Тема 3

Стандарти, регулации, политики и законова рамка

Увод

- Като важна част от въпросите касаещи информацията, информационната сигурност е предмет на управление на различни **нива**.
- Информационната сигурност може да бъде разглеждана в **четири** аспекта обект на управление.
- Първият е от **технически характер**, вторият е **управленски**, на трето място е **институционална** и четвъртото стои **държавното управление**.
- За да се повиши нивото на информационна сигурност се залага на **увеличаване** степента на прилагане на стандартите, регулациите, законовите разпоредби и т.н.

Стандарти

- Съществуват множество стандарти или работни рамки, набори от добри практики. Те са разработени и публикувани от международно признати организации и приети от професионалистите по информационната сигурност вкл. и в България.
- Най-известните от тях са:

- Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO) 27001 и 27002
- National Institute of Standards and Technology (NIST) стандарти

Security controls

- Основа единица в ИС – системата от контроли може да бъде имплементирана като: стандарт, работна рамка, добри практики, нормативна уредба, инструкция или др.
- Всеки вид защита или противодействие, използвани за избягване, откриване, противодействие или минимизиране на рисковете за сигурността на физическото имущество, информация, компютърни системи или други активи, се счита за контрол на сигурността. *
- Те включват всякакъв вид политика, процедура, техника, метод, решение, план, действие или устройство, предназначени да помогнат за постигането на тази цел. Разпознаваемите примери включват защитни стени, системи за наблюдение и антивирусен софтуер. **

* https://www.ibm.com/topics/security-controls

** What Are Securit… https://www.f5.com/labs/articles/education/what-are-security-controls

Типове контроли за сигурност *

- Контролът за физическа сигурност включва такива неща като ограда на периметъра на центъра за данни, брави, жива охрана, карти за контрол на достъпа, биометрични системи за контрол на достъпа, камери за наблюдение и сензори за откриване на проникване.
- Дигиталните контроли за сигурност са неща като потребителски имена и пароли, двуфакторно удостоверяване, антивирусен софтуер и защитни стени.
- Контролите за киберсигурност включват всичко, специално проектирано за предотвратяване на атаки срещу данни, включително смекчаване на DDoS и системи за предотвратяване на проникване.
- Контролите за сигурност в облака включват мерки, които се предприемат в сътрудничество с доставчик на облачни услуги, за да се осигури необходимата защита за данни и услуги. Ако организацията използва облачни услуги, трябва да се отговаря и на техните корпоративни или бизнес изисквания за сигурност и индустриални разпоредби.

* https://www.ibm.com/topics/security-controls

COBIT

- COBIT е работна рамка разработена от ISACA, Асоциация за одит и контрол на информационните системи през 1996г.
- ISACA е широко призната независима IT организация, и нейните COBIT препоръки се използват от ИТ професионалистите в много организации.
- COBIT е общ стандарт за IT сектора, но някои практики за сигурност са вградени в него. COBIT съдържа набор от насоки за информационна сигурност, на по-високо ниво от серията ISO 27000.
- https://www.isaca.org/resources/cobit

COBIT – ключови концепции

1. Всяка организация се нуждае от система за управление, за да задоволи нуждите на заинтересованите страни и да генерира стойност от използването на ИТ.

2. Системата за управление на ИТ на организацията е изградена от редица компоненти, които могат да бъдат от различни типове и които работят заедно по холистичен начин.

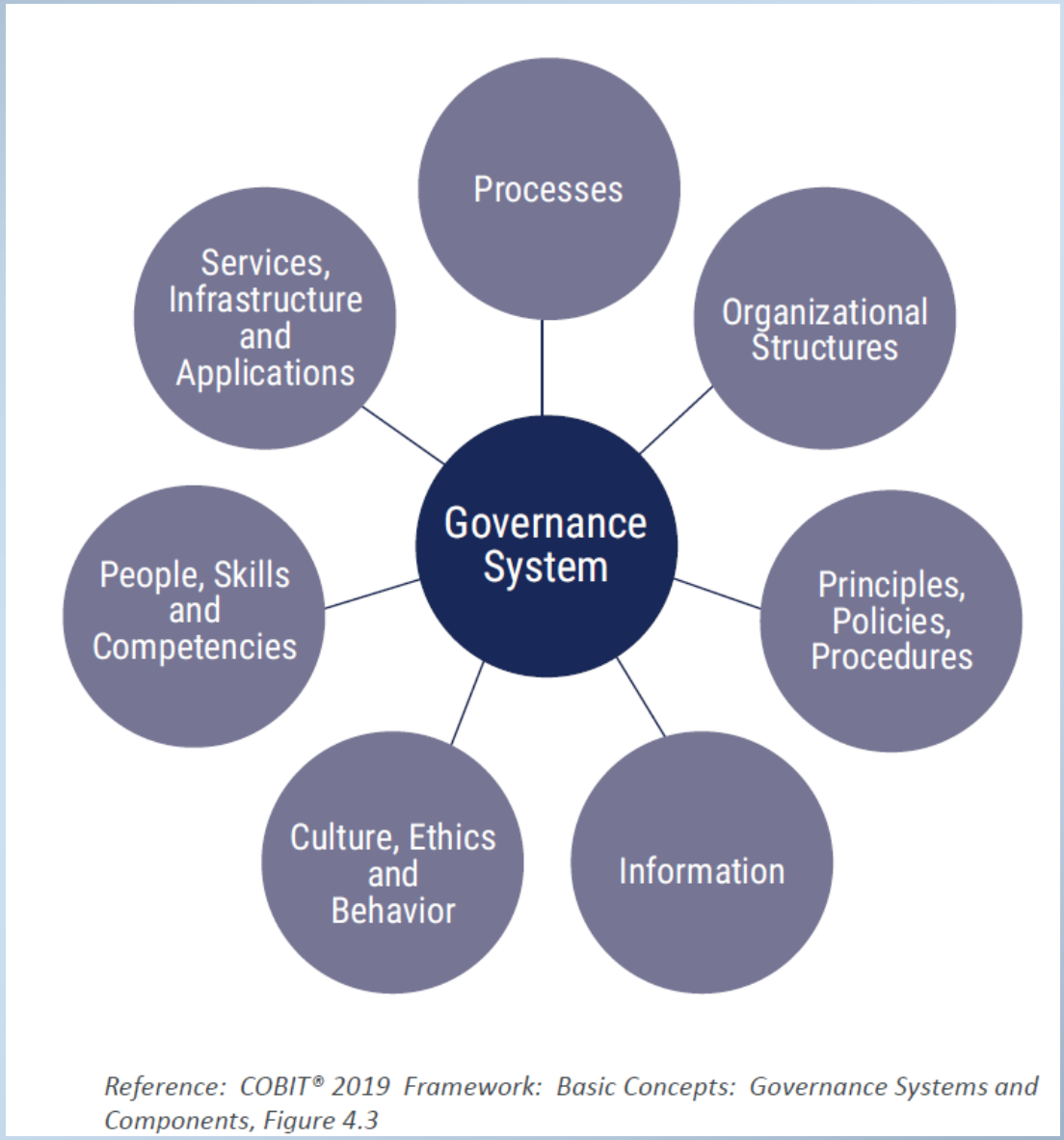
3. Системата на управление трябва да бъде динамична. Това означава, че всеки път, когато един или повече от проектните фактори се променят, трябва да се вземе предвид въздействието на тези промени върху системата EGIT.

4. Системата за управление трябва да прави ясно разграничение между дейности и структури за управление.

5. Системата за управление трябва да бъде съобразена с нуждите на организацията, като се използва набор от дизайнерски фактори като параметри за персонализиране и приоритизиране на компонентите на системата за управление.

6. Системата за управление трябва да обхваща организацията от край до край, като се фокусира не само върху ИТ функцията, но и върху всички технологии и обработка на информация, които предприятието въвежда, за да постигне целите си.

COBIT 2019
https://www.isaca.org/resources/cobit



Reference: COBIT® 2019 Framework: Basic Concepts: Governance Systems and Components, Figure 4.3

COBIT Information Security Policies

Според тази работна рамка политиките трябва да засягат следните направления:

- Information security policy
- Access control policy
- Personnel information security policy
- Incident management policy
- Asset management policy

БДС ISO/IEC 27000

- Серия международни стандарти в областта на информационната сигурност, които съдържат най-добрите практики и препоръки за създаване, развитие и поддържане на системи за управление на сигурността на информацията.
- Например: Стандартът ISO 27001 предоставя рамката за изграждане на система за защита на чувствителната бизнес информация. Целта на стандарта е постигане определено ниво на защита, чрез осигуряване на следните характеристики на информацията:
- **поверителност** – само оторизирани лица да имат достъп до съответната информация;
- **цялостност** – само оторизирани лица да имат възможност за промяна на информацията;
- **наличност** – достъпност на оторизираните служители до необходимата им информация.

БДС ISO/IEC 27001:2014 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания

- A.5: Политики за сигурност на информацията (2 контроли)
- A.6: Организиране на сигурността на информацията (7 контроли)
- A.7: Сигурност на човешките ресурси - 6 контроли, които се прилагат преди, по време или след работа
- A.8: Управление на активи (10 контроли)
- A.9: Контрол на достъпа (14 контроли)
- A.10: Криптография (2 контроли)
- A.11: Физическа сигурност и сигурност на заобикалящата среда (15 контроли)
- A.12: Сигурност на работата (14 контроли)
- A.13: Сигурност на комуникациите (7 контроли)
- A.14: Придобиване, разработване и поддържане на системи (13 контроли)
- A.15: Взаимоотношения с доставчици (5 контроли)
- A.16: Управление на инциденти със сигурността на информацията (7 контроли)
- A.17: Аспекти на сигурността на информацията при управление на непрекъснатостта на дейността (4 контроли)
- A.18: Съответствие (8 контроли)

БДС ISO/IEC 27000 (изменя се с годините)

- БДС ISO/IEC 27002:20xx Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията;
- БДС ISO/IEC 27003:20xx Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията;
- ISO/IEC 27004:20xx Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване;
- БДС ISO/IEC 27005:20xx Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията;
- БДС ISO/IEC 27006:20xx Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията.

NIST

- Националният институт за стандарти и технологии (NIST), публикува набор от “Специални Публикации“ за подпомагане на индустрията, правителствата и академичните организации със следване на добрите практики. В областта на информационната сигурност това са т.н. серии 800 и 1800 публикации (https://csrc.nist.gov/publications).
- Някои от засегнатите аспекти са:
  - Контрол на достъпа;
  - Информираност и обучение;
  - Одит и отчетност;
  - Оценка на сигурността и оторизация;
  - Планиране;
  - Идентифициране и удостоверяване;
  - Реакция на инцидент;
  - Поддръжка;
  - Сигурност на персонала и други.

NIST

- Наред с разгледаните публикации е разработена и работна рамка (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)
- Основните функции в работната рамка са:
  - Идентифициране – Разработете организационно разбиране за управление на риска за киберсигурността за системи, хора, активи, данни и възможности.
  - Защита – Разработете и приложете подходящи предпазни мерки, за да гарантирате предоставянето на критични услуги.
  - Откриване – Разработване и прилагане на подходящи дейности за идентифициране на възникване на събитие за киберсигурност.
  - Реакция – Разработете и приложете подходящи дейности за предприемане на действия по отношение на открит инцидент с киберсигурността.
  - Възстановяване – Разработете и приложете подходящи дейности за поддържане на планове за устойчивост и за възстановяване на всички способности или услуги, които са били нарушени поради инцидент с киберсигурността.

GDPR или Регламент (ЕС) 2016/679 на Европейския парламент

- Отнася се до защитата на физическите лица във връзка с обработването на личните им данни.
- GDPR въвежда нови правила при обработване на личните данни.
- Влиза в сила на 25 май 2018 г.
- **Задължителен** за всички компании, които обработват лични данни.
- Той засяга и компании извън ЕС, които обработват данни на европейски граждани.
- Неговата основна цел е да върне на гражданите контрола върху техните лични данни.
- Вече има наложени множество глоби за нарушаване на регламента. Например през 2021 г. Амазон е глобена 746 млн. евро за събиране на повече от необходимите данни, а през 2022г. Инстаграм е глобена с 405 млн. евро за лични данни(имейл, тел. номер) на тийнейджъри, които са били видими.

Определение

„**лични данни**“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като: име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

GDPR

Категории лични данни:

- „обикновени“ лични данни – имена, адрес, електронна поща, IP адрес и т.н.;
- Единен Граждански Номер;
- чувствителни лични данни – данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

GDPR

Физическите лица **имат право**:

- Да коригират грешки в личните си данни.
- Да трансферират личните си данни
- Да изискват информация кой обработва личните им данни.
- Да изтриват личните си данни.

GDPR

Всички администратори на лични данни трябва:

- При необходимост да получат **съгласие** за събирането и обработката на лични данни.
- Да **защитават** личните данни прилагайки всякакви мерки за сигурност - криптиране, Data Loss Prevention (DLP) решения (Symantec Data Loss Prevention, Trustwave Data Loss Prevention, McAfee Total Protection, Digital Guardian Endpoint DLP), антивирусен софтуер
- Да **уведомят** Надзорния орган в случай на пробив и кражба на лични данни.
- Да водят **регистър** при обработка на личните данни.

Data protection officer

Длъжностно лице по защита на данни са задължени да имат:

- Публичен орган или орган на местно самоуправление.
- Администратори, които извършват системно и мащабно наблюдение на субектите на данните.
- Администратори, които извършват мащабно обработване на специални (чувствителни) лични данни.

Отговорности:

- **УПРАВЛЕНИЕ НА РИСКА ПО ОТНОШЕНИЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ**
- Да обучават служителите как да обработват личните данни и да спазват политиките за информационна сигурност
- Да актуализират политиките за информационна сигурност при необходимост.
- Да актуализират правилата при обработка на личните данни при необходимост.

ЗАКОНОВА РАМКА В БЪЛГАРИЯ

- Закон за киберсигурност
- Наредба за минималните изисквания за мрежова и информационна сигурност

(виж на https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf)

- Закон за електронната идентификация
- Закон за защита на личните данни
- Закон за ел. документ и ел. подпис
- Закон за защита на класифицираната информация
- Закон за ел.търговия
- Закон за ел.съобщения
- Закон за ел.управление

Национална стратегия за киберсигурност „Киберустойчива България 2020”

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Прилага се за:

1. административните органи;
2. операторите на съществени услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на съществени услуги;
3. доставчиците на цифрови услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на цифрови услуги;
4. лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги по смисъла на Закона за киберсигурност, когато тези лица предоставят административни услуги по електронен път;
5. организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на Закона за киберсигурност, когато тези организации предоставят административни услуги по електронен път.

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Включва:

1. изисквания за минималните мерки за мрежова и информационна сигурност;
2. препоръчителни мерки за мрежова и информационна сигурност;
3. правила за извършване на проверките за съответствие с изискванията на тази наредба;
4. редът за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за киберсигурност;
5. образец на уведомленията за инциденти

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Политика за сигурност

Чл. 4. (1) Субектите разработват и приемат собствена политика за мрежова и информационна сигурност, която се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

(2) Политиката съдържа стратегическите цели на Субекта за мрежовата и информационната сигурност и подхода за постигането им в съответствие с общите му стратегически и оперативни цели, нормативните актове и договорите, текущите и потенциалните вътрешни и външни заплахи за постигането на тези цели и за игурността на информацията.

(3) Политиката има отношение към или включва всички съответни специфични политики за сигурност на информационните и комуникационните системи, като обмен на информация, използване на мобилни устройства, работа от разстояние, използване на криптографски механизми, управление на достъпите и автентикацията, разработване на нови системи, управление на инциденти, взаимоотношение с трети страни, повишаване на квалификацията на служителите и на осведомеността по отношение на мрежовата и информационната сигурност и др.

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Класификация на информацията

Чл. 6. (1) Субектът приема вътрешни правила по смисъла на чл. 5, ал. 1, т. 6 и 7 за класификация на информацията, които указват как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага организацията. Препоръчителна класификация е дадена в приложение № 2.

(2) Правилата по ал. 1 гарантират достатъчна, адекватна и пропорционална на заплахите защита на информацията с оглед на нейната важност, чувствителност и на нормативните изисквания към нея.

(3) Класификацията по ал. 1 се прилага и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията, като към тях трябва да се прилагат подходящи механизми за защита, съответстващи на идентифицираните от Субекта заплахи.

(4) Нивото на класификацията трябва да е подходящо нанесено върху документираната информация.

(5) За класификацията по ал. 1 не се допуска използването на нивата на класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация, както и техният гриф. (6) Информацията без класификация е достъпна за общо ползване при спазване на стандартните правила за авторски права и към нея не се прилагат механизми за защита.

(7) При обмен на информация се използва класификация TLP (traffic light protocol) съгласно приложение № 2.

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Класификация на информацията – 4 нива

TLP (traffic light protocol) – създаден от Cybersecurity and Infrastructure Security Agency (CISA) използва се при обмен на информация – има промяна от 2022г.

[TLP-RED] – Само за определени получатели: в контекста на една среща например информацията се ограничава до присъстващите на срещата. В повечето случаи тази информация се предава устно или лично.

[TLP-AMBER] – Ограничено разпространение: получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът "необходимост да се знае". Честа практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.

[TLP-GREEN] – Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.

[TLP-WHITE] – Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Управление на риска

Чл. 7. (1) Субектът извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите, влизащи в обхвата на тази наредба.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т. 6, в който са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.

(3) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от административния орган, съответно от ръководителя на субекта по чл. 1, ал. 1, т. 2 – 5, и е достъпна за лицата, на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3.

(4) На основание на анализа и оценката на риска Субектът изготвя план за намаляване на неприемливите рискове, който да включва минимум:

1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - извадка

- Чл. 25г. (Нов - ДВ, бр. 17 от 2019 г.) Администратор или обработващ лични данни може да копира документ за самоличност, свидетелство за управление на моторно превозно средство или документ за пребиваване само ако това е предвидено със закон.
- Чл. 25ж. (Нов - ДВ, бр. 17 от 2019 г.) (1) Свободен публичен достъп до информация, съдържаща единен граждански номер или личен номер на чужденец, не се допуска, освен ако закон предвижда друго.

  (2) Администраторите, предоставящи услуги по електронен път, предприемат подходящи технически и организационни мерки, които не позволяват единният граждански номер или личният номер на чужденец да е единственото средство за идентификация на потребителя при предоставяне на отдалечен достъп до съответната услуга.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - извадки

Чл. 37а. (Нов - ДВ, бр. 17 от 2019 г.) (1) Администраторът или обработващият лични данни може да откаже пълно или частично упражняването на правата на субектите на данни по чл. 12 - 22 от Регламент (ЕС) 2016/679, както и да не изпълни задължението си по чл. 34 от Регламент (ЕС) 2016/679, когато упражняването на правата или изпълнението на задължението би създало риск за:

1. националната сигурност;

2. отбраната;

3. обществения ред и сигурност;

4. предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществения ред и сигурност;

5. други важни цели от широк обществен интерес и по-специално важен икономически или финансов интерес, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;

6. защитата на независимостта на съдебната власт и съдебните производства;

7. предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регулираните професии;

8. защитата на субекта на данните или на правата и свободите на други лица;

9. изпълнението по гражданскоправни искове.

(2) Условията и редът за прилагане на ал. 1 се определят със закон и в съответствие с чл. 23, параграф 2 от Регламент (ЕС) 2016/679.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - извадки

- Чл. 37б. (Нов - ДВ, бр. 17 от 2019 г.) (1) Субектът на данни упражнява правата по чл. 15 - 22 от Регламент (ЕС) 2016/679 чрез писмено заявление до администратора на лични данни или по друг определен от администратора начин.
- (2) Заявление може да се подаде и по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация.
- (3) Заявление може да се подаде и чрез действия в потребителския интерфейс на информационната система, която обработва данните, след като лицето е идентифицирано със съответните за информационната система средства за идентификация.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - извадки

Чл. 38. (1) (Изм. - ДВ, бр. 103 от 2005 г., изм. - ДВ, бр. 91 от 2006 г., изм. - ДВ, бр. 17 от 2019 г.) При нарушаване на правата му по Регламент (ЕС) 2016/679 и по този закон субектът на данни има право да сезира комисията в срок 6 месеца от узнаване на нарушението, но не по-късно от две години от извършването му.
(2) (Нова - ДВ, бр. 17 от 2019 г.) Комисията информира жалбоподателя за напредъка в разглеждането на жалбата или за резултата от нея в тримесечен срок от сезирането ѝ.
(3) (Изм. - ДВ, бр. 103 от 2005 г., предишна ал. 2, изм. - ДВ, бр. 17 от 2019 г.) Комисията се произнася с решение, като може да приложи мерките по чл. 58, параграф 2, букви "а" - "з" и "й" от Регламент (ЕС) 2016/679 или по чл. 80, ал. 1, т. 3, 4 и 5 и в допълнение към тези мерки или вместо тях да наложи административно наказание в съответствие с чл. 83 от Регламент (ЕС) 2016/679, както и по глава девета.
(4) (Нова - ДВ, бр. 17 от 2019 г.) Когато жалбата е очевидно неоснователна или прекомерна, с решение на комисията жалбата може да се остави без разглеждане.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - извадки

- Чл. 38а. (Нов - ДВ, бр. 17 от 2019 г.) (1) Жалбата до комисията може да се подаде с писмо, по факса или по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги.
- (2) Не се разглеждат анонимни жалби, както и жалби, които не са подписани от подателя или от негов представител по закон или пълномощие.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - Права на субекта на данни

Чл. 53. (Нов - ДВ, бр. 17 от 2019 г.) (1) Администраторът предприема необходими мерки за предоставяне на субекта на данни на информацията по чл. 54 и за кореспонденция с него във връзка с чл. 52, ал. 5, чл. 55 - 58 и 68 относно обработването на лични данни в сбита, разбираема и леснодостъпна форма, като използва ясен и прост език. Администраторът предоставя информацията по начина на постъпване на искането. Когато това е невъзможно или изисква несъразмерно големи усилия, информацията се предоставя по друг подходящ начин, включително по електронен път.

(2) Администраторът улеснява упражняването на правата на субекта на данни по чл. 52, ал. 5 и чл. 55 - 58.

(3) Администраторът отговаря на искането на субекта на данни или го информира писмено за действията, предприети във връзка с неговото искане, в срок до два месеца от получаване на искането. Срокът може да се удължи с още един месец, когато това се налага заради сложността или броя на исканията.

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - Права на субекта на данни

- Чл. 54. (Нов - ДВ, бр. 17 от 2019 г.) (1) Администраторът предоставя на субекта на данни най-малко следната информация:
- 1. данните, които идентифицират администратора, и координатите за връзка с него;
- 2. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;
- 3. целите, за които се обработват личните данни;
- 4. правото на жалба до комисията, съответно до инспектората, и координатите им за връзка;
- 5. правото да се изиска от администратора достъп до, коригиране, допълване или изтриване на лични данни и ограничаване на обработването на лични данни, свързано със субекта на данните;

ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - Права на субекта на данни

- Чл. 59. (Нов - ДВ, бр. 17 от 2019 г.) (1) Администраторът на лични данни, като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, прилага подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с този закон. При необходимост тези мерки се преразглеждат и актуализират.

- (2) Когато това е пропорционално на дейностите по обработване, мерките по ал. 1 включват прилагане от администратора на подходящи политики за защита на данните.

- (3) Чрез мерки по ал. 1 администраторът осигурява защита на личните данни на етапа на проектирането, като отчита достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването на лични данни, както и рисковете за правата и свободите на физическите лица при обработването. Мерките трябва да са съобразени с изискванията на чл. 45, планират се към момента на определяне на средствата за обработването на лични данни и се прилагат при самото обработване. Мерките може да включват псевдонимизация, свеждане на данните до минимум и въвеждане на необходими гаранции в процеса на обработване на лични данни.

- (4) Чрез мерки по ал. 1 администраторът гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, срока на съхраняването им и тяхната достъпност. Чрез тези мерки се гарантира, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

Държавни организации

- CERT Bulgaria е Националният Център за Действие при Инциденти в Информационната Сигурност.
- Основната функция на центъра е да подпомага ползвателите на услугите му в извършването на проактивни дейности за намаляване рисковете от инциденти в информационната сигурност и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали.
- Центърът предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда.
- Публикува информация за текущи заплахи.
- Може да се докладва за заплаха или атака.

Държавни организации

Държавната комисия по сигурността на информацията (ДКСИ)

- Основните направления, в които комисията работи са за **защита на класифицираната информация** в съответствие с видовете сигурност регламентирани в закона:

- персонална;
- физическа;
- документална;
- индустриална;

Изпълнителна агенция "Електронни съобщителни мрежи и информационни системи"

- Дейностите са насочени в три основни направления:

- изграждане, поддръжка, развитие, експлоатация и управление на Единната електронна съобщителна мрежа на държавната администрация и за нуждите на националната сигурност (ЕЕСМДАНС), която е част от Интегрираната комуникационно-информационна система за управление на страната и въоръжените сили;
- развитие и управление на центрове за данни, автоматизирани информационни системи и портали за достъп, изградени в изпълнение на проекти и програми в областта на информационното общество и електронното управление;
- развитие и поддръжка на Център за реакция при инциденти във връзка с информационната сигурност - CERT.

Обучение в областта на ИС

- **SANS**
  - Това е водеща международна организация занимаваща се с обучение на специалисти и мениджъри.
  - Предлага магистърски програми и всякакъв вид обучение от онлайн до посещение на място в целия свят.
  - Предлага също и много безплатни ресурси.
  - Издава всепризнати сертификати.
- **(ISC)² International Information Systems Security Certification Consortium**
  - Също водеща организация, предлагаща сходни услуги.

SANS – 20 Critical Security Controls /CIS Critical Security Controls

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

Пример как се реализира дейността Secure Network Engineering

CSC 19-1	Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.
CSC 19-2	To support rapid response and shunning of detected attacks, engineer the network architecture and its corresponding systems for rapid deployment of new access control lists, rules, signatures, blocks, blackholes, and other defensive measures.
CSC 19-3	Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet.
CSC 19-4	Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses.

Документация

Всяка програма (система) за сигурност въведена в една организация се базира на документация в следните **четири** направления:

1. Политики;
2. Стандарти;
3. Процедури;
4. Насоки/Препоръки.

. . .

- **Политика** е изявление на изискванията за сигурност на високо равнище. Политиката за сигурност е основният начин, по който очакванията за управление на сигурността са предоставени на създателите, внедрители, администратори, и потребителите на информационните системи на организацията.
- **Стандартите** определят как да се конфигурират хардуерни устройства, как да се инсталира и конфигурира софтуер и как да се използват компютърни системи и други организационни активи, за да бъдат съвместими с политиките по сигурността.
- **Процедурите** уточняват инструкциите стъпка по стъпка, за да изпълняват различни задачи, в съответствие с политиките и стандартите.
- **Насоките** са съвети за това как да се постигнат целите на политиката за сигурност, но те са предложения/препоръки, а не правила. Те са важен инструмент за комуникация, за да позволи на хората да знаят как да следват политиките.

Политики за сигурност

- **Какво е политика?** 1) Система от принципи използвани при вземане на решение. 2) Политиката е израз на намерение. 3) Политиката е набор от идеи или планове, които се използват като основа за вземане на решения. 4) План за действие.
- ***Пример: ПУ следва политика за недопускане на тютюнопушене в сградите на университета.*** *Има издадена заповед на Ректора, определени са лица, които да контролират, предвидени са санкции.*
- Политиката за сигурност е множество от правила, които потребителите да спазват когато работят с IT активи. Тя е от съществено значение и е основата за **ефективна** и **всеобхватна** програма за сигурност.
- Политика за сигурност трябва да бъде кратка и лесна за разбиране, така че всеки да може да проследи насоките, заложени в нея.
- В основната си форма, политиките за сигурност е документ, който описва изискванията за сигурност на организацията. Чрез политиката за сигурност се посочва **какво** трябва да се направи, а не как, като тук не се уточняват конкретни технически решения.

. . .

- Политиката за сигурност установява специфични очаквания за управлението, техническия персонал, както и служителите.
- Една ясна и добре документирана политика за сигурност ще определи какви **действия** да се предприемат в случай на нарушение на сигурността.
- При **липсата** на ясни политики, организациите се излагат на **риск** и често стават жертви на атаки и големи загуби.
- Политиките за сигурност се **базират** на добре направен анализ на риска, организационната структура, бизнес целите на организацията, законовата рамка в съответната страна или регион.

Субекти

- За **мениджърите**, политиката за сигурност идентифицира очакванията на висшето ръководство за ролите, отговорностите и действията, които следва да бъдат предприети от ръководството по отношение на процедурите за сигурност.
- За **техническия персонал**, политиката за сигурност изяснява, какви мерки за сигурност следва да се използват за контрол на сигурността в мрежата, за материалната база, както и на компютърни системи.
- За всички **служители**, политиката за сигурност описва как те трябва да действат при използване на компютърни системи, електронна поща, телефони и гласова поща.

Пример за политика на една фирма

1. Ангажираност на Ръководството

Настоящата политика по информационна сигурност задава рамката на система от мерки, насочени към:

- Гарантиране на ***конфиденциалност*** на информацията, чрез прилагането на одобрени ограничения върху достъпа и разкриването на информация;
- Осигуряване на ***цялостност*** на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
- Осигуряване на ***достъпност*** на информацията, чрез осигуряване на надежден и навременен достъп на информацията;
- Постигане на ***отчетност*** на информацията, чрез въвеждане на контрол върху достъпа и правата върху информационните ресурси.
- Идентифициране на адекватни ***цели*** по информационна сигурност;
- Създаване, привеждане в изпълнение и периодичен ***преглед и обновяване*** на актуален План за намаляване на риска, задаващ адекватни мерки спрямо идентифицираните цели по ИС.

Пример за политика на една фирма

2. Обхват на Системата

Системата за управление на информационната сигурност обхваща:

- Всички документи (в електронен вид и на хартия);
- Бази данни;
- Компютри, в т.ч. преносими;
- Софтуерни активи;
- Локална мрежа;
- Електронната страница на фирмата;
- Носители на информация (дискове, USB памети и др.);
- Устройства за копиране и предаване на данни;
- Комуникационни устройства;
- Инфраструктура на фирмата (електрозахранване, кабели за локална мрежа и др.);
- Персонал.

Пример за политика на една фирма

Принципи: Ръководството на фирмата ще прилага следните основни принципи при разработване, внедряване и поддържане на система за управление на информационната сигурност:
1. От законова гледна точка:
a) Осигуряване на съответствие с нормативни и професионални изисквания за конфидециалност;
b) Защита на данни и неприкосновеност на лична информация;
c) Опазване на архивите на организацията;
d) Защита на авторски права, търговска информация и други права върху интелектуална собственост.
2. От общоприетите най-добри практики за информационна сигурност:
a) Разработване на политика по информационна сигурност;
b) Разпределяне на отговорностите по информационна сигурност;
c) Обучение по информационна сигурност;
d) Докладване на инциденти, свързани със сигурността;
e) Управление непрекъснатостта на работа;
f) Дисциплинарен процес вследствие от нарушенията на политиката по сигурността.

Пример за политика на една фирма

Отговорности. За осъществяване на настоящата политика и за осигуряване функционирането, Ръководството определя следните отговорности:

- Съвет по информационна сигурност (определен със Заповед) - Формулира, преглежда и одобрява Политиката по информационна сигурност и контролира ефикасността на нейното изпълнение; .....
- Системен администратор - Отговарят за управление и поддържане на интернет свързаността в организацията, електронна поща, сървъри, локална мрежа, архивиране, техническа защита на активите (софтуер и хардуер); ....
- Отговорник по сигурността (определен със Заповед) - Координира дейностите по прилагане на Политиката и мерките по осигуряване на информационна сигурност. Отговаря, заедно с останалите членове на Съвета по информационна сигурност за изготвяне на методика за оценка на риска и за класификация на информацията, извършва оценка на риска и .....
- Собственици на информационния ресурс (информация, програми, приложения и поддържащите компютърни системи и периферия) - Участват в определяне на степента на риска, идентификацията и оценката на мерките за сигурност, правата и привилегиите за достъп до съответния ресурс. Отговарят за спазването на правилата за правилна употреба на ресурса, генерирането, събирането, обработката, ...
- Потребители - Потребителите на информационната система, се задължават да следват процедурите и инструкциите по информационна сигурност, да докладват за проблеми и инциденти в информационната система.

Примери

- Според SANS :

✓ Acceptable Use Policy

✓ Data Breach Response Policy

✓ Disaster recovery plan

✓ Business continuity plan

✓ Remote access policy

✓ Access control policy

- Пример UCLA - https://policy.ucop.edu/doc/7000543/BFB-IS-3

Процедури

- Процедурите представляват **детайлни инструкции**, стъпка по стъпка, за това как да се извърши дадена задача.
- В зависимост от това каква информация се събира и обработва могат са се изготвят **различни** процедури за работа с нея.
- Например, ако се работи с класифицирана или лична информация процедурата ще включва стъпки, където такава информация се кодира, като например се използва допълнителен софтуер.
- Процедурите се изготвят от лицата разписани в политиките (вж. отговорник по сигурността или системен администратор).

Пример за процедури

4. APACHE уеб сървър процедура за сигурност

4.1. Компилирайте и инсталирайте както следва:

4.1.1. ./configure --prefix=/usr/local/apache --disable-module=all --serveruid=

apache --server-gid=apache --enable-module=access --enable-module=log_

config --enable-module=dir --enable-module=mime --enable-module=auth

4.1.2. make

4.1.3. su

4.1.4. umask 022

4.1.5. make install

4.1.6. chown -R root:sys /usr/local/apache

4.2. След това ограничете достъпа до файловата система на процеса Apache. Първоначално създайте /chroot/httpd директория:

4.2.1. mkdir -p /chroot/httpd/dev

4.2.2. mkdir -p /chroot/httpd/etc

4.2.3. mkdir -p /chroot/httpd/var/run

Насоки/препоръки

- Насоките или препоръките **не са регулаторен документ**.
- Те са само **предложения** как да се следват политиките по сигурността.
- Те обикновено са **резултат от анализ** на добрите практики в областта и миналия опит на компанията.
- На практика те са един от най-полезните **инструменти** за повишаване на сигурността.
- В общия случай са насочени към **обикновените потребители** а не към професионалистите.

Пример – препоръки за избор на парола

- Използвайте, колкото се може повече различни символи, включително цифри и препинателни знаци.
- Използвайте малки и главни букви.
- Използвайте поне по една цифра и препинателен знак.
- За парола използвайте нещо, което лесно ще запомните.
- **Не използвайте за парола следното**:

➢ Имена - вашето, на членове на семейството или на домашни любимци;

➢ Дата на раждане;

➢ Месторождение;

➢ Телефонни номера;

➢ Думи от речник (една от атаките за разпознаване на парола е именно от речници)

Заключение

- Всички стандарти, закони, препоръки и т.н. са документи, които търпят **промяна**.
- Тази промяна е относително **честа**, а не на няколко години.
- В тази връзка всички тези документи трябва да се **актуализират** редовно на подходящ интервал.
- Нужно е всички заинтересовани да бъдат **уведомявани** за направени промени в документите.
- Най-добрия начин е **да се публикуват на Интернет страниците** на организациите (евентуално в защитени секции на тези страници).

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата стандарти и регулации. Търсенето може да направите и на чужди езици, които владеете и за други държави.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Напишете на един лист каква лична информация сте предоставяли на хора, сайтове и организации и проучете начините на защита, която прилагат.
- Ако имате съмнения, че личната Ви информация не се съхранява или обработва според изискванията на GDPR набележете мерки от Ваша страна.