост да съответстват няколко риска.

Определяне на вероятността за случване на събитието

- На база на статистика за открити уязвимости;
- На база познаване на заплахите;
- Чрез оценка на риска от възникване на заплаха.

Определяне на възможната вреда

- За да се даде количествена стойност на вредата е необходимо да се определят засегнатите информационни и неинформационни активи и да се определи тяхната стойност.

- Рискът може да се ограничи, но не и да се елиминира.

Стойност на информационните активи

Сума от:

- Цената на придобитата и разработена информация;
- Цената за поддръжка и защита;
- Стойност на информацията за собствениците и легалните потребители;
- Стойност на информацията за конкурентите;
- Цена на интелектуалната собственост;
- Разходите за възстановяване на загубената информация;
- Загубите от намалената продуктивност, ако информацията не е достъпна;
- Последиците, ако информацията е компрометирана.

Стойност на неинформационните активи

Сума от:

- Цената за закупуване на ново оборудване;
- Стойността на ремонта на повреденото оборудване.

Количествен анализ на риска

- Дава количествена стойност на риска (обикновено в пари).

- Изчислява се цената на засегнатите активи.

Качествен анализ на риска

- Използват качествени показатели:
  - човешки живот,
  - национална сигурност,
  - пропуснати ползи и др.
- Представя се с относителни стойности.
- Получава се с индиректни механизми:
  - Експертно мнение,
  - Опит,
  - Интуиция.

Управление на риска

Включва:

- Анализ на риска;
- Намаляване на риска до допустимо ниво;
- Задържане на риска на допустимото ниво.

Контрамерки за риска

Параметри:

- Ефективност на противодействие на риска;
- Влияние върху продуктивността на решенията;
- Цена на средствата за защита;
- Съвместимост с другите елементи на организацията;
- Стойност на проектирането и тестването;
- Цена на внедряването;
- Изисквания за поддръжка и възстановяване;
- Стойност при употреба.

Процесът е цикличен

- Откриват се уязвимостите
- Оценяват се по скала
- Тества се решението и ако няма ефект за намаляване на риска – започва се процесът отново

Въпроси ?

Благодаря за вниманието !