СТАНДАРТИ ЗА КИБЕРСИГУРНОСТ – АНАЛИЗ И ПРИЛОЖЕНИЕ СРЕД БЪЛГАРСКИТЕ БИЗНЕС ОРГАНИЗАЦИИ

Виктория Ангелова, Ива Костадинова

Университет по библиотекознание и информационни технологии

Резюме: Стандартите по киберсигурност в българските организации се използват за установяване на ефективни мерки за защита на информацията, смекчаване на рисковете и гарантиране на поверителността, целостта и наличността на данните. Те предоставят рамка за управление на риска, разработване на политики и процедури за сигурност, прилагане на контроли и технологии, обучение на служителите и подлагане на одити за съответствие. Чрез тези стандарти организациите осигуряват надеждна защита срещу киберзаплахи и спазват регулаторните изисквания в областта на киберсигурността.

Ключови думи: киберсигурност, стандарти, България, организации.

Въведение

Стандартите за киберсигурност играят решаваща роля за опазването на информацията и защитата от киберзаплахи в българските бизнес организации. Тези стандарти предоставят рамка за установяване на ефективни мерки за сигурност, смекчаване на рисковете и гарантиране на поверителността, целостта и наличността на чувствителни данни. Разликите между тях са в основата им, обхвата им на приложение и конкретните изисквания, които те поставят пред организациите и институциите.

Този доклад представя сравнителен анализ на стандартите по киберсигурност, които се използват в България. Стандартите са групирани по вид, като са описани техните основни разлики. Целта на анализа е да предостави обобщена представа за разнообразието и приложението на стандартите по киберсигурност в България.

Методология на изследването

Методологията на проведеното изследване се базира на преглед на описаните стандарти. Анализирани са сферите на приложение на тези стандарти и разликите между стандартите в

една и съща сфера. Направен е преглед на приложението на описаните стандарти.

Резултати

Стандартите са документи, разработени с консенсус на основата на обединяване на резултатите от науката, технологиите и производствения опит. Те представляват общопризнати правила и норми и може да включват подробни технически спецификации (характеристики и изисквания към продуктите), процедури за производство, методи за изпитване и оценяване на съответствието. Стандартите са незадължителни насоки, съдържащи технически спецификации за продукти, услуги и процеси – от предпазни каски за сектора на промишлеността или зарядни устройства за електронни изделия до равнища на качество на услугите в областта на обществения транспорт.

Стандартите за киберсигурност имат значение и решаваща роля за опазването на информацията и защитата от киберзаплахи в бизнес организации както в България, така и по целия свят. Те предоставят рамка за установяване на ефективни мерки за сигурност, смекчаване на рисковете и гарантиране на поверителността, целостта и наличността на чувствителни данни. В зависимост от силата си на действие те могат да бъдат:

- български стандарти;
- европейски стандарти;
- международни стандарти.

В зависимост от своето действие могат да бъдат валидни на територията на дадена страна, на територията на Европейския съюз или международни.

Едни от тях са:

- **ISO/IEC 27001** – международен стандарт, който определя изискванията за създаване, внедряване, поддържане и непрекъснато подобряване на система за управление на информационната сигурност (ISMS). Той осигурява систематичен подход за управление на рисковете за информационните активи и включва мерки за оценка на риска, политика за сигурност, управление на активи, сигурност на човешките ресурси, контрол на достъпа, криптография и реакция при инциденти;
- **GDPR** – въпреки че, строго погледнато, не е стандарт за киберсигурност, Общият регламент за защита на данните (GDPR) оказва значително влияние върху практиките за

данните в Европейския съюз, включително в България. Той установява правила за защита на личните данни, налага мерки за сигурност и изисква от организациите незабавно да докладват за нарушения на данните;

- **NIST Cybersecurity Framework** – разработена е от Националния институт за стандарти и технологии (NIST) в Съединените щати и предоставя набор от насоки и най-добри практики за управление и намаляване на рисковете за киберсигурността. Въпреки че не е нормативно изискване в България, много организации приемат тази рамка като еталон за своите програми за киберсигурност;
- **PCI DSS** – стандартът за сигурност на данните в сектора на разплащателните карти (PCI DSS) се прилага за организации, които обработват данни от платежни карти. Той очертава изчерпателен набор от изисквания за сигурност за защита на данните на картодържателя, включително мрежова сигурност, контрол на достъпа, криптиране на данни, управление на уязвимостите и редовно тестване;
- **Насоки на Българския орган за национална сигурност (NSA)** – NSA в България предоставя насоки и препоръки за подобряване на киберсигурността в страната. Тези насоки обхващат различни области, като управление на риска, реагиране при инциденти, развитие на сигурна система и съответствие със законовите изисквания.

Класификация на стандартите в зависимост от сферата им на приложение

Стандартите по киберсигурност, които се използват в България, може да бъдат групирани в следните категории:

- **Информационна сигурност на организациите**
  - **БДС ISO/IEC 27001:** Информационна сигурност – Мениджмънт на информационната сигурност – Изисквания.
  - **БДС ISO/IEC 27002:** Информационна сигурност – Мениджмънт на информационната сигурност – Практически насоки и контролни мерки.
- **Сигурност на системи за обработка на информация**
  - **БДС ISO/IEC 27017:** Информационна технология – Сигурност в облачните услуги – Ръководство за контрол на информационната сигурност в рамките на облачните услуги.

- **БДС ISO/IEC 27018:** Информационна технология – Защита на личните данни в облачните услуги, предлагани от обработващи данни.
- **Киберсигурност на критична информационна инфраструктура**
- **БДС ISO/IEC 27010:** Информационна технология – Сигурност на информационната технология – Киберсигурност на критичната информационна инфраструктура.
- **БДС ISO/IEC 62443:** Киберсигурност на промишлени автоматизирани системи и контроли.

В таблица 1 са представени някои от най-известните стандарти по киберсигурност, които се използват в България. Всеки стандарт има свой обхват и приложение и помага за подобряването на киберсигурността в организациите, както и за спазването на законодателните изисквания в областта на защитата на данните и информационната сигурност.

Таблица 1. Стандарти по киберсигурност, използвани в България

Стандарт	**Описание**	**Приложение**	**Обхват**
ISO/IEC 27001	Международен стандарт за управление на информационната сигурност	Всички организации, които желаят да защитават данните си	Включва установяването, внедряването, поддръжката и непрекъснатото подобряване на СУИС.
GDPR	Общият регламент за защита на данните	Всички организации, обработващи лични данни	Фокусира се върху правата на субектите на данните, задълженията на организациите за защита на данните и механизмите за осигуряване на сигурността на данните.

NIST Cybersecurity Framework	Рамка за управление на киберсигурността, разработена от NIST	Много организации възприемат тази рамка.	Включва основните дейности по киберсигурност, които трябва да бъдат извършвани от организациите, като установяване на политики и процедури, идентифициране и защита на активи, управление на риска, прилагане на мерки за откриване и реагиране на инциденти и др.
PCI DSS	Стандарт за сигурност на данните в сектора на платежните карти	Организации, които обработват данни от платежни карти	Свързан е с опазването на кредитната информация и сигурността на плащанията.
БДС ISO/IEC 20000-1:2012	Системи за управление на услуги	Организации, предлагащи ИТ услуги	Обхватът включва управлението на услугите от страна на доставчици на ИТ услуги, които предоставят услуги на клиенти.
ISO/IEC 27002	Препоръчвани практики за управление на информационната сигурност	Допълващ стандарт към ISO/IEC 27001	Обхватът включва мерки за сигурността на информацията, включително политики, организационни мерки, физически мерки, мерки за управление на риска и сигурността на технологиите.

ISO/IEC 22301	Системи за управление на бизнес непрекъснатостта	Организации, които искат да се подготвят за бедствия и кризи	Обхватът включва планирането, изграждането, установяването, внедряването, функционирането, надзора, прегледа, поддръжката и постоянното подобряване на системи за управление на бизнес общността.
ISO/IEC 38500	Управление на ИТ в организацията	Ръководство за управителите на организации	Включва ръководенето, контрола и надзора на информационните технологии в организациите.
ISO/IEC 27005	Управление на риска за информационна сигурност	Организации, които искат да идентифицират и управляват рискове	Включва процеса на идентифициране, оценка и управление на риска от свързани с информацията заплахи и уязвимости.
ISO/IEC 15408	Сертификационна схема за оценка на сигурността на информационни технологии	Организации, които желаят да сертифицират своите продукти или системи	Включва процеса на оценка и сертифициране на сигурността на ИТ продукти и системи, като включва анализ на заплахи, оценка на риска, оценка на сигурността и проверка на съответствие.

Извод

Стандартите по киберсигурност в България се нуждаят от подобрение и приспособяване към съвременните предизвикателства в областта на киберсигурността.

Актуализацията и хармонизацията на стандартите, по-широкото им прилагане, повишаването на обучението и осведомеността, сътрудничеството и иновациите са ключови фактори за подобряването на киберсигурността в организациите в България. Само чрез тези инициативи ще можем да се справим по-ефективно с нарастващите киберзаплахи и да защитим информационната сигурност в страната.

Описание на разликите между стандарти, класифицирани в една и съща група

Информационна сигурност на организациите

Стандарт	Зона на прилагане	Същност
БДС ISO/IEC 27001	международен	Стандарт за мениджмънт на информационната сигурност, който установява изискванията за създаване, въвеждане, поддържане и непрекъснато подобряване на информационната сигурност в организации. Осигурява рамка за управление на риска, прилагане на подхода Plan-Do-Check-Act (Планирай – Практикувай – Провери – Действай) и въвеждане на система за управление на информационната сигурност (СУИС).
БДС ISO/IEC 27002	международен	Предоставя практически насоки и контролни мерки за имплементиране на информационна сигурност в организации. Представя обширен каталог от мерки за защита на информацията и се използва за ръководство при изграждането на системи за управление на информационната сигурност.

Сигурност на системи за обработка на информация

Стандарт	Зона на прилагане	Същност
БДС ISO/IEC 27017	международен	Фокусира се върху сигурността в облачните услуги и предоставя насоки за контрол на информационната сигурност в рамките на облачните услуги. Обхваща аспекти като физическа и околна сигурност, управление на идентичността и достъпа, защита на информацията и др.
БДС ISO/IEC 27018	международен	Свързан е със защитата на личните данни в облачните услуги, предлагани от обработващи данни. Предлага контролни мерки и насоки за обработка на личните данни в облака, като подчертава значението на поверителността, защитата на данните и съответствието с регулаторните изисквания.

Киберсигурност на критична информационна инфраструктура

Стандарт	Зона на прилагане	Същност
БДС ISO/IEC 27010	международен	Отнася се до киберсигурността на критичната информационна инфраструктура. Осигурява насоки за установяване на киберсигурността на критичната информационна инфраструктура и предоставя препоръки за защита на системите и данните в нея.
БДС ISO/IEC 62443	международен	Насочен е към киберсигурността на промишлени автоматизирани системи и контроли. Дефинира цялостна рамка за киберсигурността на промишлените системи и включва принципи, изисквания и контролни мерки за защита на автоматизираните системи в индустриалните среди.

Приложение на стандартите за киберсигурност в българските бизнес организации

- **Оценка и управление на риска:** Организациите в България прилагат стандарти за киберсигурност, за да

идентифицират и оценят потенциални рискове, включително уязвимости, заплахи и въздействие върху информационните активи. Процесите за управление на риска помагат да се определят подходящи контроли за сигурност и мерки за ефективно смекчаване на идентифицираните рискове.

- **Политика и процедури за сигурност:** Стандартите за киберсигурност ръководят разработването и прилагането на политики, процедури и насоки за сигурност в българските организации. Тези документи очертават правилата за служителите, определят приемливото използване на технологични ресурси и установяват протоколи за реакция при инциденти, класифициране на данни и контрол на достъпа.
- **Контроли и технологии за сигурност:** Организациите прилагат набор от контроли и технологии за сигурност, базирани на стандарти за киберсигурност, за да защитят своите системи и данни. Това включва защитни стени, системи за откриване на проникване, криптиране, контрол на достъпа, антивирусен софтуер и редовни актуализации на защитата.
- **Информираност и обучение на служителите:** Българските организации дават приоритет на информираността и обучението на служителите, за да гарантират, че стандартите за киберсигурност се прилагат ефективно. Програмите за обучение обучават служителите относно най-добрите практики за сигурност, важността на силните пароли, информираността за фишинг и процедурите за докладване на инциденти.
- **Съответствие и одит:** Организациите в България се подлагат на редовни вътрешни и външни одити, за да се оцени тяхното съответствие със стандартите за киберсигурност. Тези одити помагат да се идентифицират пропуски, да се измери ефективността на контролите за сигурност и да се гарантира непрекъснато спазване на установените стандарти.

Важно е да се отбележи, че стандартите за киберсигурност могат да варират в зависимост от индустрията, размера на организацията и специфичните регулаторни изисквания в България. Организациите трябва да са в крак с най-новите стандарти, насоки и законови задължения, за да поддържат стабилна позиция в областта на киберсигурността.

Ето няколко примера за официални източници, правителствени уебсайтове, индустриални асоциации и организации за киберсигурност в България, към които можем да се обърнем за актуална информация относно стандартите и разпоредбите за киберсигурност:

- **Държавна агенция за електронно управление (СЕГА)** – отговаря за координирането на изпълнението на инициативи за електронно управление, включително мерки за киберсигурност. Техният уебсайт предоставя информация за разпоредбите и насоките за киберсигурност в България: http://www.egov.bg/;
- **Българска комисия за защита на данните (КЗЛД)** – наблюдава прилагането на законите и разпоредбите за защита на данните в България, включително спазването на GDPR. Въпреки че се фокусират върху поверителността, уебсайтът им предлага подходяща информация за сигурността на данните и киберсигурността: https://www.cpdp.bg/;
- **Българска търговско-промишлена палата (БТПП)** – известна индустриална асоциация в България, която предоставя подкрепа и информация за бизнеса в различни сектори. Предлага ресурси и насоки относно най-добрите практики за киберсигурност. Уебсайт: https://www.bcci.bg/;
- **Асоциация за киберсигурност България (CAB)** – организация с нестопанска цел, която има за цел да популяризира информираността за киберсигурността и най-добрите практики в България. Сътрудничи си със заинтересовани страни от индустрията, организира събития и предоставя ресурси, свързани с киберсигурността. Уебсайт: https://www.cybersecurityaustria.at/;
- **Агенция за информационна сигурност и защита на критичната инфраструктура (ДАНС)** – държавна агенция, която отговаря за гарантирането на сигурността на информационните системи и критичната инфраструктура. Разработва политики, насоки и регулации, свързани с киберсигурността в България. Уебсайт: https://www.dans.bg/.

Тези източници осигуряват ценна информация за текущия ландшафт на киберсигурността, стандартите и разпоредбите в България.

Заключение

Стандартите по киберсигурност, използвани в България, представят важни насоки и инструменти за защита на информацията и съответствие на организациите с международни стандарти. БДС ISO/IEC 27001 и БДС ISO/IEC 27002 са широко прилагани в организациите за управление на информационната сигурност. Стандартите, свързани със сигурността на облачните услуги и критичната информационна инфраструктура, отразяват съвременните предизвикателства в киберсигурността. Защитата на личните данни и сигурността на промишлените автоматизирани системи също са от значение за сигурността в България. Организациите трябва да прилагат подходящите стандарти в съответствие със своите потребности и рискови профили, за да осигурят надеждна защита на информацията и инфраструктурата си.

За подобряването на стандартите по киберсигурност в България може да бъдат въведени следните инициативи:

- **Актуализация и хармонизация:** Необходими са актуализация и хармонизация на стандартите с последните технологични предизвикателствата в сферата на киберсигурността, за да се отразят нови заплахи и решения;
- **По-широко прилагане:** Развитието на свързаните с киберсигурност индустрии и сектори в България изисква повече организации да прилагат стандартите, особено в критичните сектори, като банки, енергетика, транспорт и здравеопазване;
- **Обучение и осведоменост:** Повишаването на обучението и осведомеността относно киберсигурността е от съществено значение както за специалистите в областта, така и за обществото като цяло. По-широкото разпространение на информация и провеждането на обучителни програми ще помогнат да се подобрят подготовката и реакцията на организациите;
- **Сътрудничество и споделяне на информация:** Важно е установяването на по-тясно сътрудничество между организациите, експертите по киберсигурност, правителството и академичната общност за споделяне на информация, обмен на най-добри практики и създаване на платформи за сигурно изпитване и анализ;
- **Гъвкавост и иновации:** Стандартите трябва да бъдат гъвкави и да поддържат иновациите в киберсигурността. Това включва приспособяване към нови технологии, като

изкуствен интелект, блокчейн и интернет на нещата, както и насърчаване на инициативи за изследвания и разработки в областта на киберсигурността.

Тези подобрения могат да увеличат ефективността и реактивността на стандартите по киберсигурност в България и да помогнат за справяне с нарастващите киберзаплахи и предизвикателства.

References/Литература

1. **BDS ISO/IEC 27001.** Informatsionni tehnologii. Metodi za sigurnost. Sistemi za upravlenie na sigurnostta na informatsiyata. Iziskvania.

[**БДС ISO/IEC 27001.** Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания.]

2. **BDS ISO/IEC 27002**. Informatsionni tehnologii. Metodi za sigurnost. Kodeks za dobra praktika za upravlenie na sigurnostta na informatsiyata.

[**БДС ISO/IEC 27002.** Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията.]

3. **BDS EN ISO/IEC 27017:2021.** Informatsionni tehnologii. Tehniki za sigurnost. Prakticheski kodeks za kontrol na informatsionnata sigurnost, baziran na ISO/IEC 27002 za oblachni uslugi (ISO/IEC 27017:2015).

[**БДС EN ISO/IEC 27017:2021.** Информационни технологии. Техники за сигурност. Практически кодекс за контрол на информационната сигурност, базиран на ISO/IEC 27002 за облачни услуги (ISO/IEC 27017:2015).]

4. **BDS ISO/IEC 27018.** Kodeks za dobra praktika za zashtita na lichnata informatsia za identifitsirane (LII) v obshtestveni oblatsi, deystvashti kato obrabotvashti lichni danni (ISO/IEC 27018:2019).

[**БДС ISO/IEC 27018.** Кодекс за добра практика за защита на личната информация за идентифициране (ЛИИ) в обществени облаци, действащи като обработващи лични данни (ISO/IEC 27018:2019).]

5. **BDS ISO/IEC 27010.** Ukazania za upravlenie na sigurnostta na informatsiyata za mezhdusektorni i mezhduorganizatsionni komunikatsii (ISO/IEC 27010:2015).

[**БДС ISO/IEC 27010.** Указания за управление на сигурността на информацията за междусекторни и междуорганизационни комуникации (ISO/IEC 27010:2015).]

6. **BDS EN IEC 62443-3-2:2020.** Sigurnost za promishleni sistemi za avtomatizatsia i kontrol. Chast 3-2: Otsenyavane na riska za sigurnostta i proektirane na sistemata.

[**БДС EN IEC 62443-3-2:2020.** Сигурност за промишлени системи за автоматизация и контрол. Част 3-2: Оценяване на риска за сигурността и проектиране на системата.]

7. **Standarti** i informatsionni tehnologii. Natsionalna strategicheska referentna ramka 2007 – 2013 g. [online resurs] https://bds-bg.org/bg/download/file/page-section/140.

[**Стандарти** и информационни технологии. Национална стратегическа референтна рамка 2007 – 2013 г. [online ресурс] https://bds-bg.org/bg/download/file/page-section/140.]

8. **ISO/IEC 27001:2013.** Information technology – Security techniques – Information security management systems – Requirements. ("INCITS/ISO/IEC 27001:2013 (R2019)").

9. **IEEE.** IEEE Standard for Incident Management. IEEE Xplore Digital Library, 2021.

10. **NIST SP 800-53.** Rev. 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.

11. **PCI DSS v3.2.1.** Payment Card Industry Data Security Standard. Payment Card Industry Security Standards Council, Wakefield, MA, USA, 2018.

12. **ENISA.** Baseline Security Recommendations for IoT. European Union Agency for Cybersecurity, Athens, Greece, 2020.

За авторите

Виктория Ангелова е докторант в УниБИТ в областта на компютърните науки. Притежава магистърска степен по специалностите „Софтуерно инженерство" и „Национална сигурност". Проявява интерес към дигиталната криминалистика. Извършва изследователска работа на тема „Стандарти и политики в дигиталната криминалистика", фокусирайки се върху стандартите по киберсигурност и технологичните решения на проблеми в бизнеса, както и върху добрите практики в света. Стреми се да допринесе за развитието и правилното използване на всички мерки, свързани с киберсигурността, и да внесе нови знания и иновации.

За контакт с автора: v.angelova@unibit.bg

Ива Костадинова е преподавател в катедра „Информационни системи и технологии" към Факултета по информационни науки на УниБИТ. Научните ѝ интереси са в областите: електронно обучение, дистанционно обучение, онлайн комуникации, ИКТ в обучението, образователни технологии.

За контакт с автора: i.kostadinova@unibit.bg