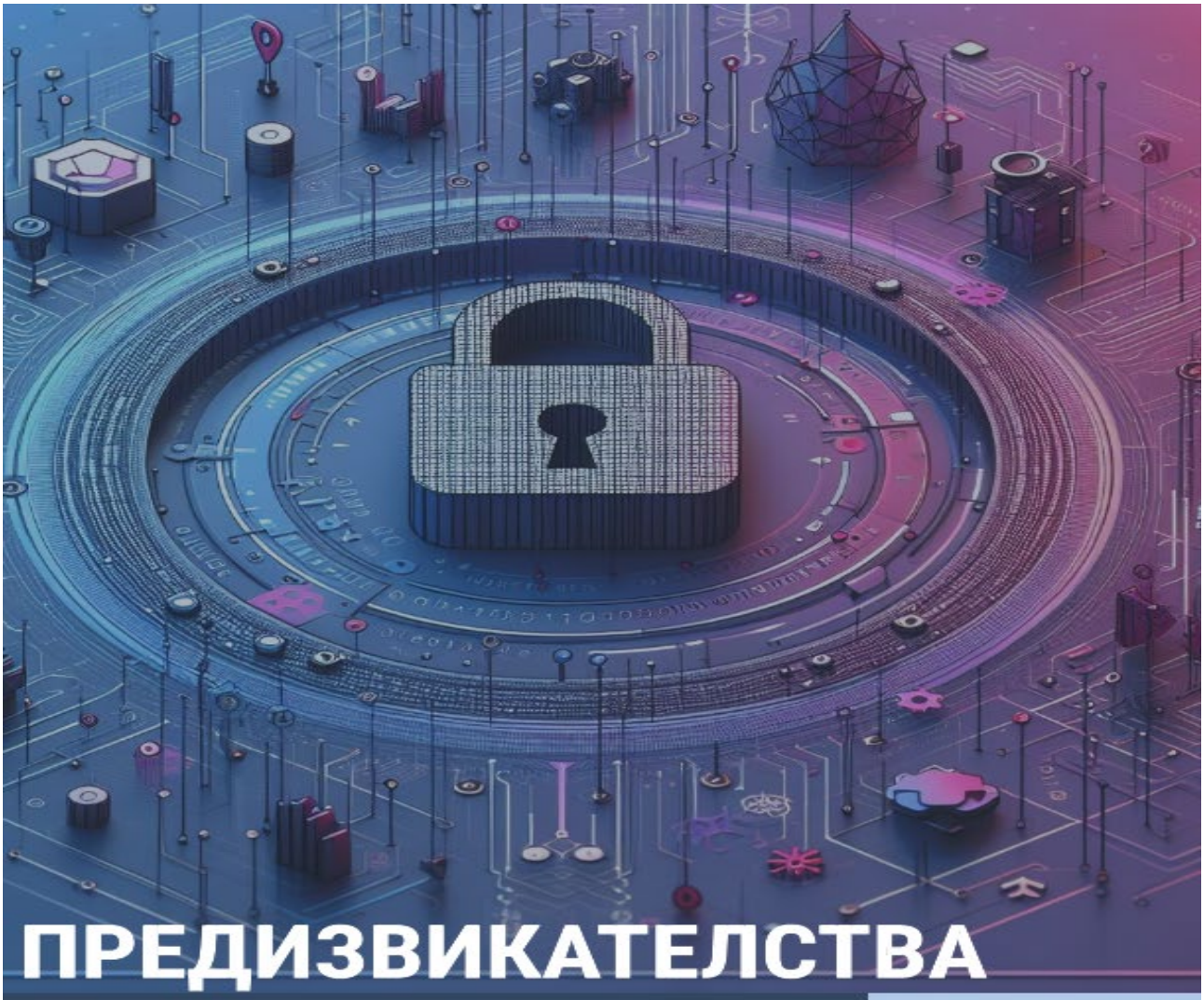
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ИНСТИТУТ
ПО ПУБЛИЧНА
АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ



ПРЕДИЗВИКАТЕЛСТВА

ПРЕД ПРИЛОЖЕНИЕ НА

НОВАТА ЕВРОПЕЙСКА ПОЛИТИКА ЗА КИБЕРСИГУРНОСТ

в българската държавна администрация

София, 2024

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ИНСТИТУТ ПО ПУБЛИЧНА АДМИНИСТРАЦИЯ

ОПЕРАТИВНА ПРОГРАМА ДОБРО УПРАВЛЕНИЕ

АНАЛИТИЧЕН ДОКУМЕНТ

„ПРЕДИЗВИКАТЕЛСТВА ПРЕД ПРИЛОЖЕНИЕ НА НОВАТА ЕВРОПЕЙСКА ПОЛИТИКА ЗА КИБЕРСИГУРНОСТ В БЪЛГАРСКАТА АДМИНИСТРАЦИЯ“

Автор: Ясен Танев е докторант към Факултет „Информационни науки“, към Университета по библиотекознание и информационни технологии и притежава магистърска степен от Техническия университет, София. Ясен Танев е ключова фигура в разработването на стратегии и образователни програми по киберсигурност. Преподава в Пловдивски университет „Паисий Хилендарски“. Водещ експерт в областта, който със своите иновативни обучения в Института по публична администрация е допринесъл за подобряване нивото на осведоменост а служителите от държавната администрация. Г-н Танев е и сертифициран водещ одитор по ISO 27001:2022 и активно допринася към инициативите на Европейския цифров иновационен хъб „Тракия“, като неговата мисия е повишаването на кибер-устойчивостта и осведомеността на обществото в тази сфера.

Съ-автори:

Мирослав Митев има магистърска степен по специалностите „Киберсигурност и цифрова криминалистика“ и „Информационни технологии и информационно брокерство“, а през 2015 г. защитава докторска степен в научно направление 3.5 „Обществени комуникации и информационни науки“ на тема „Развитие на системи за управление на качеството на информационни продукти и услуги“ към катедра „Компютърни науки“ при Университета по библиотекознание и информационни технологии. Понастоящем е хоноруван преподавател хоноруван преподавател в Университета и научен ръководител в бакалавърски и магистърски програми. В процес е на придобиване на квалификация като мрежови инженер Cisco Certified Network Associate. Д-р Митев е международно признат висококвалифициран експерт в сферата на информационната и киберсигурност, с дългогодишен опит в одита на системи за управление на сигурността на информацията, защита на личните данни, качеството, ИТ услуги, околна среда, здраве и безопасност при работа и др. съгласно стандарти ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018, ISO/IEC 9001:2015, ISO/IEC 14001:2018 и ISO/IEC 13485:2016. Обучител е на оценители за одити от първа, втора и трета страна. От 2011 г. е активен член на Федерацията на научно-техническите съюзи и активен член на Българския съюз на стандартизаторите, член е и на „Клуб 9000“.Има богат научен опит и задълбочени академични познания, участник е в множество национални и международни проекти, научни и научно-приложни конференции, семинари и обучения.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Николета Венева има магистърска степен по специалността „Право“, придобита в Нов български университет и очаква придобиването на втора магистърска степен по специалност „Киберсигурност и цифрова криминалистика“ в Университета по библиотекознание и информационни технологии. Има дългогодишна практика като корпоративен юрист. Допълнително специализира в сферата на защита на личните данни, като през 2022 г. получава сертификат „Information Privacy Professional/Europe (CIPP/E) от Международната асоциация на професионалистите в областта на защита на личните данни (The International Association of Privacy Professional/IAPP). Съвместява юридическата си дейност с изпълнение на дейности като длъжностно лице по защита на личните данни.

ISBN 978-619-7262-52-0

ANALYTICAL DOCUMENT

CHALLENGES FOR THE IMPLEMENTATION OF THE NEW EUROPEAN CYBER SECURITY POLICY IN THE BULGARIAN ADMINISTRATION

Abstract: The document "Cybersecurity Challenges" examines the state of cybersecurity within the Bulgarian administration and its alignment with European Union policies. It covers current cybersecurity practices, legal frameworks, and international standards, while addressing the implementation of the new European cybersecurity directive, NIS 2. The document also presents models for risk management, digital competence assessment for public administration employees, and strategies for adapting to EU cybersecurity requirements. Overall, it seeks to enhance Bulgaria's digital security infrastructure, compliance with EU directives, and response to cyber threats.

Keywords: Cybersecurity, EU Cybersecurity Regulations, Bulgarian State Administration, Cyber Threats, Digital Competences,

Sofia, 2024

For the author: Yassen Tanev is a PhD student at the Faculty of Information Sciences, University of Library and Information Science and holds a Master's degree from the Technical University of Sofia. Yassen Tanev is a key figure in the development of cyber security strategies and educational programs. He teaches at Plovdiv University „Paisii Hilendarski“. He is a leading expert in the field, who has contributed to improving the level of awareness of public administration employees with his innovative trainings at the Institute of Public Administration. Mr. Tanev is also a certified ISO 27001:2022 Lead Auditor and actively contributes to the initiatives of the European Digital Innovation Hub "Trakia", his mission is to increase cyber resilience and public awareness in this area.

Co-authors:

Miroslav Mitev holds a Master's degree in Cyber Security and Digital Forensics and Information Technology and Information Brokerage, and in 2015 he defended his PhD in the scientific field 3.5 "Public Communications and Information Sciences" on the topic "Development of Quality Management Systems for Information Products and Services" at the Department of Computer Science at the University of Library and Information Science. He is currently a Visiting Lecturer at the University and a research supervisor in undergraduate and graduate programs. He is in the process of qualifying as a Cisco Certified Network Associate. Dr. Mitev is an internationally recognized highly qualified expert in the field of information and cyber security, with extensive experience in auditing information security management systems, data protection, quality, IT services, environment, occupational health and safety, etc. according to ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018, ISO/IEC 9001:2015, ISO/IEC 14001:2018 and ISO/IEC 13485:2016. He has trained assessors for first, second and third party audits. Since 2011, he is an active member of the Federation of Scientific and Technical Unions

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

and an active member of the Bulgarian Union of Standardizers, he is also a member of Club 9000. He has extensive scientific experience and in-depth academic knowledge, has participated in numerous national and international projects, scientific and applied conferences, seminars and trainings.

Nikoleta Veneva holds a Master's degree in Law from New Bulgarian University and is awaiting the acquisition of a second Master's degree in Cyber Security and Digital Forensics from the University of Library and Information Science. She has many years of experience as a corporate lawyer. Additionally, he specializes in the area of privacy protection, and in 2022 he obtained the Information Privacy Professional/Europe (CIPP/E) certification from The International Association of Privacy Professionals/IAPP. She combines her legal work with performing activities as a data privacy officer.

СЪДЪРЖАНИЕ

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ВЪВЕДЕНИЕ

Нарастващият брой цифрови заплахи и киберинциденти през последните години превръщат информационната сигурност в първостепенна грижа за българската публична администрация. Настоящият документ има за цел да разгледа настоящата ситуация в областта на киберсигурността в България, като я приведе в съответствие със стандартите и директивите на Европейския съюз. В анализа са разгледани правните и организационните рамки, които оформят политиката на България. Разгледани са практики в областта на информационната и мрежова защита, като е подчертана критичната роля на кибер-сигурността за гарантиране на националната сигурност, неприкосновеността на личния живот на гражданите и целостта на обществените услуги.

Фокусът на анализа е върху многостранния характер на киберсигурността. Това включва аспектите на мрежовата и информационната сигурност, противодействието на киберпрестъпността и механизмите за киберзащитата. Анализът е рамкиран в контекста на световните тенденции в областта на киберсигурността и специфичните предизвикателства, пред които са изправени българските административни структури.

Целта на анализа е да резюмира, на база на налична публична информация, настоящите мерки за киберсигурност, да се идентифицират пропуските в политиката и практиката и да се предложат приложими мерки за повишаване на устойчивостта срещу киберзаплахи. Този встъпителен анализ поставя основите на бъдещ цялостен преглед, насочен към укрепване на инфраструктурата за киберсигурност на България и осигуряване на сигурна и надеждна цифрова среда за всички граждани.

Основните предизвикателства преди приемането на директивата (ЕС) 2022/2555 от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза (Директива МИС2) бяха свързани с в начина, по който се прилагаха мерките за киберсигурност в различните държави членки; различията в капацитета за прилагане и мерките за киберсигурност, недостатъчен обмен на информация между държавите членки, което се отразяваше на ефективността на мерките за киберсигурност.

В отговор на това в Директивата за МИС2 се предлагат системни и структурни промени за подобряване на рамката за киберсигурност на ЕС, включително по-всеобхватен подход, обхващащ по-широк сегмент от икономиката, рационализирани задължения за сигурност и по-ясни определения и критерии за основни и важни субекти. Новата директива има за цел също така да подобри съвместната осведоменост за ситуацията и колективния капацитет за реагиране при инциденти и кризи в областта на киберсигурността.

България следва да се възползва от възможността да бъде лидер в ЕС по отношение на прилагане на директивата в нейния обхват и замисъл.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ГЛАВА 1. Анализ на текущото състояние на държавната администрация и инциденти в контекста на мрежовата и информационна сигурност

1.1 Дефиниране на понятието „киберсигурност“

За да оценим текущото състояние на киберсигурността в държавната администрация, е необходимо да дефинираме понятието „**киберсигурност**“, като с цел постигане на по- цялостно разбиране на това понятие, ще разгледаме няколко източника.

Законът за киберсигурност (*Обн. ДВ. бр.94 от 13 Ноември 2018 г.*) предлага следните дефиниции, които очертават националната правна рамка за понятието[1]:

„Чл. 2. (1) Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

(2) Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана.

(3) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях”.

На ниво Европейски съюз Европейската агенция за киберсигурност ENISA[2] формулира понятието “киберсигурност”, като включва разбирането за информационна сигурност по следния начин:

Информационна сигурност.

Класическият модел за информационна сигурност дефинира три цели: **Поверителност, Цялостност и Наличност**.

Мрежовата и информационната сигурност[3], както е дефинирана в Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 г. относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004, означава“ *способността на мрежа или информационна система да устоява при определено ниво на надеждност на случайни събития или незаконни или злонамерени действия, които компрометират поверителността, целостта и наличността на съхраняваните или предавани данни и свързаните с тях услуги, предлагани от или достъпни чрез тези мрежи и системи”*.

Информационната сигурност, мрежовата и информационната сигурност са подмножества на киберсигурността.

---

[1] https://e-gov.bg/

[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/

[3] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

Киберсигурността[4] обхваща всички аспекти на предотвратяването, прогнозирането, толерирането, откриването, смекчаването, отстраняването, анализ и разследване на киберинциденти. Като се имат предвид различните видове компоненти на киберпространството, киберсигурността следва да съдържа следните атрибути: наличност, достоверност, безопасност, поверителност, цялостност, възможност за поддържане (за материални системи, информация и мрежи), устойчивост, оцеляване, способност за възстановяване (в подкрепа на динамичността на киберпространството), Отчетност, автентичност и неоспоримост (в подкрепа на информационната сигурност).

И за да завършим анализа на дефинициите, е необходимо да добавим и начина, по който киберсигурността е описана в международен стандарт ISO/IEC 27100:2020[5] и свързаните с него. Според този стандарт „киберсигурност са действия за предпазване на хората, обществото, организациите и държавите от киберрискове“.

Под **киберриск** се разбира риск, предизвикан от киберзаплаха. От своя страна киберзаплаха е заплаха, използваща слабост в киберпространството. А дефиницията на киберпространство може да бъде представена като: свързана цифрова среда от мрежи, услуги, системи, хора, процеси, организации и това, което се намира в цифровата среда или преминава през нея.

За да дефинираме ясен подход за оценка на текущото състояние на държавната администрация, ще разгледаме наличната обществено достъпна информация и за нейното текущо състояние в контекста на киберсигурността и влезлите в сила регламенти и директиви на ЕС, като тук е важно да опитаме да отговорим на въпроса **какво е киберсигурност**.

Киберсигурността изисква мултидисциплинарен подход, който се стреми към защита на цифровата среда и информацията в нея от различни видове заплахи, като същевременно поддържа целостта, поверителността и наличността на данните.

Подходът за оценка на сегашното състояние на нормативна адекватност по отношение на дефинирането на киберсигурността в контекста на държавната администрация, е комбинация от изследване и анализ на Национална рамка за оценка на възможностите[6], Закона за киберсигурност, Наредба за минималните изисквания за мрежова и информационна сигурност[7], Методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност[8] (и приложение 1 и 2 към нея), както и информацията, налична в портала за обществено обсъждане - Актуализиран национален стратегически документ „Цифрова трансформация на България за периода

[4] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[5] https://www.iso.org/standard/72434.html

[6] https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-bg.pdf

[7] https://e-gov.bg/wps/wcm/

[8] https://e-gov.bg/wps/wcm/

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

2020-2030 г.“ и Националната пътна карта за цифрова трансформация на България до 2030 г.[9]

Тези документи ни дават отправна точка и поставят основата за идентифициране на пътя, целите и стратегиите за постигане на устойчива дигитална трансформация, както и показатели, с които да измерим сегашното състояние по прилагането на европейските политики за киберсигурност.

В допълнение, за да се установи реалното състояние на киберсигурността и да се позволи да се измери, са необходими данни за осъществени одити, проверки, подадени инциденти и друга информация от български и европейски източници, както и да се използва методиката, с която Европейският съюз измерва постигнатото на стратегическо ниво чрез National Capabilities Assessment Framework[10] и дефинираните 4 клъстера:

- (I) Управление и стандарти за киберсигурност
- (II) Изграждане на капацитет и осведоменост
- (III) Правни и регулаторни въпроси
- (IV) Сътрудничество

1.2. Управление и стандарти за киберсигурност. Разработване на национален план за действие при извънредни ситуации, свързани с киберсигурността

По време на изследването са анализирани всички релевантни и посочени по-горе документи както и нормативната рамка, и структурата за планиране и координиране на действия, свързани с киберсигурността[11] на държавната администрация (Решение № 192 на МС от 9 април 2019 г.), с което се определят административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност. Националната стратегия за киберсигурност е надградена от първоначалната ѝ версия и ясно показва нуждата от периодично осъвременяване с оглед променящата се среда и възникващите нови регулации или предизвикателства в национален, европейски и международен аспект.

Ролята на секторните CERT (Computer Emergency Response Team или Екип за реагиране при инциденти в компютърната сигурност) е ясно идентифицирана и в координацията им с националния CERT, е разработен механизъм за взаимодействие, който е и подкрепен със съответната нормативна база.

Успешното изпълнение на тези критерии може да се идентифицира и от данните в National Cyber Security Strategies - Interactive Map[12], както и от отчетените успехи в

[9] https://strategy.bg/publicconsultations/View.aspx?Id=8094

[10] https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

[11] https://www.mtc.government.bg/sites/default/files/rms192imetodika.pdf

[12] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Аналитичния доклад за цифрова трансформация т.7, Политики и регулация и институции, ръководство и координация.

1.2.1. Установяване на базови мерки за сигурност

Друг аспект от този клъстер е установяване на базови мерки за сигурност и това изискване е приложено чрез приемане на Закона за киберсигурност и Наредбата за минимални изисквания за мрежова и информационна сигурност - НМИМИС, (*Обн.ДВ.бр.59 от 26 Юли 2019 г.*).

Още в Глава първа, раздел“ Обхват,” член 1. (1) т.1 НМИМИС изрично включва административните органи, като субект, за който се прилага наредбата. Този регулаторен подход е уникален за държава членка на ЕС и е адаптиран като всеобщо приложим за всички европейски юрисдикции посредством новата Директива (ЕС) 2022/2555 на ЕП и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза[13].

В допълнение, НМИМИС дава и изрични принципи за прилагане на базовите мерки, а именно: в чл.2 посочва, че“ *по своя характер мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на дейността на Субекта и трябва да са подходящи и пропорционални на рисковете за постигането на основните цели на мрежовата и информационната сигурност*”.

За да подсигури добри практики, които да бъдат приложени от администрацията, ясно реферира към източници в чл.2 ал. 3 и 4, като в Глава втора - МИНИМАЛНИ МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, конкретно навлиза в детайл с препратка към БДС ISO/IEC 27001, който в последната си версия съответства на БДС ISO/IEC 27001:2022, и предоставя систематичен и проследим подход за управление на информационната сигурност и и киберсигурността. Към Наредбата има разписан и детайлен списък на добри практики, съдържащи се в Приложения № 1-9.

За да се провери и установи качеството на въведените базови мерки за сигурност, законодателят е заложил мерки, обособени в Глава трета от Наредбата: Контрол, които визират извършване на вътрешни и външни одити на Субекта (чл. 35 ал. 1 , т.1, 2 и 3), и които одити, съгласно Наредбата са препоръчителни. В ал. 3 има конкретна референция към приложение на стандарт по отношение на вътрешните одити: “(3) Одитите по ал. 1, т. 1 се извършват в съответствие със стандарт БДС EN ISO 19011 „Указания за извършване на одит на системи за управление“, изискванията на стандарт БДС EN ISO/IEC 17020 „Оценяване на съответствието“, като се спазва най-малко следното:.....”

Прави впечатление, че независимо от доброто планиране на процеса по въвеждането на базовите мерки, което коментирахме по-горе, и процедурата за контрол, описана в чл.35,

[13] https://eur-lex.europa.eu/eli/dir/2022/2555

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

дефинирането в чл.35 ал. 2 на одитите по ал. 1, т. 2 и 3, като препоръчителни мерки, създава предпоставка за възможен риск от пропуски при осъществяване на мерките.

При разглеждането на европейските актове, транспонирани в националното законодателство, не би трябвало да се пропускат и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните[14] и променения в тази връзка Закон за защита на личните данни[15] .

Член 5 (параграф 1, буква е) от Регламента издига като основен принцип цялостност и поверителност на личните данни, като конкретно гласи, че личните данни "са обработвани по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност"). Този принцип следва да се спазва от всички администратори и обработващи лични данни, включително и държавната администрация, като в подкрепа в прилагането на адекватни технически и организационни мерки има разработен и отделен международен стандарт ISO/IEC 27701, който определя изискванията и дава указания за създаване, прилагане, поддържане и постоянно подобряване на система за управление на неприкосновеността на личната информация под формата на разширение към ISO/IEC 27001.

На база Консолидирания годишен доклад за вътрешния контрол в публичния сектор за 2022[16], Аналитичния доклад за цифровата трансформация в България и публична информация за инциденти, идентифицирахме прилагането на заложените мерки и предизвикателствата напред:

1. Затвърждава се тенденцията част от звената за вътрешен одит в част от общините да не се съобразяват с области за одит, като много от българските общини се сблъскват с нарастващи кибератаки, поради липсата на инфраструктура за защита на събраните лични данни. Тази комбинация предизвиква притеснение от липсата на разбиране и приложение на базовите изисквания и показва необходимост в подхода за одит.
2. На ниво общини се идентифицират проблеми с информационната сигурност и съвместимостта на различните системи поради липсата на квалифицирани ИТ специалисти на локално ниво.
3. Най-често са констатирани пропуски при разпределение на отговорностите в областта на мрежовата и информационната сигурност (МИС)

[14] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679
[15] https://cpdp.bg/
[16] https://fukvopublic.minfin.bg/File/File_Download/3597

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

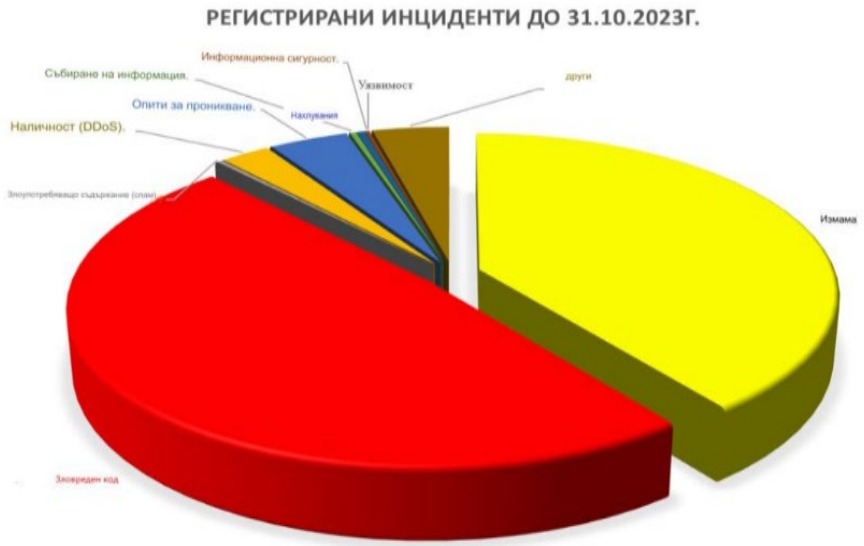
Фигура 1. *Предпрети действия от ръководителите на организации за осигуряване на служител/звено по МИС8Съвет по МИС*

4. Ръководителите на 130 организации (около 76% от докладвалите) са утвърдили собствена Политика по мрежова и информационна сигурност, като в 87 от тях тя е изготвена в съответствие с нормативните изисквания. Най-често несъответствията са свързани с разделението на ролите и отговорностите на участниците в процеса по МИС, при управлението на риска, класификацията на информацията, управлението на инциденти. Информацията за това, че има предизвикателства с подаване на информацията за инциденти, може да бъде намерена и в аналитичния доклад, в който се подават следните данни: По данни на Националния екип за реакция при инциденти в компютърната сигурност – CERT-BG, към 31.10.2023 г. са получени 6089 сигнала, от които са регистрирани 1558 инцидента в българското интернет пространство, което сравнено със същия период за 2022 г. е намаление с 8,5 % (1687 инцидента до 31.10.2022 г.).

В същия доклад се посочва, че се повишава рискът от инциденти поради високата свързаност и променената геополитика.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Фигура 2. *Регистрирани киберинциденти в България до 31.10.2023 г.*



Източник: CERT-BG

5. За да се постигне качествено управление на МИС, е необходимо да се разработят процедури и политика, които освен разработени, е необходимо да бъдат представени на служителите и подкрепени от ръководството. На база обобщените данни за 2022 година е видно, че само 50,5 % от организациите са утвърдили политика по МИС, която е изготвена в съответствие с нормативните изисквания (25.5 % имат политика, но не отговаря на изискванията).

6. Друг важен компонент е частта, свързана с управление на риска. В НМИМИС ясно е посочена методология, по която да се управляват рисковете. Резултатите от доклада на МФ показват, че едва 57% от проверените 170 организации извършват такава. Едва 33% могат да бъдат посочени, като постигащи пълно съответствие с разпоредбите на НМИМС и които извършват ежегоден анализ и оценка на рисковете за МИС по утвърдената от ръководителя на организацията Методика за оценка на риска и е утвърден план за намаляване на неприемливите рискове. Тази констатация е притеснителна, защото оценката на риска е свързана с познаване на процесите, касаещи информация, заплахите срещу тях и агентите на заплаха, които биха използвали слабости, за да атакуват.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

***Фигура 3**. Физическа сигурност, източник: доклад на МФ*

***Фигура 4**. Управление на достъпите, източник: доклад на МФ*

7. В контекста на физическия достъп и защитата на инфраструктура, обезопасяването и въвеждане на мерки за пожарогасене, защита от наводнение или др., държавната администрация има установени традиции и нивото на защита е приемливо, имайки предвид, че се наследява от процедурите за защита на информацията и класифицирана информация[17]. По този показател над 70% от организациите вземат мерки. В контекста на променената социално-икономическа среда и пандемията от COVID-19, които имаха за последица въвеждане на

[17] https://www.dksi.bg/media/9527/zakon_za_zasita_na_klasificiranata_informaciq.pdf

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

дистанционна работа, организациите също са взели мерки и повечето от тях разполагат с изградени системи за отдалечен достъп.

8. България винаги е била в червената зона по темата за използване на нелицензиран софтуер. Международни доклади показват съществена промяна в тази тенденция, Това се държи на държавната политика по управление на лицензите, законовите промени (включително в Наказателния кодекс), както и въвеждането на изисквания по НМИМИС. Независимо от тези промени и на база трафични данни от публични торент тракери може да се отбележи, че все още има органи на държавната и общинска администрация, които достъпват, съхраняват и използват софтуер без легитимно право на ползване или такъв, който е с нарушени лицензионни права. Много е важно да се отбележи, че ползването на такъв тип софтуер крие не само правен риск, поради за нарушение на защитата на авторското право, но носи риск от това да са заразени със зловреден код. Докладът на МФ отчита, че 76% от организациите имат политика за управление на приложен и системен софтуер и разполагат с резервни копия и дистрибутиви, когато това е възможно и необходимо.

9. Аспект "непрекъсваемост на услугите" е важен компонент от функционирането на държавната администрация и в контекста на електронните и цифрови услуги. Очакванията на потребителите са по-големи от това да получат традиционното обслужване на гише, поради техния профил - такива с опит, които имат необходимост да получат услугата винаги когато им е нужна, и тези, които имат пречка да получат достъп до услугите на държавната администрация, поради което достъпът трябва да бъде лесен и логичен. Аспектът с въвеждане на опция за резервиране на услугите е посока, в която електронното управление се развива в положителна посока, като включва услуги, предоставяни от Изпълнителна агенция „Инфраструктура на електронното управление". Услугите са обобщени в няколко различни категории, но в контекста на непрекъсваемостта могат да бъдат отнесени тези от Инфраструктура[18]. Използването от все повече администрации на услугите повишава покриването на базовите изисквания и гарантира по-висока степен на непрекъсваемост при обслужване, както и при архивиране на данни в сигурна среда. Докладът на МФ идентифицира за 2022 година, че 64 % от организациите са разработили вътрешни правила/инструкции за резервиране и архивиране на информацията, като е установено ограничение за планиране или приложение поради липса на оборудване или остаряло такова. Използването на централизирани услуги би могло да компенсира този дефицит и да подобри надеждността. Притеснителна е обаче констатацията, че само в малка част от тези организации, плановете са били тествани поне веднъж в годината, с цел да се провери тяхната актуалност и да се тренират лицата, които имат отговорности за изпълнението им. Също така прави впечатление и констатацията, че за част от останалите организации са спазени изискванията на Наредбата за изготвяне на правила/процедури за резервиране и

[18] https://iaieu.egov.bg/wps/portal/agency-iaieu/infrastructure

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

архивиране на информацията, но същите се нуждаят от актуализиране, включително и изготвяне на планове за непрекъсваемост.Това отново се извежда на видно място предизвикателството с внедряване и поддръжка на изискванията по НМИМИС, поставяща изискване за базови мерки за сигурност.

***Фигура 5**. Физическа сигурност, източник: доклад на МФ*

10. Препоръките и обобщенията за качествата на одитите е заключителната част при анализиране на достъпната информация. За съжаление, публични източници за план на одит за 2023 г. не могат да бъдат намерени. За това ще използваме информация от Траекторията за инцидентите и ще я комбинираме с информацията от доклада на МФ за 2022 година. В 11 организации от публичния сектор вътрешните одитори са оценявали периодично ефикасността на системата за управление на сигурността на информацията в организацията чрез извършването на вътрешни одити при спазване изискванията на Наредбата. Външни одити, провеждани от независими организации за одит, имащи право да извършват сертификация, са изпълнявани в 10 организации, като срокът на валидност на притежаваните от тях сертификати е продължен. Тези данни могат да бъдат използвани, като добър пример и добра практика, която показва, че внедряването и поддържането на международни признати стандарти не само подобрява разбирането и гарантира защита на информационната и киберсигурност на базовото ниво, но и ангажира цялата организация с това. Тези изводи са разпознати и от ENISA и прилагането им ще бъде въплътено в разпоредбите на в NIS2 и транспонирано в нашето законодателство, което вероятно ще доведе и до промени в НМИМИС. Обобщението в Доклада на МФ за качеството на одита е следното: слабостите при изготвянето на докладите са свързани с непосочване на причините за установените несъответствия; липсват

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

изводи какъв ще е ефектът върху дейността на организацията, ако не се предприемат действия за подобрение; посочена е подробна информация, която е по-подходящо да бъде част от работните документи по ангажимента; дадените препоръки не са добре адресирани и др.

Като финален акцент за анализа на базовите мерки за сигурност реферираме към информацията от траекторията за регистрирани инциденти по видове и обобщаване на тази информация на база данни от Националния CERT.

***Фигура 6**. Видове регистрирани инциденти за 2023 г., 2022 г. и 2021 г.*

Според Националния CERT през 2020 г. са регистрирани 2100 киберинциденти в/от българското интернет пространство, което е 10 % увеличение спрямо 2019 г. България е една от страните с най-висок дял на локални инфекции от злонамерен софтуер (с който се сблъскват 30 % от интернет потребителите, 2-ра в Европа), злонамерени уеб-базирани атаки (15 % от интернет потребителите), банкови злонамерени атаки (1,2 %), „троянски коне“ за рансъмуер (0,3 %).

Като допълнение към посочената по-горе статистика смятаме, че нужно да се отбележат и още няколко инцидента и тенденции, споменати от МЕУ в публичното представяне на проекта, свързан с Националния координационен център и екосистемата по киберсигурност[19] и научените уроци:

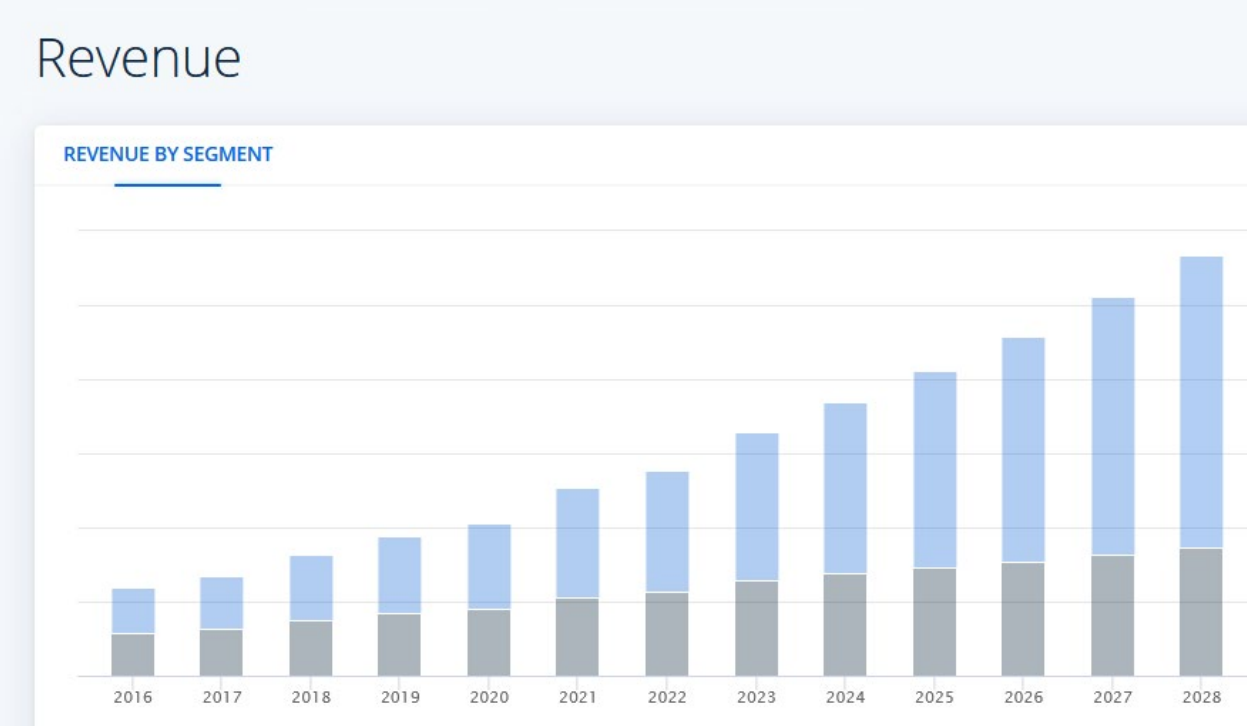
- Инцидент с Търговския регистър - създаване на политика за поддържане на архивни копия на критични данни - включени 36 администрации;
- Увеличено количество от DDoS атаки след началото на войната между Русия и Украйна, взети мерки за повишаване на киберустойчивостта чрез развитие на интернет възел за обща защита;

[19] https://www.bta.bg/en/news/bulgaria/577238-6-100-plus-cyber-incidents-registered-in-public-sphere-in-2023

- България претърпя нарушение на сигурността на данните на 5 милиона граждани[20] по вина на Националната агенция за приходите (която по-късно беше глобена с 2,6 милиона евро) - преглед и модернизиране на инфраструктурата и подобрен модел на управление.

Анализът, направен до момента в контекста на мерките за киберсигурност, и нуждата от инвестиция сега ясно идентифицира и очакванията за нарастване на пазара за киберсигурност, поради увеличаващи се рискове.[21]

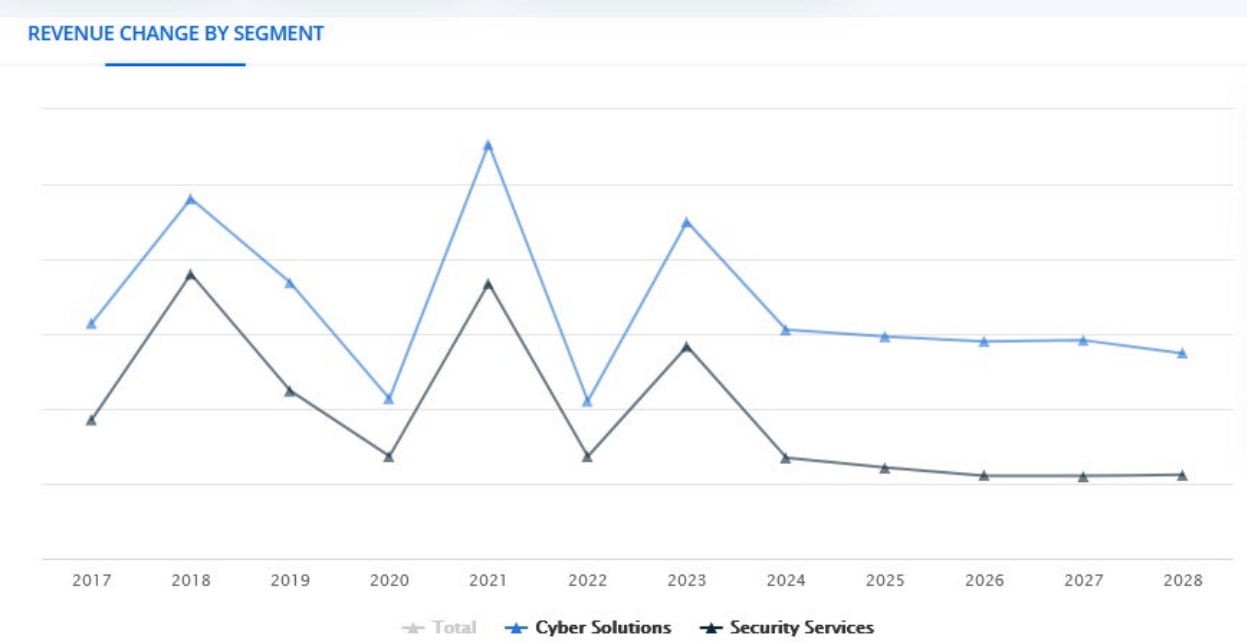
***Фигура 7**. Приходи по сегменти. Източник statista.com*



[20] https://www.e-gover.net/the-national-cert-has-registered-2100-cyber-incidents-in-bulgaria-in-2020

[21] https://www.statista.com/outlook/tmo/cybersecurity/bulgaria

Фигура 8. *Промяна на приходите по сегменти. Източник statista.com*



Тенденцията за услугите и продуктите е интересна и показва ясната свързаност между технологичните решения и стойността и за внедряване и поддръжка.

Обобщението на текущото състояние води до следните основни изводи:

- *Държавната администрация притежава добра и съвременна нормативна рамка, която при изпълнение ще предостави необходимото базово ниво на киберсигурност и информационна сигурност и дори ще го надмине.*
- *От идентифицираните случаи от неприложимост или невъзможност да се приложат изискванията на разгледаните по-горе документи може да се направи извод, че недостатъчното осигуряване на нормативно съответствие, се дължи на липсата на разбиране на предизвикателствата, поставени пред администрацията при въвеждане на дигитални технологии, недостатъчната ресурсна обезпеченост за внедряване на тези технологии и тяхната поддръжка или недостатъчното наемане на експертни кадри и условността по отношение на извършването на одити съгласно НМИМИС.*
- *Чрез ефективното прилагане на изискванията на нормативната рамка в сферата на мрежовата и информационна сигурност, включително Закона за киберсигурност, НМИМИС, и признатите международни стандарти, както и навременното и регистриране на инциденти на сигурността, налагането на адекватни санкции и удостоверяване на несъответствия посредством извършване на одити би довело до получаване на обективна и точна информация за нивото на цифрова зрялост на*

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

държавната администрация, както и би дало ценна обратна връзка за целите на стратегическото планиране.

1.2.2. Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги

Не на последно място и преди да направим изводи за текущото състояние на държавната администрация е необходимо да разгледаме темата за цифрова идентичност и изграждането на доверие в цифровите обществени услуги. Европейската комисия има ясна политика и цели и те са интегрирани в цифровата декада[22]. Дефинирани са по следният начин: *Интелигентни обществени услуги, известни още като електронно правителство, които използват технологии за предоставяне на услуги на гражданите на местно, регионално и национално равнище. Тези услуги позволяват на гражданите, предприятията и организациите да осъществяват взаимодействието си с правителствата по-лесно, по-бързо и на по-ниска цена*.

Развитието на тези услуги е залегнало в ***национални прогнозни траектории***. За равнището на цифровите цели на Република България по Европейска политическа програма „Цифрово десетилетие“ до 2030 г. има описание в глава 4 цифровизация на обществените услуги. Резултатът от приложението им е видим през информация за Статистиката на предоставянето на електронни административни услуги чрез Единния модел[23].

Фигура 9. *Топ 5 на заявителите на вътрешни електронно административни услуги. Източник Система за справочна и удостоверителна информация (Regix)*

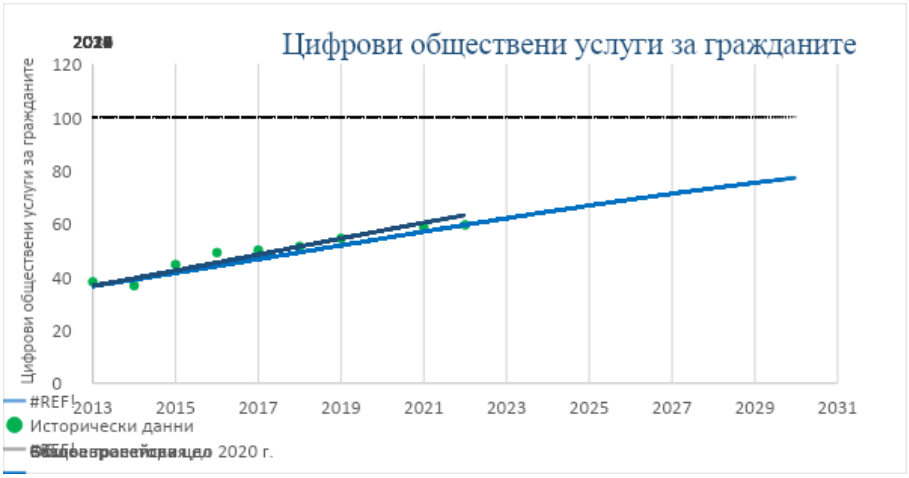
[22] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_bg

[23] https://unifiedmodel.egov.bg/wps/portal/unified-model/unified-model/statistics/statistics/

***Фигура 10**. Брой предоставени вътрешни електронно административни услуги. Източник Система за справочна и удостоверителна информация (Regix)*

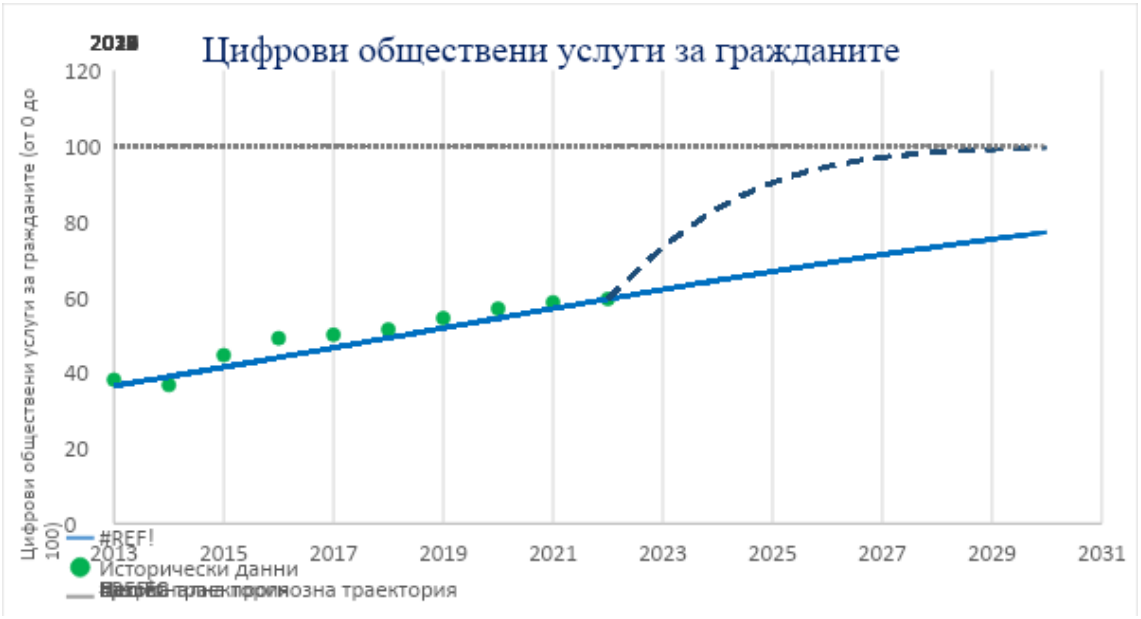
Тенденцията при тези услуги е да нарастват, но траекторията ясно очертава предизвикателствата и показва необходимостта процесът по въвеждане да бъде ускорен. Като една от причините да има забавяне може да бъде изтъкната и липсата на единна електронна идентификация eID, както и фрагментираните системи и липсата на интеграция между тях по дизайн. Тези дефицити са установени и на национално ниво и както е заложено в траекторията, се очаква да бъдат компенсирани и съответно тя да бъде коригирана.

***Фигура 11**. Цифрови обществени услуги за гражданите.*

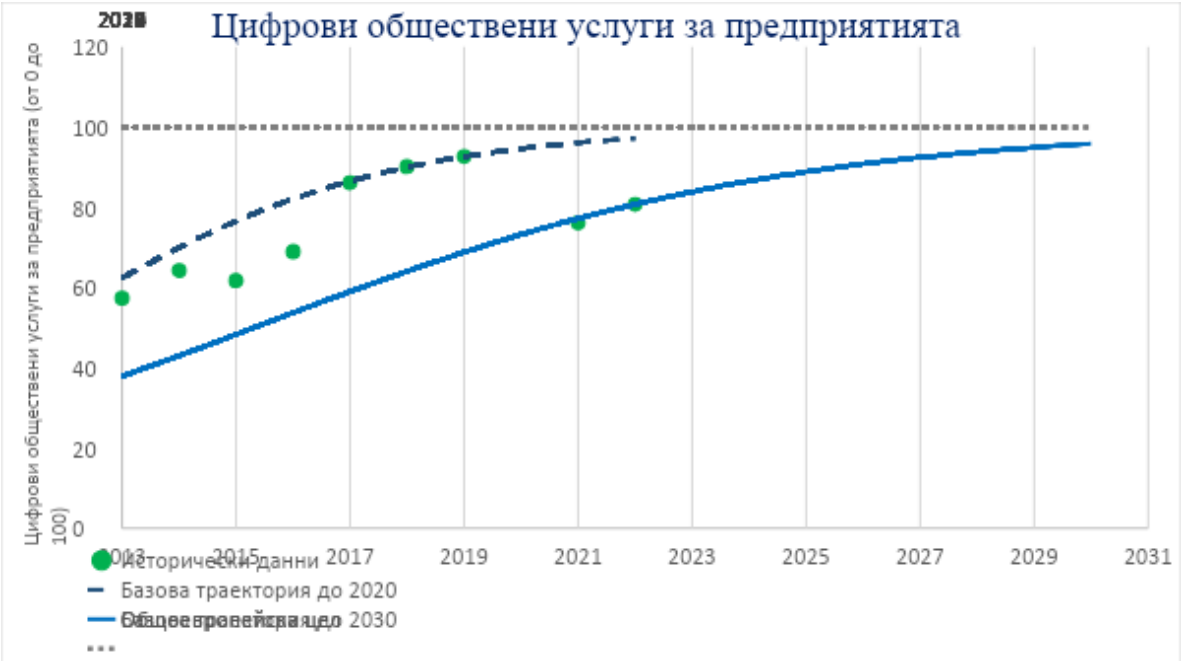


Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Фигура 12. *Цифрови обществени услуги за гражданите – прогнозна траектория.*

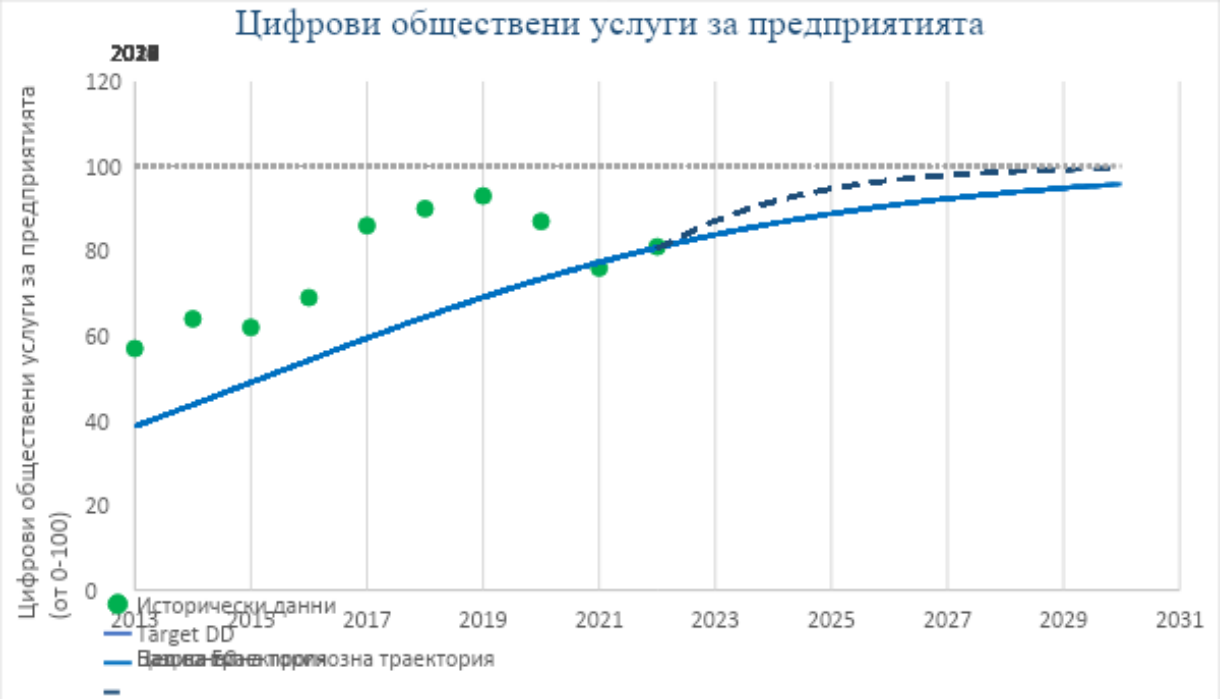


Фигура 13. *Цифрови обществени услуги за предприятията*



Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

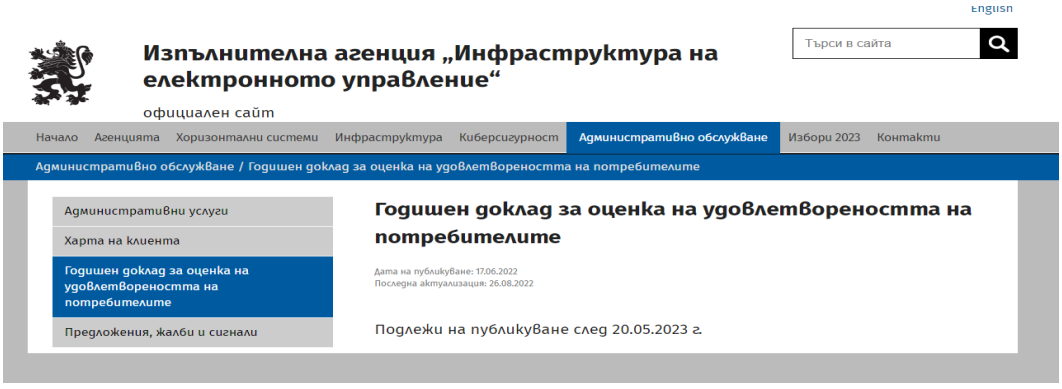
Фигура 14. *Цифрови обществени услуги за предприятията – прогнозна траектория*



Може да се направи извод, че има ясна траектория за въвеждане на цифрови услуги с по-високо ниво на сигурност и надеждност, което ще подобри и общата рамка на киберсигурността в държавната администрация.

За бизнеса и обществото би било полезно, освен публикуваната статистиката за употреба, да има и повече публични данни за удовлетвореността на потребителите.

Фигура 15. *Снимка на екран/скрийншот на сайта на ИА „Инфраструктура на електронното управление*



Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Препоръчваме и създаване на карта за миграция на услуги със срокове и отговорности, за да може да бъде информирано обществото в детайл и да може да осъществява обществен контрол, което би имал стимулиращ и позитивен ефект и върху администрацията.

1.3. Изграждане на капацитет и осведоменост

Вторият клъстер от рамката за оценка е ключова и тя се интегрира с Клъстер 1, защото, както установихме, дефицитите в разбирането и мотивацията на базовите изисквания за киберсигурност и тяхното приложение, и спецификата на променящата се среда имат пряка връзка със знанията по темите. Но знанията не е достатъчно да бъдат предоставени, те трябва да бъдат усвоени и комбинирани с умения. Като знанията и уменията трябва да засягат аспектите за превенция, реакция, както и действия, свързани с възстановяване след инцидент.

1.3.1. Организиране на дейности по киберсигурност

Организирането на дейностите по киберсигурност е залегнала в множество нормативни актове, в това число закони, наредби, приложения и правилници, както и чрез създаване на структура за организиране на дейността по киберсигурност. Проучената база показва, че на институционално ниво има добро разбиране на Европейската рамка, международните стандарти добрите национални практики, като всички тези компоненти са внедрени в общата стратегия за киберсигурност, а именно: Националната стратегия за киберсигурност във версия 2020[24] и последващата редакция 2023: Актуализирана Национална стратегия за киберсигурност „Киберустойчива България 2023”[25] и поставените цели за изграждането на напълно завършена интегрирана Национална екосистема за киберсигурност със способности за адаптиране към динамиката на глобалните киберзаплахи и за реакция при мащабни атаки срещу български информационни ресурси, включително за интегриране в системата за киберсигурност на Европейския съюз е стратегическа цел, дефинирана в Националната програма за развитие „България 2030[26].

Внимателният анализ на стратегическата рамка показва ясно разбиране на процеса по организиране на дейността по киберсигурност. Това, което е необходимо, е да се наблюдава изпълнението на дейностите и целите, както и качеството на отчитане на постигнатите резултати. Дефицит е и активната комуникация за постигнатото с всички заинтересовани страни, като е необходимо да се използва зараждащата се екосистема в държавната администрация и частния сектор, за да може тази информация да достигне до по-широк кръг потребители.

[24] http://cyberbg.eu/

[25] https://strategy.bg/PublicConsultations/

[26] https://strategy.bg/StrategicDocuments/View.aspx?Id=1330

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

1.3.2. Създаване на възможности за реагиране при инциденти

В нормативната рамка ясно са разписани правилата и изискванията за реакция при инциденти и посредством НМИМИС те са приложени като изискване на всички органи на държавната администрация (като изключенията са описани). Законът за киберсигурност също определя реда, органите и начина за реакция при инциденти и киберпрестъпление. За всяка една организация в обхвата на НМИМИС и съгласно Раздел II – Защита, Управление на инциденти с мрежовата и информационната сигурност, чл. 30 и 31 са разписани ясни процедури и правила. За да могат организациите да реагират при инцидент, те създават план по чл.30 ал.(3) и провеждат тестове за приложимост на мерките. На база наличната информация става ясно, че при инциденти с обекти от критичната инфраструктура или глобални заплахи (описани в предишния клъстер) са взети мерки и са подобрени мерките за мрежова и информационна сигурност. Но, от друга страна, в малките и по-периферни администрации, е установено формално наличие на изпълнение на изискванията за базови мерки по НМИМИС, както и рядко тестване на плановете за реакция при инцидент и липса на капацитет и ресурси за управление на инциденти. Повечето усилия в текущия момент са съсредоточени в обекти от критичната инфраструктура и превенция на рискове, като тестовете, симулации и тренировки за реакция при инциденти са недостатъчни или публично недостъпни.

1.3.3. Повишаване на осведомеността на потребителите

Тази дейност е изключително важна за общото ниво на киберсигурност и постигане на необходимите минимални нива от знания за лична и групова защита. При реализиране на планове за повишаване на осведомеността на потребителите е необходимо да се предвиди широк спектър от обучения в зависимост от специфичните задачи и роли на потребителите. Като не трябва да се пренебрегват базовите знания, създаващи устойчива киберхигиена[27] и киберкултура/етика[28].

Важността на този компонент е засегната в НМИМИС, не само за отделните потребители, но и в конкретика за ангажираните с наредбата в Чл. 9. (4) а именно: „(4) *Субектът обезпечава нивото на мрежова и информационна сигурност посредством:*

1. подходящо професионално обучение за повишаване на квалификацията на служителите в съответствие с използваната техника и технологии;

2. периодично инструктиране на служителите за повишаване на вниманието им по отношение на мрежовата и информационната сигурност; инструктажът се прави по утвърден график и се документира по начин, гарантиращ проследяемост.

Както е видно от изложеното имаме поставена рамка, дефиниран процес и цели (траектория). Тези действия би трябвало да са регулярно документирани и измерими.

[27] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[28] https://www.enisa.europa.eu/publications/cyber-hygiene/@@download/fullReport

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Последният доклад на състоянието на администрацията от 2022 г. Показва, че едва 10% от администрацията преминава задължителните си годишни обучения.

На база 150 000 работещи в държавната администрация, анализирахме колко от тях са преминали през програмата на ИПА за базова осведоменост по киберсигурност в рамките на една година. Приблизителния процент преминали е 10,9%, което е ръст и показва тенденция, която трябва да бъде поддържана.

Друг риск, който трябва да се вземе предвид, е изоставането на България в областта на базовите цифрови компетенции, като вероятността този дефицит да бъде валиден в държавната администрация трябва да бъде измерен и да бъде въведен праг за цифрова компетентност при заемане на позиция в държавната администрация.

През изминалата година Институтът по публична администрация, съвместно с обучителите по цифрова компетентност, е провел присъствено обучение за 400 представители на държавната администрация. На база данни, налични в ИПА, можем да се направят следните изводи:

- Потребителите са запознати с нормативната рамка и техните задължения;
- Потребителите смятат киберсигурността за ангажимент на ИТ отдела;
- Потребителите познават жертви на кибератаки (67%), но само 37% смятат, че те са били жертви на атака;
- Потребителите на правят разлика между отделните типове заплахи;
- За потребителите е трудно да определят, кои дейности са допустими в работно пространство;
- При инцидент, потребителите нямат отработен рефлекс с кого да се свържат;
- Потребителите нямат усещане и разбиране за оценка на киберриск в работата им

След провеждане на обучение тенденциите се променят в положителна посока в над 80% процента от участниците.

Тези и други факти водят до извода, че добрите практики за обучение трябва да бъдат развивани, а обратната връзка от обучаваните показва, че курсовете трябва да бъдат практични, кратки, визуално богати на съдържание и насочени към целева група.

Като част от кампанията за осведоменост може да бъде добавена активността на МЕУ в месеца на киберсигурност, дейността на CERT в издаването на бюлетин и информиране за заплахи, публичното присъствие на МЕУ и експертите по ключови теми, развиващата се киберекосистема, създаващият Европейска мрежа и център за компетентност в областта на киберсигурността, както и множеството НПО и Дигитални Хъбове с фокус киберсигурност.

1.3.4. Засилване на обучението и образователните програми

Идентифицираната нужда от осведоменост, предразполага необходимостта от засилване на обучителните и образователни програми. В показателите, измерващи цифровата зрялост, този показател разграничава обучението и образователните програми по киберсигурност и свързаните с нея професии от програмите по общи информационни и телекомуникационни технологии. Липсата на професии и направления киберсигурност,

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

разграничени от общите ИТ профили, създава проблем за прилагане на общата европейска рамка за компетенции умения в областта на киберсигурността – ECSF[29].

Независимо от дефинираните роли, свързани с НМИМС и ЗЗЛД е необходимо:

- Създаване на отделни професии свързани с киберсигурността;
- Създаване на отделно направление киберсигурност;
- Създаване на сертифицирани за държавната администрация бакалавърски програми, които да могат да преминат в магистърски – предоставящи знания и умения съгласно ECSF;
- Следдипломни квалификации;

Анализът идентифицира потенциал за развитие, но достига до извод, че текущото състояние на стратегическо развитие е закъсняло, необходимо е да се навакса и да се постигнат целите от програмата „ЦИФРОВО ДЕСЕТИЛЕТИЕ“ ДО 2030 и Приложение III от нея.

1.3.5 Насърчаване на научно-изследователска и развойна дейност и осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност

Към момента тази тема излиза извън обхвата на изследването, трябва да се привлича систематично фокуса върху съвместни дейности на администрация с университетската и академична общност, както и да се ангажират частни компании и НПО в процеса по развитие на капацитета на държавната администрация по темите киберсигурност и обезпечаване на капацитет и постигане на еластичност и устойчивост.

1.3.6.Подобряване на киберсигурността на веригата за доставки

Веригата за доставки е ключов идентифициран риск от ENISA. Към текущия момент съществуват добри практики при избор на доставчици на ИКТ услуги и разработка на решения или доставка на оборудване, като те могат да бъдат идентифицирани в изискванията на НМИМИС в смисъла на управление на отношения с доставчици ISO 27001:2022 – контроли A 5.19, A 5.20, A 5.22 (в случаите когато те са приложими).

В част от случаите, при възлагане на обществени поръчки, се поставят изисквания за покриване на международни стандарти и това е добра практика, когато е необходимо. В практическия ни опит е установено, че част от доставчиците притежават международни сертификати, но в оперативен план има пропуски в управлението им, което създава дефицити и рискове.

За да бъдем изчерпателни в представяне на рамката е важно да отбележим, че тя съдържа още два клъстера 3 и 4. Съдържанието на клъстерите ще бъде споменато, само като информация, но обхвата и анализа им не попада в директния обхват на доклада. При изработване на разширени анализ е необходимо да бъдат взети предвид защото напредъка по тях гарантира правната и социална устойчивост на киберсигурността. Препоръки по тях ще бъдат направени в следващите глави. Клъстерите и тяхното съдържание е както следва:

[29] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

1.4 Правни и регулаторни въпроси

1. Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги
2. Справяне с киберпрестъпленията
3. Създаване на механизми за докладване на инциденти
4. Укрепване на неприкосновеността на личния живот и защитата на данните

1.5. Сътрудничество

1. Създаване на публично-частно партньорство
2. Институционализиране на сътрудничеството между публичните агенции
3. Участие в международно сътрудничество

ГЛАВА 2. Регулации, свързани с промените в европейското законодателство и в частност новата европейска директива по мрежова и информационна сигурност

2.1. Обзор на текущата национална законова и административна рамка

Управлението в сферата на киберсигурността и мрежовата и информационна сигурност на всички публични структури се постига чрез разработване на стратегии на високо ниво и чрез изграждане и прилагане на съответната нормативна база.

2.1.1. Националната програма за развитие БЪЛГАРИЯ 2030

Националната програма за развитие БЪЛГАРИЯ 2030 е рамков стратегически документ, определен като документ от „най-висок порядък в йерархията на националните програмни документи, детерминиращ визията и общите цели на политиките за развитие във всички сектори на държавното управление, включително техните териториални измерения“[30].

В Националната програма за развитие са представени областите на въздействие, които ще бъдат обект на целенасочени инвестиции до 2030 г. В стратегическия документ тези области са подредени по приоритети и под приоритети, съпътствани от индикатори за резултат, финансов ресурс и източници за финансиране. Програмата определя три стратегически цели, групирани в пет области на развитие, и очертава 13 национални приоритета. Приоритет № 10 „Институционална рамка“ е пряко насочен към цифровото управление и възможностите за включването на гражданите и бизнеса в процесите на взимане на решения, свързани с цифровата трансформация. Приоритетът „Институционална рамка“ на програмата указва, че публичният сектор следва да се развива чрез принципите на доброто управление.

Като под приоритет в 10.3 е включено и Електронното управление, което е посочено, като основен двигател за цифрова трансформация на публичните институции. Модерните цифрови технологии следва да подпомогнат прехода от институционално центриран подход в държавното управление към управление, фокусирано върху нуждите на гражданите и бизнеса. В основата на тази трансформация са данните като основен капитал на електронното управление, както и тяхната наличност и защита. В тази връзка са очертани области на въздействие, като управление, основано на данни, съгласно което, посредством развитието и прилагането на национална рамка за интелигентно управление на данните, да бъде изградена устойчива екосистема на електронното управление, реализираща принципите на добро управление в модерна цифрова среда.

Дигитализация на публичния сектор включва развитието на ключови системи в публичния сектор (социален и финансов сектор, сигурност, защитата на населението при бедствия, аварии и други извънредни ситуации и гарантиране на бърз и лесен достъп до

[30] Национална програма за развитие България 2030, https://www.minfin.bg/bg/1394

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

спешна и неотложна помощ). Развитието на необходимите компетентности сред ключовите длъжности в администрацията е основа за успеха на цифровата трансформация.

При мрежовата и информационна сигурност се поставя акцент на връзката с доверието на потребителите на електронните услуги и зависимостта от прилагането на най-високи стандарти за киберсигурност за обезпечаване на безопасно и широко използване на продукти и услуги, базирани на данни. Съгласно документа е необходимо създаване на ефективна институционализирана единна система за мониторинг на общото състояние на киберпространството - за превенция и възстановяване от киберинциденти и за анализ и противодействие на киберзаплахите.

Националната програма „Цифрова България 2025“ се фокусира върху цифровата трансформация, обхващайки области като образование, иновации, електронно управление и киберсигурност, с цел модернизиране на икономиката и социалния живот на страната.

Като приоритетни се очертават следните области на действие на програмата:

- Условия за развитие на цифровите мрежи и услуги и по-добър достъп до тях;
- Развитие на динамична и иновативна цифрова икономика;
- Повишаване на цифровите компетенции и умения;
- Ефективни и висококачествени публични електронни услуги;
- Насърчаване на сигурна киберекосистема;
- Интернет управление

В документа киберсигурността е припозната като област от критично значение за благополучието на обществото и неговата сигурност, като се поставя акцент на необходимостта от защита от киберзаплахи и предотвратяване на киберинциденти. Политиката е насочена към развитие на способности за защита от киберзаплахи, като разчитаме на надеждни цифрови системи, което определя и бъдещата сигурност на държавата.

2.1.2. Актуализирана Национална стратегия за киберсигурност „Киберустойчива България 2023”

Политиката за киберсигурност включва различни инструменти на политиките на ЕС и НАТО, следвани от Република България. Справянето с предизвикателствата пред киберсигурността изисква действия, които произтичат от следните стратегически приоритети:

- Постигане на устойчиво киберпространство;
- Намаляване на киберпрестъпността;
- Повишаване устойчивостта на комуникационните и информационните системи, подкрепящи отбраната и националните интереси в областта на сигурността;
- Стимулиране на изследванията и иновациите за разработване на промишлени и технологични ресурси, необходими за киберсигурността;
- Разгръщане на международното сътрудничество и взаимодействие.

Очакваните дейности, цели и резултати от изпълнението на актуализираната Национална стратегия за киберсигурност „Киберустойчива България 2023” са:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Изграждане на механизъм за стратегическо и оперативно планиране и ръководство, координирани действия на политическо и стратегическо ниво за развитие на необходимия капацитет и способности за киберсигурност;
- Осигуряване на актуална киберкартина и разбиране на ситуацията в киберпространството и вземане на навременни и адекватни решения;
- Взаимодействие за ефективна и координирана превенция, реакция и възстановяване;
- Основната цел по отношение на мрежовата и информационна сигурност (МИС) е изграждането на Национална система за киберсигурност, базирана на инструментариум и решения за постигане на високо ниво на мрежова и информационна сигурност. Тя трябва да осигури ефективна киберзащита и да подпомага укрепване възможностите на мрежите и системите в държавата за противодействие срещу кибератаки от престъпници, кибертерористи, хактивисти и дори държавно-спонсорирани играчи;
- Подобряване на защитата и устойчивостта на комуникационните и информационни системи на ведомствата, които са стратегически обекти, критичните информационни инфраструктури (КИИ) и първичните администратори на данни и поддържаните от тях първични регистри;
- Установяване на ефективен и ефикасен процес по превенция и защита, реакция, разследване и адекватно правоприлагане;
- Подобрен оперативен капацитет и способности за противодействие на киберпрестъпленията и сътрудничество на национално, европейско и международно ниво;
- Защита и противодействие на различни видове атаки и организирани действия с деструктивен характер в киберпространството, които застрашават сигурността и стабилното функциониране и развитие на държавата и обществото, както и партньорски държави по силата на взаимни договорености и ангажименти;
- Постигане на устойчивост към организирани мащабни хибридни въздействия на институционално и национално ниво, гарантиране и поддържане на основните функции на държавата (управление, бизнес, граждани) и възстановяване на нормалната дейност;
- Развитие на ефективен механизъм и среда за споделяне на информация и взаимодействие между всички групи заинтересовани страни за постигане на отворено, сигурно и безопасно киберпространство;
- Усъвършенстване на нормативната уредба съобразно динамиката на обществените отношения в областта на киберсигурността. Своевременно транспониране на законодателните инструменти на ЕС във вътрешното право на Република България;
- Адаптиране на политическата и правната рамка към новите технологични тенденции и нововъзникващи технологии;
- Постигане на висока осведоменост на всички заинтересовани страни и споделено разбиране и оценка за заплахите в киберпространството във връзка с

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

нарастващата всеобща зависимост от цифровите технологии и необходимостта от адекватни мерки на всички нива за постигане на информационна и киберсигурност, развитие на обща киберкултура;

- Включване на аспекти на киберсигурността и придобиване на адекватни компетентности във всички нива и форми на образование и обучение за създаване на специалисти и лидери за сигурно и устойчиво развитие на цифровата икономика, общество и държавно управление;
- Развитие на капацитет и стимулираща среда за развитие на изследванията и иновативни приложения за превръщането на Република България във водещ център за разработване на киберустойчиви системи на бъдещето в сътрудничество със съюзниците в ЕС и НАТО.

2.1.3. Закон за киберсигурност

Основният закон, уреждащ МИС в Република България, е Законът за киберсигурност (ЗКС), (*приет от 44-то Народно събрание на 31 октомври 2018 г.. Обн. ДВ. Бр.94 от 13 Ноември 2018г., изм. ДВ. Бр.69 от 4 Август 2020г., изм. И доп. ДВ. Бр.85 от 2 Октомври 2020г., изм. И доп. ДВ. Бр.15 от 22 Февруари 2022г., изм. ДВ. Бр.25 от 29 Март 2022*г.) В своята същност, ЗКС транспонира Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза като е внимателно съобразен с българската киберекосистема, рискове, заплахи, предизвикателства и действителност. Посредством Закона за киберсигурност се уреждат:

- организацията, управлението и контрола на киберсигурността, определянето на компетентните органи в областта на киберсигурността, както и техните функции и правомощия, регламентирането на дейностите по предприемане на необходимите мерки за постигане на високо общо ниво на сигурност на мрежите и информационните системи, като един основен стълб на киберсигурността, така че да се подобри функционирането на вътрешния пазар;
- институционалната рамка в областта на киберсигурността, превенцията и противодействието на кибератаките, насочена към по-голяма ефективност и по-добра координация между съществуващите органи и звена в държавната администрация;
- създаването на нови компетентни органи, като Национално единно звено за контакт, регламентира се управлението и организацията на националната система за киберсигурност, Националния координатор по киберсигурност, секторни екипи за реакция при инциденти в киберсигурността – ЕРИКС, както и Национален ЕРИКС, разработването на Националната стратегия за киберсигурност, регламентират се въпросите за междуинституционална взаимосвързаност и сътрудничество;
- Регулацията на мрежовата и информационна сигурност на административните органи, изискванията към тях да осигуряват и отговарят за мрежовата и информационната сигурност на използваните от тях информационни

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

системи, също така изискванията и стандартите за сигурност, на които трябва да отговарят информационните системи за въвеждане, изпращане, обработка, достъп, обмен, съхраняване и архивиране на данни, както и общите мерки за сигурност, които трябва да предприемат;

- Статутът и функционирането на операторите на съществени услуги (ОСУ);
- Националните компетентни органи (НКО), които разполагат с всички необходими правомощия и средства за оценяване на това дали операторите на съществени услуги изпълняват задълженията си;
- Статутът и функционирането на доставчиците на цифрови услуги (ДЦУ).

Със закона се определят секторите на въздействие, а именно:

- Публична администрация;
- Енергетика: електроенергия, нефт, природен газ;
- Транспорт: Въздушен транспорт, Железопътен транспорт, Воден транспорт, Автомобилен транспорт;
- Банково дело;
- Инфраструктури на финансовия пазар;
- Здравеопазване – Здравни заведения (включително болници и частни клиники);
- Доставка и снабдяване с питейна вода;
- Цифрова инфраструктура: ТОИ (точка за обмен в интернет),
- Доставчици на DNS услуги, Регистри на имената на домейни от първо ниво.

2.1.4. Наредба за минималните изисквания за мрежова и информационна сигурност

Посредством чл. 3. ал.2 от Закона се изисква създаването на Наредбата за минималните изисквания за мрежова и информационна сигурност. В Наредбата, освен организационни, се съдържат и технически изисквания. Посредством НМИМИС се уреждат:

✓ Определяне на минималните изисквания за мрежова и информационна сигурност;

✓ Въвеждане на правила за извършване на проверките за съответствие с изискванията за мрежова и информационна сигурност;

✓ Определяне на реда за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за киберсигурност;

✓ Стандартизиране на формите за уведомленията за инциденти, съгласно чл. 21, ал. 4 от Закона за киберсигурност, формата за обобщена статистическа информация за инциденти, съгласно чл. 17, ал. 8 от Закона за киберсигурност и уеднаквяване на таксономията и приоритизацията в тази област. Съгласно задълженията, заложени в чл.12, т.7 от ЗКС, се разработва и утвърждава методика и правила за извършване на

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

оценка на съответствието с мерките за мрежова и информационна сигурност, определени с НМИМИС.

2.1.5 Методика за определяне на оператори на съществени услуги в съответствие с изискванията на закона за киберсигурност

Методиката определя последователността на дейностите при идентифициране и регистриране на оператори на съществени услуги в съответствие с изискванията на Закона за киберсигурност.

В процеса на идентифициране на операторите на съществени услуги административните органи, определени с Решение на Министерския съвет съгласно чл. 16, ал. 1 от Закона за киберсигурност (административни органи), оценяват за всеки подсектор от ресорния им сектор кои услуги трябва да се считат за съществени за поддържането на критични обществени и икономически дейности и дали субектите, които ги предоставят, отговарят на критериите на чл. 4, ал. 2 от Закона за киберсигурност, а именно предоставянето на тази услуга да зависи от мрежи и информационни системи и инцидентите в мрежовата и информационна сигурност да имат значително увреждащо въздействие върху предоставянето на тази услуга.

2.1.6. Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност

Предприятията, предоставящи обществени електронни съобщителни мрежи или услуги, съгласно чл. 243, ал.1 на Закона за електронните съобщения (ЗЕС), предприемат подходящи и пропорционални технически и организационни мерки за управление на риска за сигурността на мрежите и услугите, осигуряващи ниво на сигурност, съответстващо на оценения риск.

С Решение №162 от 19.05.2022 г., в изпълнение на чл. 243, ал. 3 на Закона за електронни съобщения (ЗЕС), КРС е приел Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност (Правила).

Съгласно чл. 243б, ал.1 от ЗЕС предприятията, предоставящи обществени електронни съобщителни мрежи или услуги, уведомяват незабавно комисията за всеки инцидент, свързан със сигурността, който е оказал значително въздействие върху функционирането на мрежите или услугите.

В Правилата са определени критериите за определяне на въздействието като значително на инцидент свързан със сигурността, изисканата информация, форматът и начинът на уведомяване на инцидентите, свързани със сигурността.

За уведомяване за възникнал инцидент, свързан със сигурността се използва формата, съгласно Приложение №3 на Правилата.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

С цел разпознаваемост и максимална експедитивност при обработка на уведомленията е необходимо изпратеното до КРС писмо задължително да съдържа „Относно: Инцидент свързан със сигурността".

Прегледът на стратегическите документи и регулаторна рамка, показва, че държавата има воля да възприеме киберсигурността като императив на националната сигурност при съобразяване с основните европейски изисквания.

Към настоящия момент е изградена основната нормативна рамка, уреждаща киберсигурността – Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), чиито правила за извършване на проверки за съответствие с изискванията за мрежова и информационна сигурност са допълнени с „Методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с Наредбата за минималните изисквания за мрежова и информационна сигурност".

Динамичното развитие на европейската нормативна рамка за киберсигурност, ускорено от световната политическа и технологична конюнктура, ще наложи значителни промени, породени от влизане в сила и последващо задължение за транспониране в националното ни законодателство на определени директиви и регламенти, включително, но не само:

- Директива за мрежите и информационните системи 2 (NIS2): Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. Относно мерките за високо общо ниво на киберсигурност в ЕС, за изменение на Регламент (ЕС) 910/ 2014 и Директива (ЕС) 2018/1972; за отмяна на Директива (ЕС) 2016/1148
- Директива за устойчивостта на критични субекти (CER): Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. Относно устойчивостта на критични субекти; за отмяна на Директива 2008/114/ЕО
- Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. Относно цифровата оперативна устойчивост за финансовия сектор; за изменение на Регламенти (ЕО) 1060/2009, (ЕС) 648/2012, (ЕС) 600/2014, (ЕС) 909/2014 и (ЕС) 2016/1011 (DORA).

Промените поставят сериозни предизвикателства пред държавната администрация, която безспорно е определена, като задължен субект в цитираните европейски актове, които ще се разгледат в следващите раздели от настоящия доклад.

2.1.7. Единна политика за киберсигурност

Формирането на единна политика за киберсигурност е отговорност на Народното събрание, Министерския съвет и Президента. Функциите и отговорностите по киберсигурността са разпределени между висшите държавни органи както следва: Народното събрание на Република България осигурява приемането на закони и други актове, свързани с киберсигурността и упражнява парламентарен контрол. Президентът, в качеството му на Върховен главнокомандващ на въоръжените сили на Република България, получава цялостна информация за състоянието и развитието на Националната система за киберсигурност, а при въвеждане на „извънредно положение", „военно положение" или

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

„положение на война“ ръководи дейностите по осигуряване на киберустойчивост на държавното и военното управление. Управлението на Националната система за киберсигурност се осъществява от Министерския съвет в съответствие с Конституцията, законите и подзаконовите нормативни актове и при съобразяване с целите и приоритетите, посочени в приети стратегически документи. Министерският съвет приема и периодично актуализира Националната стратегия за киберсигурност. В периода 2017-2021г. Програмата за управление на правителството на Република България, в секторните програми и плановете на компетентните административни органи и техните администрации, са отразени съответните цели, насоките и очакваните резултати от създаването и развитието на Националната система за киберсигурност. Министерският съвет приема Пътна карта и План за изпълнение и следи за постигане на приоритетите и целите, както и за осигуряване на необходимите ресурси за изпълнение на заложените дейности. Министерският съвет в своите дългосрочни програмни документи определя краен срок за изграждане на напълно завършена интегрирана национална екосистема за киберсигурност.

Съветът по сигурността към Министерския съвет анализира състоянието на системата за защита на националната сигурност, изготвя оценки и предлага решения и действия, по отношение осигуряване и защита на мрежовата и информационната сигурност от посегателства, включително и по отношение на способностите за противодействие на заплахи и управление при кризи/киберкризи, като съществен елемент от дейностите по защита на националната сигурност.

Координирането на действията на политическо и стратегическо ниво за гарантиране постигането на необходимите капацитет и способности за киберсигурност, се осъществява от постоянно действащ консултативен орган Съвет по киберсигурност към Министерски съвет. Съветът осигурява сътрудничеството между компетентните държавни органи, бизнеса, академичния сектор, неправителствените организации при определянето и провеждането на държавната политика в областта на киберсигурността. Съставът и функциите на Съвета се определят със закон. Организацията на дейността на Съвета се урежда с акт на Министерски съвет. Функциите на секретар на Съвета се изпълняват от националния координатор по киберсигурност, определен от министър-председателя. Националният координатор, под ръководството на Председателя на Съвета по киберсигурност организира, ръководи изготвянето/актуализирането на Националната стратегия за киберсигурност и Пътната карта към нея, които са основа за реализиране на политиката на стратегическо ниво. Към Съвета могат да се създават работни групи за изготвяне на проекти на стратегически документи и нормативни актове или на други експертни предложения по конкретни въпроси, свързани с компетентността им.

2.2 Обзор на регулации, директиви и политика на ЕС, променящи изискванията за киберсигурност към държавната администрация

За целите на изследването екипът направи обзор с кратки коментари на всички нови регулации в сферата на мрежовата и информационна сигурност. Въпреки че не претендира

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

за изчерпателност, обзорът показва динамично развиваща се европейска нормативна база в сектора на мрежовата и информационна сигурност. Резултатите са отразени в таблица 1.

Таблица 1. Обзор на регулации, директиви и политика на ЕС

Европейски нормативен акт	Означение	Статус към края на 2023 г.
Регламент относно ENISA и сертифицирането на киберсигурността на ИКТ както и за отмяна на Акта за киберсигурността	(EU) 2019/881 17.04.2019	Действащ
https://eur-lex.europa.eu/eli/reg/2019/881/oj Регламентът укрепва статута на Агенцията за киберсигурност (ENISA) като й дава постоянен мандат, повече ресурси и отговорности. Въвежда за първи път Европейска рамка за сертифициране на киберсигурността за продукти, услуги и процеси в областта на ИКТ. С Регламента се създава и Европейска рамка за сертифициране на киберсигурността. С нея се предвижда механизъм за установяване на европейски схеми за сертифициране на киберсигурността и за удостоверяване, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, които са били оценени в съответствие с такива схеми, отговарят на определени изисквания за сигурност с цел да се защити наличността, автентичността, целостта или поверителността на съхраняваните, предаваните или обработваните данни или на функциите и услугите, предлагани или направени достъпни чрез тези продукти, услуги и процеси през целия им жизнен цикъл. Всяка държава членка определя един или повече национални органи за сертифициране на киберсигурността на своя територия или, по взаимно съгласие с друга държава членка, определя един или повече национални органи за сертифициране на киберсигурността, установени във въпросната друга държава членка, които да отговарят за задачите по надзора в определящата държава членка. С Регламента се определят изискванията и правомощията на националните органи за сертифициране на киберсигурността. С Регламента се създава Европейска група за сертифициране на киберсигурността. Тя е съставена от представители на националните органи за сертифициране на киберсигурността или представители на други съответни национални органи.		
Регламент относно хармонизирани правила за справедлив достъп до данни и за тяхното използване (Акт за данните)	(EU) 2023/2854 13.12.2023	в сила, прилага се от 12 септември 2025 г.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

https://www.europeansources.info/record/proposal-for-a-regulation-on-harmonised-rules-on-fair-access-to-and-use-of-data-data-act/ Актът за данните задължава юридическите или физическите лица - „притежатели на данни“, да споделят събрани данни с други във веригата на стойността чрез „свързани продукти“, „свързани услуги“ и „виртуални асистенти“. Актът за данните задължава притежателите на данни да предоставят данните на органи от публичния сектор, Европейската комисия, Европейската централна банка и органи на Европейския съюз в случай на изключителна необходимост business to government B2G		
Регламент за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза EURATOM	2023/2841 - 13.12.2023	Действащ
https://www2.deloitte.com/content/dam/Deloitte/bg/Documents/legal/Legal%20Newsletter%20Issue%20124_1-15Jan2024.pdf С Регламента се определят мерки за създаването на вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността за всеки субект на Съюза и се създава нов Междуинституционален съвет по киберсигурност (МСК), който да наблюдава и подкрепя неговото прилагане от субектите на Съюза. Предоставя се разширен мандат на екипа за незабавно реагиране при компютърни инциденти за институциите, органите, службите и агенциите на ЕС (CERT-EU) като център за разузнавателни данни за заплахи, обмен на информация и координация на реакцията при инциденти, централен консултативен орган и доставчик на услуги. CERT-EU се преименува на „Служба за киберсигурност за институциите, органите, службите и агенциите на Съюза“, но запазва краткото си наименование CERT-EU, тъй като то вече е познато		
Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA)	2022/2554 14.12.2022	в сила, прилага се от 17 януари 2025

Това е секторен правен акт за финансови институции, с който се въвеждат правила за управлението на риска в областта на ИКТ (установяване, защита и предотвратяване, откриване, реакция и възстановяване, обучение и задълбочаване на познанията, и комуникиране), докладване на инциденти, тестване на оперативна устойчивост и мониторинг на риска от трети страни в ИКТ. държавите членки не следва да прилагат разпоредбите на Директивата МИС 2 относно управлението на риска в киберсигурността и задълженията за докладване, както и надзора и правоприлагането спрямо финансови субекти, обхванати от DORA. засяга Поднадзорни на КФН лица: • Инвестиционни посредници • Лица, управляващи алтернативни инвестиционни фондове • Управляващи дружества • Застрахователни и презастрахователни дружества; • Застрахователни, презастрахователни посредници и посредници, предлагащи застрахователни продукти като допълнителна дейност • Институции за професионално пенсионно осигуряване • Доставчици на услуги за колективно финансиране • Централни депозитари на ценни книжа • Централни контрагенти • Места на търговия • Регистри на трансакции		
Регламент за създаване на програмата „Цифрова Европа“ Регламент Програма Цифрова Европа	2021/694 29.04.2021	Действащ

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

https://www.frr-bg.org/wp-content/uploads/2023/09/analysis-a1-final-version.pdf
E-codex: https://www.e-codex.eu/faq-e-codex

Програма „Цифрова Европа“ (Digital Europe) е със срок на действие 2021 – 2027 г. Определеният бюджет за нейното изпълнение е в размер на 7 588 млрд. евро и ще се изразходва посредством четири независими двугодишни работни програми по специфичните ѝ цели, които съдържат процедурите за съответния период.

Първата работна програма обхваща процедурите в областта на данните, ИИ, облачни инфраструктура и услуги, квантова комуникационна инфраструктура, специализирани цифрови умения и внедряване на дейности за най-доброто използване на тези технологии. Останалите три работни програми са посветени на следните области на интервенция:

- Високопроизводителни изчисления
- Мрежа от европейски центрове за цифрови иновации (под пряко управление от Европейска комисия)
- Дейности в областта на киберсигурността
- Киберсигурност и доверие.

Регламент за създаване на Програма на Съюза за сигурна свързаност за периода 2023 - 2027 г.	2023/588 15.03.2023	Действащ

https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32023R0588

Обща цел: гарантиране на предоставянето и наличието в дългосрочен план на територията на Съюза и в световен мащаб на непрекъснат достъп до сигурни, автономни, висококачествени, надеждни и разходноефективни правителствени услуги за спътникови комуникации за оправомощените от правителствата ползватели чрез създаване на многоорбитална система за сигурна свързаност под граждански контрол и чрез подкрепа на защитата на критични инфраструктури. 1 от специалните цели повишаване на надеждността на комуникационните услуги на Съюза и на държавите членки и киберустойчивостта на Съюза чрез разработване на резервна инфраструктура, пасивна, проактивна и реактивна киберзащита и оперативна киберсигурност и защитни мерки срещу киберзаплахи, както и други мерки срещу заплахи от електромагнитни смущения.

Директива относно мерки за високо общо ниво на киберсигурност в Съюза NIS 2	2022/2555 14.12.2022	срок за транспониране до 17 октомври 2024 г.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Разширен обхват спрямо NIS 1, много повече сектори, като пощенски и куриерски услуги, публична администрация и управление на отпадъците. По-строги изисквания за сигурност и докладване на инциденти, което отразява необходимостта от по-високи стандарти поради напредващите киберзаплахи. Въвежда по-строги мерки за прилагане, включително по-високи глоби и по-строг регулаторен надзор, за да се гарантира съответствие.

Силен акцент върху сигурността на веригата за доставки, като признава нейното критично въздействие върху киберсигурността като цяло. Премахва се разграничението между операторите на основни услуги и доставчиците на цифрови услуги. Субектите се класифицират въз основа на тяхната важност и разделени на две категории: съществени и важни субекти,. Държавната администрация е съществен субект.

Приложение 1 към Директивата - СЕКТОРИ С ВИСОКА СТЕПЕН НА КРИТИЧНОСТ

1. Енергетика
2. Транспорт
3. Банков сектор
4. Инфраструктури на финансовия пазар
5. Здравеопазване
6. Питейна вода
7. Цифрова инфраструктура
8. Управление на услуги в областта на ИКТ (между предприятия)
9. Публична администрация:
   - Органи на държавната администрация на централното държавно управление, определени от държава членка в съответствие с националното право
   - Органи на държавната администрация на регионално равнище, определени от държава членка в съответствие с националното право
10. Космическо пространство

Приложение 2 към Директивата – ДРУГИ КРИТИЧНИ СЕКТОРИ:

Пощенски и куриерски услуги, Управление на отпадъците, Производство, изготвяне и дистрибуция на химикали, Производство, преработка и разпространение на храни, Производство на медицински изделия и медицински изделия за инвитро диагностика, Производство на компютри, електронни и оптични продукти, Производство на електрически съоръжения, Производство на машини и оборудване, некласифицирани другаде, Производство на моторни превозни средства, ремаркета и полуремаркета, Производство на друго транспортно оборудване

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламент за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове	2021/887 20.05.2021	Действащ
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R0887 Регламентира се създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове. С него се цели ЕС да запази и развие технологичния и промишления капацитет в областта на киберсигурността, необходим за укрепване на доверието и сигурността, включително поверителността, целостта и достъпността на данните в цифровия единен пазар. Регламентът задължава всяка държава членка да определи национален координационен център, който да отговаря на уредените в Преамбюла на Регламента задължителни критерии. Като Европейски център е определен Букурещ, за България: Дирекция „Мрежова и информационна сигурност“ към Изпълнителна агенция „Инфраструктура на електронното управление“ е Национален Координационен център по смисъла на член 7, параграф 1 от Регламент (ЕС) 2021/887.		
Регламент относно компютризирана система за трансграничен електронен обмен на данни в областта на съдебното сътрудничество по гражданскоправни и наказателно правни въпроси (система e-CODEX)	2022/850 30.05.2022	Действащ

https://eur-lex.europa.eu/eli/reg/2022/850/oj

Услугите, предоставяни от e-CODEX, позволяват сигурна комуникация и обмен на информация между държавите-членки в областта на правосъдието. По-широката визия на e-CODEX е, че всеки гражданин или юрист в Европейския съюз може да комуникира по електронен път с всеки правен орган, включително комуникацията на съдебните органи помежду си. Системата e-CODEX в момента се внедрява за европейски нареждания за разследване и плащане, процедури за искове с малък материален интерес, взаимно признаване на финансови санкции и присъди лишаване от свобода. Освен това експертите проучват e-CODEX като система за предаване за сигурен обмен на електронни доказателства между съдебните органи по наказателни дела. e-CODEX е децентрализирана мрежа от точки за достъп до e-CODEX, установени с всеки участник в e-CODEX. Без да замества съществуващите бек-енд системи в държавите-членки, e-CODEX свързва националните и европейските ИТ системи в областта на електронното правосъдие. Следователно всеки участник в e-CODEX трябва да настрои своя собствена точка за достъп, за да участва в комуникацията.

Регламент за създаване на европейска единна точка за достъп, осигуряваща централизиран достъп до публично достъпна информация от значение за финансовите услуги, капиталовите пазари и устойчивото развитие	2023/2859 13.12.2023	Действащ

https://eur-lex.europa.eu/eli/reg/2023/2859

До 10 юли 2027 г. ЕОЦКП създава и управлява европейска единна точка за достъп (ЕЕТД), предоставяща централизиран електронен достъп до следната информация:

- информация, оповестявана публично съгласно законодателните актове на Съюза, изброени в приложението, или съгласно всеки друг правнообвързващ акт на Съюза, който предвижда централизиран електронен достъп до информация в ЕЕТД;
- информация, която всеки субект, уреден от правото на държава членка, избере да предостави на доброволен принцип в ЕЕТД в съответствие с член 3, параграф 1 и която е посочена в законодателните актове на Съюза, изброени в приложението, или в други правнообвързващи актове на Съюза, които предвиждат централизиран електронен достъп до информацията чрез ЕЕТД.

Регламент относно европейска рамка за управление на данните	2022/868 30.05.2022	Действащ
https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022R0868 Акт за управление на данните - С Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 г. относно европейска рамка за управление на данните и за изменение на регламент (ЕС) 2018/1724 (Акт за управление на данните) се установяват: ● условията за повторното използване в рамките на ЕС на някои категории данни, притежавани от организациите от обществения сектор; ● рамка за уведомяване и надзор за предоставяне на посреднически услуги за данни; ● рамка за доброволна регистрация на субекти, които събират и обработват данни, предоставени за алтруистични цели; рамка за създаването на Европейски комитет за иновации в областта на данните.		
Делегиран регламент за определяне на правила за прилагането на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за управление на рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност за организациите, обхванати от регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014	2022/1645 14.07.2022	в сила, прилага се от 16 октомври 2025 г.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Определят се изискванията, на които трябва да отговарят организациите, посочени в член 2 - производствени и проектантски организации, които са предмет на подчасти Ж и Й на раздел А от приложение I (част 21) към Регламент (ЕС) № 748/2012, с изключение на проектантски и производствени организации, които участват единствено в проектирането и/или производството на въздухоплавателни средства ELA2 съгласно определението в член 1, параграф 2, буква й) от Регламент (ЕС) № 748/2012; б) летищни оператори и доставчици на обслужване по управление на перона, за които се прилага приложение III — част „Изисквания към организацията“ (част ADR.OR)“ към Регламент (ЕС) № 139/2014. 2. Настоящият регламент не засяга изискванията за информационна сигурност и киберсигурност, определени в точка 1.7 от приложението към Регламент за изпълнение (ЕС) 2015/1998 и в член 14 от Директива (ЕС) 2016/1148., за да идентифицират и управляват рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност, които биха могли да засегнат системите на информационните и комуникационните технологии и данни, използвани за целите на гражданското въздухоплаване, и да откриват събития, свързани с информационната сигурност, да идентифицират тези, които се считат за инциденти, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, както и да реагират на тези инциденти, свързани с информационната сигурност, и да се възстановяват от тях.

Регламент за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки	2020/1536 22.10.2020	Действащ

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.351.01.0001.01.ENG

в списъка на подлежащите на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложение I към Регламент (ЕС) 2019/796, следва да бъдат включени две физически лица и един орган. Тези физически лица и този орган са отговорни за кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членове, или са участвали в такива кибератаки, по-специално в кибератаката срещу Германския федерален парламент (Deutscher Bundestag), която беше извършена през април и май 2015 г.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламент относно подробните правила за условията за функциониране на уеб услугата и правилата за защита и сигурност на данните, приложими за уеб услугата, както и мерките за разработването и техническото изпълнение на уеб услугата	2022/1409 18.08.2022	Действащ

С Регламент (ЕС) 2017/2226 се създава Система за влизане/излизане за електронно записване и съхранение на датата, часа и мястото на влизане и излизане на граждани на трети страни Entry/Exit System (EES, на които им е разрешен или им е отказан краткосрочен престой на територията на държавите членки, и се изчислява продължителността на разрешения им престой. С Регламент (ЕО) № 767/2008 се създава Визовата информационна система Visa Information System (VIS) за обмен на данни между държавите членки относно заявленията за визи за краткосрочно пребиваване, визи за дългосрочно пребиваване и разрешения за пребиваване, както и относно взетото решение за анулиране, отмяна или удължаване на визата. (3) Агенцията на Европейския съюз за оперативното управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие, създадена с Регламент (ЕС) № 1077/2011 на Европейския парламент и на Съвета (3) (eu-LISA), отговаря за разработването на Системата за влизане/излизане и за оперативното управление на Системата за влизане/излизане и Визовата информационна система. eu-LISA управлява три основни системи за правосъдие и вътрешни работи, които гарантират ефективното функциониране на Шенгенското пространство:

- Шенгенската информационна система (SIS),
- Визовата информационна система (VIS),
- Европейската база данни за дактилоскопия за убежище (Eurodac).
- eu-LISA е в процес на разработване на нови ИТ системи, заедно с новата оперативна съвместимост
- архитектура за домейна ЈНА:
- системата за влизане/излизане (EES),
- Европейската система за информация и разрешаване на пътувания (ETIAS),
- Европейската информационна система за съдимост за граждани на трети страни и лица без гражданство лица (ECRIS-TCN),
- компонентите за оперативна съвместимост: sBMS, CIR, ESP, MID и CRRS. През 2022 г. eu-LISA също започна подготовка за поемане на оперативното управление на e-CODEX (e-Justice

Комуникация чрез онлайн обмен на данни), система, която улеснява сигурната комуникация между съдебните органи в трансгранични граждански и наказателни производства.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

С Регламент за изпълнение (ЕС) 2021/1224 на Комисията се определят спецификациите и условията за функционирането на уеб услугата, предвидена в член 13 от Регламент (ЕС) 2017/2226, включително специални разпоредби за защита и сигурност на данните. При тези спецификации и условия също се вземат предвид освободените от изискването за виза пътници по смисъла на член 45, параграф 2 от Регламент (ЕС) 2018/1240 на Европейския парламент и на Съвета (5). Тези спецификации и условия следва да бъдат адаптирани, като се вземат предвид гражданите на трети страни, за които се изисква притежаването на виза за краткосрочно пребиваване, виза за дългосрочно пребиваване или разрешение за пребиваване по смисъла на член 45в от Регламент (ЕО) № 767/2008. Регламент (ЕО) № 767/2008 се изисква въздушните, морските и международните автобусни превозвачи на групи от хора по сухопътен маршрут да използват портала за превозвачи, за да проверяват дали гражданите на трети страни, за които има изискване за виза за краткосрочно пребиваване или виза за летищен транзит, или които са длъжни да притежават виза за дългосрочно пребиваване или разрешение за пребиваване, имат валидна виза за краткосрочно пребиваване, виза за летищен транзит, виза за дългосрочно пребиваване или разрешение за пребиваване. (7) За да се даде възможност на превозвачите да проверяват дали гражданинът на трета страна, който подлежи на изискване за виза или от когото се изисква да притежава виза за летищен транзит, виза за дългосрочно пребиваване или разрешение за пребиваване, има валидна виза или разрешение за пребиваване, те следва да имат достъп до уеб услугата. Превозвачите следва да имат достъп до уеб услугата чрез схема за идентифициране и да могат да изпращат и получават съобщения във формат, определен от eu-LISA С Регламент 1409/2022 се създават правила за защита и сигурност на данните, приложими към схемата за идентифициране и се регулира достъпа на превозвачите до описаните системи.		
Регламент 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги)	(ЕС) 2022/2065 от 19.10.2022	в сила, прилага се от 17 февруари 2024

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

https://strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=8035 Регламентът въвежда редица мерки и задължения за доставчиците на посреднически услуги на информационното общество, пропорционални на размера, въздействието и рисковете, които техните услуги могат да създадат за гражданите и обществото. За проследяване изпълнението на тези задължения, както и за правилното функциониране на Единния цифров пазар, регламентът предвижда създаването на механизъм и структури на европейско и национално ниво, които да осигурят ефективен надзор, сътрудничество и правоприлагане. На европейско ниво ще бъде създаден Европейски съвет за цифровите услуги, а всяка държава членка на ЕС, съгласно изискванията на чл. 49 от регламента, следва да определи един национален орган, който да изпълнява функциите на национален Координатор за цифровите услуги и самостоятелно или подпомогнат от други компетентни органи, определени на национално равнище, ще отговаря за надзора на доставчиците на посреднически услуги и прилагането на регламента. Съгласно разпоредбите на Регламент (ЕС) 2022/2065, компетентните органи, определени на национално ниво, във връзка с неговото прилагане, разполагат с изключителни правомощия да упражняват надзор и да осигуряват спазването на регламента по отношение на доставчиците на посреднически услуги с място на установяване в България, с изключение на надзора на много големите онлайн платформи и много големите онлайн търсачки, който ще се осъществява от ЕК и по-отношение на който ще имат само подпомагащи функции. В тази връзка има необходимост от изменение и допълнение на действащата нормативна уредба за регламентиране на функциите и правомощията на националите органи, тяхната компетентност за осъществяване на контрол над доставчиците на посреднически услуги за изпълнение на изискванията на Регламент (ЕС) 2020/2065, както и за въвеждане на механизми за налагане на определените в регламента санкции и глоби. С проекта на ЗИД на ЗЕС урежда статута и правомощията на Координатора за цифровите услуги (КЦУ/Координатора), а именно Комисията за регулиране на съобщенията (КРС/Комисията). КРС ще осъществява контрол върху дейността на доставчиците на посреднически услуги на информационното общество, които не представляват платформи за споделяне на видеоклипове, за изпълнение на задълженията им по Регламента.		
Регламент за достъпни и справедливи пазари в цифровия сектор (Digital Markets Act)	(ЕС) 2022/1925 14.09.2022	Действащ

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

DMA https://en.wikipedia.org/wiki/Digital_Markets_Act

Целта на регламента е да се допринесе за правилното функциониране на вътрешния пазар, като се определят хармонизирани правила, които гарантират за всички предприятия достъпни и справедливи пазари в цифровия сектор навсякъде в Съюза, където присъстват контролиращи достъпа предприятия, в полза на бизнес ползвателите и крайните ползватели. DMA се прилага по отношение на основните платформени услуги, предоставяни или предлагани от контролиращи достъпа предприятия на бизнес ползватели, които са установени в Съюза, или на крайни ползватели, които са установени или се намират в Съюза, независимо от мястото на установяване или на пребиваване на контролиращите достъпа предприятия и независимо от приложимото към предоставянето на услугата право. Не се прилага за пазари, свързани със: а) електронни съобщителни мрежи съгласно определението в член 2, точка 1 от Директива (ЕС) 2018/1972; б) електронни съобщителни услуги съгласно определението в член 2, точка 4 от Директива (ЕС) 2018/1972, различни от свързаните с междуличностни съобщителни услуги без номерà.. Двадесет и две услуги в шест компании (считани за „gatekeepers“ или контролиращи достъпа предприятие) – Alphabet, Amazon, Apple, ByteDance, Meta и Microsoft – са идентифицирани като „основни платформени услуги“ от ЕС през септември 2023 г. Тези компании трябва да изпълнят всички разпоредби на закона до 6 март 2024 г.

DMA обхваща осем различни сектора, които се наричат основни платформени услуги (CPS). Поради наличието на контролиращи достъпа предприятиея върху конкуренцията на пазара, CPS се считат за проблематични от Европейската комисия:

- онлайн търсачки;
- онлайн посреднически услуги
- социални мрежи;
- платформи за споделяне на видео;
- комуникационни платформи
- рекламни услуги;
- операционни системи;
- облачни услуги

Регламент за създаване на рамка от мерки за укрепване на европейската екосистема в областта на полупроводниците Chips Act	2023/1781 13.09.2023	Действащ

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

https://www.europeansources.info/record/proposal-for-a-regulation-establishing-a-framework-of-measures-for-strengthening-europes-semiconductor-ecosystem-chips-act/ю

Установява рамка за укрепване на екосистемата на полупроводниците в Европейския съюз (ЕС). Мерките включват създаването на инициативата „Чипове за Европа“, определянето на критерии за признаване и подпомагане на интегрирани производствени мощности и открити леярни в ЕС, както и създаването на механизъм за координация между държавите-членки на ЕС и Европейската комисия за картографиране и наблюдение на Полупроводниковия сектор на ЕС, както и предотвратяване на кризи, реакция при недостиг и, когато е уместно, консултиране на заинтересованите страни. Общата цел на инициативата е да се постигне широкомащабно изграждане на технологичен капацитет и да се подкрепят свързаните научноизследователски и иновационни дейности в цялата верига за създаване на стойност в областта на полупроводниците в Съюза, за да се даде възможност за разработване и внедряване на авангардни полупроводникови технологии, полупроводникови технологии от следващо поколение и авангардни квантови технологии и за въвеждане на иновации в утвърдените технологии, които ще укрепят способностите за усъвършенствано проектиране, системна интеграция и способности за производство на интегрални схеми в Съюза и по този начин ще повишат конкурентоспособността на Съюза. Тя допринася и за постигането на екологичния и цифровия преход, по-специално като намалява въздействието на електронните системи върху климата, подобрява устойчивостта на интегралните схеми от следващо поколение и укрепва процесите на кръговата икономика, способства за качествени работни места в екосистемата в областта на полупроводниците и отчита принципа „сигурност на етапа на проектирането“, който осигурява защита срещу заплахи за киберсигурността - виж Приложенията ! https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.229.01.0001.01.ENG

Директива за устойчивостта на критичните субекти	2022/2557 14.12.2022	срок за транспониране до 17 октомври 2024 г.

https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Директива 2008/114/ЕО, транспонирана посредством Закона за защита при бедствия. CER цели създаване на всеобхватна рамка, насочена към устойчивостта на критични субекти по отношение на всички рискови фактори на средата. CER значително увеличи обхвата на приложимост спрямо Директива 2008/114/ЕО- вече обхваща и обхваща банкови и финансови пазари, здравеопазване, питейни и отпадъчни води, цифрова инфраструктура, публична администрация и космическо пространство. Интересното е, че CER третира всички критични субекти като доставчици на основни услуги.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламент относно европейска рамка за управление на данните	COM (2020) 767 25.11.2020	Предложение

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767

Предложението допълва Директива (ЕС) 2019/1024 на Европейския парламент и на Съвета от 20 юни 2019 г. относно отворените данни и повторната употреба на информация от обществения сектор (Директива за отворени данни) . Това предложение се отнася до данни, съхранявани от органи от обществения сектор, които са обект на правата на други лица и следователно попадат извън обхвата на настоящата директива. Предложението има логични и последователни връзки с другите инициативи, обявени в Европейската стратегия за данните. Има за цел да улесни споделянето на данни, включително чрез засилване на доверието в посредниците за споделяне на данни, които се очаква да бъдат използвани в различните пространства за данни. То не цели предоставяне, изменение или премахване на съществени права за достъп и използване на данни.https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020PC0767

Регламент относно информационната сигурност в институциите, органите, службите и агенциите на Съюза	2022/119	Предложение

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0119

Предложението за Регламент има за цел да създаде минимален набор от правила за информационна сигурност, приложими за всички институции и органи на Съюза. Той се прилага за цялата информация, обработвана и съхранявана от институциите и органите на Съюза, включително информацията, свързана с дейностите на Европейската общност за атомна енергия, различна от класифицираната информация на Евратом. Както некласифицираната информация, така и European Union classified information (‘EUCI’) са обхванати от настоящото предложение.

Всички институции и органи на Съюза си сътрудничат в Междуинституционална координационна група за информационна сигурност, която действа с консенсус и в общ интерес на институциите и органите на Съюза. Координационната група събира органите по сигурността на всички институции и органи и изготвя насоки за прилагането на настоящия регламент..

Създадени са пет подгрупи, съставени от експерти, представляващи различни институции и органи, с цел рационализиране на процедурите и други практически аспекти, свързани с информационната сигурност.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламентът предвижда 3 категории некласифицирана информация: информация за обществено ползване, нормална информация и чувствителна некласифицирана информация. Дефинирани са всички категории, като са определени маркировки и условия за работа за защита на такава информация.

EUCI Като най-обемната част от предложението, тази глава е структурирана в седем раздела, както следва: Общи разпоредби, Сигурност на персонала, Физическа сигурност, Управление на EUCI, Защита в комуникационните и информационните системи, Индустриална сигурност и Споделяне на EUCI и обмен на класифицирана информация.

Разделът относно общите разпоредби предвижда четири нива на EUCI: TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL, RESTREINT UE/EU RESTRICTED и предвижда задължение за институциите и органите на Съюза да предприемат необходими мерки за сигурност в съответствие с резултатите от процеса на управление на риска за информационната сигурност.

Всеки от останалите раздели се фокусира върху стандартите за защита на КИЕС, свързани с тяхната специфична област. Подробностите за тази защита на EUCI са посочени в приложения от II до V. Приложение VI предоставя таблица за еквивалентност на КИЕС с класификациите за сигурност на държавите-членки и Европейската общност за атомна енергия.

Регламент относно хоризонтални изисквания за киберсигурност за продукти и цифрови елементи	2022/0272 (COD) 15.09.2022	Предложение

https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52022PC0454

С предложения регламент се определят (а) правила за пускане на пазара на продукти с цифрови елементи, за да се гарантира киберсигурността на такива продукти; б) съществени изисквания за проектиране, разработване и производство на продукти с цифрови елементи и задължения за икономическите оператори във връзка с тези продукти по отношение на киберсигурността; в) съществени изисквания за процесите за справяне с уязвимостите, въведени от производителите, за да се гарантира киберсигурността на продуктите с цифрови елементи през целия им жизнен цикъл, и задължения за икономическите оператори във връзка с тези процеси; г) правила за надзор на пазара и прилагане на горепосочените правила и изисквания.

Предложеният регламент ще се прилага за всички продукти с цифрови елементи, чиято предвидена и разумно предвидима употреба включва пряка или непряка логическа или физическа връзка за данни към устройство или мрежа.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Предложеният регламент няма да се прилага за продукти с цифрови елементи в обхвата на Регламент (ЕС) 2017/745 [медицински изделия за употреба от човека и аксесоари за такива устройства] и Регламент (ЕС) 2017/746 [ин витро диагностични медицински изделия за хора употреба и аксесоари за такива устройства], тъй като и двата регламента съдържат изисквания по отношение на устройствата, включително относно софтуера и общи задължения на производителите, обхващащи целия жизнен цикъл на продуктите, както и процедури за оценка на съответствието. Настоящият регламент няма да се прилага за продукти с цифрови елементи, които са сертифицирани в съответствие с Регламент 2018/1139 [високо единно ниво на безопасност на гражданското въздухоплаване], нито за продукти, за които се прилага Регламент (ЕС) 2019/2144 [относно изискванията за одобрение на типа за моторни превозни средства и техните ремаркета и системи, компоненти и отделни технически възли, предназначени за такива превозни средства].

Регламент относно управляваните услуги за сигурност	COM(2023)208 COM(2023)0108 18.04.2023	Предложение

https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2023/0208/COM_COM(2023)0208_EN.pdf

Предложеното целенасочено изменение има за цел да даде възможност чрез прилагане от Комисията на актове, приемането на европейски схеми за сертифициране на киберсигурността за „управлявани услуги по сигурността“ в допълнение към информационните и технологични (ИКТ) продукти, ИКТ услуги и ИКТ процеси, които вече са обхванати от Закона за киберсигурността - Regulation (EU) 2019/881. Управляваните услуги за сигурност играят все по-важна роля в превенцията и смекчаването на киберинциденти.

Предложението съдържа два члена. член 1 съдържа измененията на Регламент (ЕС) 2019/881, член 2 се отнася до влизането в сила. Член 1 съдържа целеви изменения за изменение на обхвата на Европейската рамка за сертифициране на киберсигурността в

Закона за киберсигурността да включва „управлявани услуги за сигурност“ (членове 1 и 46 от Закон за киберсигурността). Той въвежда определение на тези услуги, което е много тясно съгласувано към определението за „доставчици на управлявани услуги за сигурност“ съгласно Директивата NIS 2 (член 2от Закона за киберсигурността). Той също така добавя нов член 51а относно целите на сигурността на Европейска сертификация за киберсигурност, адаптирана към „управлявани услуги за сигурност“.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламент за определяне на хармонизирани правила относно изкуствения интелект	2021/0106 21.05.2021	Предложение Awaiting Parliament's position in 1st reading

https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52021PC0206

Предмета на регламента и приложното поле на новите правила, - пускането на пазара, въвеждането в експлоатация и използването на системи с ИИ. Определението за система с ИИ в правната рамка има за цел да бъде възможно най-неутрално по отношение на технологиите и да бъде съобразено с бъдещето предвид бързите технологични и пазарни развития, свързани с ИИ. Има приложение I, в което се съдържа подробен списък на подходите и техниките за развитието на ИИ, Ключовите участници по веригата за създаване на стойност в областта на ИИ също са ясно определени, като например доставчиците и ползвателите на системи с ИИ, които обхващат както публични, така и частни оператори.

- установява списък на забранените ИИ. Регламентът следва основан на риска подход, като разграничава употребите на ИИ, които създават i) неприемлив риск, ii) висок риск и iii) нисък или минимален риск. Списъкът на забранените практики в дял II включва всички системи с ИИ, чието използване се счита за неприемливо поради това, че противоречи на ценностите на Съюза, Забраните обхващат практики, които имат значителен потенциал да манипулират хората чрез сублиминални техники отвъд рамките на съзнаваното от човека, или да използват уязвимите места на конкретни уязвими групи, като деца или хора с увреждания, с цел съществено да изменят поведението им по начин, който би могъл да причини на тях или на друго лице психологическа или физическа вреда. Други манипулативни или злоупотребяващи практики спрямо зрели хора, за които могат да спомогнат системите с ИИ, биха могли да бъдат обхванати от съществуващото законодателство в областта на защитата на данните, защитата на потребителите и цифровите услуги, което гарантира, че физическите лица са надлежно информирани и имат свободен избор да не бъдат подлагани на профилиране или други практики, които биха могли да повлияят на реакциите им. Предложението забранява социалния рейтинг въз основа на ИИ за общи цели, извършвано от публични органи. използването на системи за биометрична идентификация от разстояние в реално време на публично достъпни места за целите на правоприлагането също е забранено, освен ако се прилагат някои ограничени изключения.
- специфични правила за системите с ИИ, които създават висок риск за здравето и безопасността или за основните права на физическите лица. В съответствие с основан на риска подход тези високорискови системи с ИИ са разрешени на европейския пазар при спазване на определени задължителни изисквания и предварително оценяване на съответствието.
- определят правилата за класификация и се обособяват две основни категории високорискови системи с ИИ:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- системи с ИИ, предназначени да бъдат използвани като защитен елемент на продукти, които подлежат на предварително оценяване на съответствието от трета страна;
https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52021PC0206

Предмета на регламента и приложното поле на новите правила, - пускането на пазара, въвеждането в експлоатация и използването на системи с ИИ. Определението за система с ИИ в правната рамка има за цел да бъде възможно най-неутрално по отношение на технологиите и да бъде съобразено с бъдещето предвид бързите технологични и пазарни развития, свързани с ИИ. Има приложение I, в което се съдържа подробен списък на подходите и техниките за развитието на ИИ, Ключовите участници по веригата за създаване на стойност в областта на ИИ също са ясно определени, като например доставчиците и ползвателите на системи с ИИ, които обхващат както публични, така и частни оператори.

- установява списък на забранените ИИ. Регламентът следва основан на риска подход, като разграничава употребите на ИИ, които създават i) неприемлив риск, ii) висок риск и iii) нисък или минимален риск. Списъкът на забранените практики в дял II включва всички системи с ИИ, чието използване се счита за неприемливо поради това, че противоречи на ценностите на Съюза, Забраните обхващат практики, които имат значителен потенциал да манипулират хората чрез сублиминални техники отвъд рамките на съзнаваното от човека, или да използват уязвимите места на конкретни уязвими групи, като деца или хора с увреждания, с цел съществено да изменят поведението им по начин, който би могъл да причини на тях или на друго лице психологическа или физическа вреда. Други манипулативни или злоупотребяващи практики спрямо зрели хора, за които могат да спомогнат системите с ИИ, биха могли да бъдат обхванати от съществуващото законодателство в областта на защитата на данните, защитата на потребителите и цифровите услуги, което гарантира, че физическите лица са надлежно информирани и имат свободен избор да не бъдат подлагани на профилиране или други практики, които биха могли да повлияят на реакциите им. Предложението забранява социалния рейтинг въз основа на ИИ за общи цели, извършвано от публични органи. използването на системи за биометрична идентификация от разстояние в реално време на публично достъпни места за целите на правоприлагането също е забранено, освен ако се прилагат някои ограничени изключения.

- специфични правила за системите с ИИ, които създават висок риск за здравето и безопасността или за основните права на физическите лица. В съответствие с основан на риска подход тези високорискови системи с ИИ са разрешени на европейския пазар при спазване на определени задължителни изисквания и предварително оценяване на съответствието.

- определят правилата за класификация и се обособяват две основни категории високорискови системи с ИИ:

.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- системи с ИИ, предназначени да бъдат използвани като защитен елемент на продукти, които подлежат на предварително оценяване на съответствието от трета страна;
- други самостоятелни системи с ИИ с последици предимно за основните права, които са изрично изброени в приложение III.

- правните изисквания за високорисковите системи с ИИ във връзка с данните и управлението им, съхраняването на документацията и записите, прозрачността и предоставянето на информация на ползвателите, човешкия надзор, надеждността, точността и сигурността. Точните технически решения за постигане на съответствие с тези изисквания могат да бъдат предоставени чрез стандарти или други технически спецификации или да бъдат разработени по друг начин в съответствие с общите инженерни или научни познания по преценка на доставчика на системата с ИИ. Тази гъвкавост е особено важна, тъй като позволява на доставчиците на системи с ИИ да избират начина, по който да изпълнят приложимите към тях изисквания, отчитайки съвременния технически и научен напредък в тази област.
- предвижда ясен набор от хоризонтални задължения за доставчиците на високорискови системи с ИИ. На ползвателите и другите участници по веригата за създаване на стойност в областта на ИИ се възлагат пропорционални задължения (напр. вносители, дистрибутори, упълномощени представители).
- определя рамката за участие на нотифицираните органи като независими трети страни в процедурите за оценяване на съответствието,
- Дял IV се отнася до някои системи с ИИ, за да се вземат предвид специфичните рискове от манипулиране, които те пораждат. Задълженията за прозрачност ще се прилагат за системи, които i) взаимодействат с хора, ii) се използват за разпознаване на емоции или за определяне на връзка със (социални) категории въз основа на биометрични данни или iii) генерират или манипулират съдържание („дълбинни фалшификати“). Когато хората взаимодействат със система с ИИ или техните емоции или характеристики се разпознават чрез автоматизирани средства, те трябва да бъдат информирани за това обстоятелство.
- В дял VI се определят системите за управление на равнището на Съюза и на национално равнище. На равнището на Съюза с предложението се създава Европейски съвет по изкуствен интелект („Съвета по ИИ“), съставен от представители на държавите членки и на Комисията.
- установява рамка за създаването на кодекси за поведение, които имат за цел да поощрят доставчиците на невисокорискови системи с ИИ да прилагат доброволно задължителните изисквания за високорисковите системи с ИИ.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Регламент за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти -Закон за кибер солидарност	2023/0109/COD	Предложение
https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2023/0209/COM_COM(2023)0209_EN.pdf Основната цел на Закона за киберсолидарност е по-добро откриване, подготовка и реагиране на заплахи и инциденти за киберсигурността. Тази цел ще бъде изпълнена чрез следните действия: ● Разгръщането на Европейски киберщит, състоящ се от всички национални оперативни центрове за сигурност („Национални SOC“) и трансгранични оперативни центрове за сигурност („Трансгранични SOC“) за изграждане и подобряване на общи способности за откриване и ситуационна осведоменост; ● Създаване на механизъм за извънредни ситуации в кибернетичното пространство, който ще се състои главно от резерва на ЕС за киберсигурност и има за цел да подкрепи държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и широкомащабни инциденти в киберсигурността. Резервът на ЕС за киберсигурност ще бъде осигурен от така наречените „доверени доставчици“, т.е. предварително избрана група от частни компании, които могат да предоставят услуги за реагиране при инциденти при поискване; и ● Създаване на Европейски механизъм за преглед на инциденти в киберсигурността за преглед и оценка на конкретни значими или широкомащабни инциденти		
Регламент за определяне на мерки за високо ниво на оперативна съвместимост на публичния сектор в целия Съюз (Акт за оперативно съвместима Европа) Резюме на становището на Европейския надзорен орган по защита на данните относно предложението за акт за оперативно съвместима Европа 2023/C 60/12	2022/0379/COD	Предложение

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Пълният текст на настоящото становище може да се намери на английски, френски и немски език на уебсайта на ЕНОЗД - https://edps.europa.eu

Целта на Предложението е насърчаване на трансграничната оперативна съвместимост на мрежите и информационните системи, които се използват за предоставяне или управление на обществени услуги в Съюза, чрез установяване на общи правила и рамка за координация на оперативната съвместимост в публичния сектор, с цел да се насърчи развитието на оперативно съвместима трансевропейска инфраструктура за цифрови обществени услуги. по-специално Предложението има за цел:

- да се гарантира последователен, ориентиран към човека подход на ЕС към оперативната съвместимост - от създаването на политиката до нейното изпълнение;
- да се създаде структура за управление на оперативната съвместимост, която да даде възможност на публичните администрации от всички равнища и сектори, както и на заинтересованите страни от частния сектор, да работят заедно — с ясен мандат за постигане на съгласие по споделени решения за оперативна съвместимост (напр. рамки, отворени спецификации, отворени стандарти, приложения или насоки);
-да се създаде съвместно екосистема от решения за оперативна съвместимост за публичния сектор на ЕС, така че публичните администрации на всички равнища в ЕС и други заинтересовани страни да могат да допринасят за такива решения и да ги използват повторно, да правят съвместни иновации и да създават обществена стойност.

Регламент относно европейското пространство на здравни данни	2022/0140/COD	Предложение

https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlsnbu94sklt

Предлага се установяване на европейско пространство на здравни данни (ЕПЗД), като се предвиждат правила, общи стандарти и практики, инфраструктури и рамка за управление на първичното и вторичното използване на електронни здравни данни. С настоящия регламент:

а) се утвърждават правата на физическите лица във връзка с наличността и контрола върху техните електронни здравни данни;

б) се определят правила за пускане на пазара, предоставяне на пазара или въвеждане в експлоатация на системи за електронни здравни досиета („системи за ЕЗД“) в Съюза;

в) се определят правила и механизми за подпомагане на вторичното използване на електронни здравни данни;

г) се създава задължителна трансгранична инфраструктура, позволяваща първичното използване на електронни здравни данни в целия Съюз;

д) се създава задължителна трансгранична инфраструктура за вторично използване на електронни здравни данни.

3.Настоящият регламент се прилага по отношение на: а) производителите и доставчиците на системи за ЕЗД и приложения за поддържане на добро здравословно състояние, пуснати на пазара и въведени в експлоатация в Съюза, и потребителите на такива продукти; б) администратори и обработващи лични данни, установени в Съюза, които обработват електронни здравни данни на граждани на Съюза и граждани на трети държави, законно пребиваващи на територията на държавите членки; в) администратори и обработващи лични данни, установени в трета държава, която е осигурила свързаност или оперативна съвместимост с платформата MyHealth@EU в съответствие с член 12, параграф 5; г) ползватели на данни, на които държателите на данни в Съюза предоставят електронни здравни данни. 4. Настоящият регламент не засяга други нормативни актове на Съюза относно достъпа до електронни здравни данни, тяхното споделяне или вторично използване, или изискванията, свързани с обработването на данни във връзка с електронни здравни данни, по-специално Регламент (ЕС) 2016/679, Регламент (ЕС) 2018/1725, […] [Акт за управление на данните COM(2020) 767 final] и Регламент […] [Законодателен акт за данните COM(2022) 68 final]. 5. Настоящият регламент не засяга Регламент (ЕС) 2017/745 и Регламент […] [Законодателен акт за изкуствения интелект COM(2021) 206 final] по отношение на сигурността на медицинските изделия и системите с ИИ, които взаимодействат със системи за ЕЗД. 6. Настоящият регламент не засяга правата и задълженията, установени в правото на Съюза или в националното право по отношение на обработването на данни за целите на докладването, удовлетворяването на исканията за информация или доказването или проверката на спазването на правните задължения.
https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlsnbu94sklt Предлага се установяване на европейско пространство на здравни данни (ЕПЗД), като се предвиждат правила, общи стандарти и практики, инфраструктури и рамка за управление на първичното и вторичното използване на електронни здравни данни. С настоящия регламент: а) се утвърждават правата на физическите лица във връзка с наличността и контрола върху техните електронни здравни данни; б) се определят правила за пускане на пазара, предоставяне на пазара или въвеждане в експлоатация на системи за електронни здравни досиета („системи за ЕЗД“) в Съюза; в) се определят правила и механизми за подпомагане на вторичното използване на електронни здравни данни; г) се създава задължителна трансгранична инфраструктура, позволяваща първичното използване на електронни здравни данни в целия Съюз;

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

д) се създава задължителна трансгранична инфраструктура за вторично използване на електронни здравни данни.

3. Настоящият регламент се прилага по отношение на:

а) производителите и доставчиците на системи за ЕЗД и приложения за поддържане на добро здравословно състояние, пуснати на пазара и въведени в експлоатация в Съюза, и потребителите на такива продукти;

б) администратори и обработващи лични данни, установени в Съюза, които обработват електронни здравни данни на граждани на Съюза и граждани на трети държави, законно пребиваващи на територията на държавите членки;

в) администратори и обработващи лични данни, установени в трета държава, която е осигурила свързаност или оперативна съвместимост с платформата MyHealth@EU в съответствие с член 12, параграф 5;

г) ползватели на данни, на които държателите на данни в Съюза предоставят електронни здравни данни.

4. Настоящият регламент не засяга други нормативни актове на Съюза относно достъпа до електронни здравни данни, тяхното споделяне или вторично използване, или изискванията, свързани с обработването на данни във връзка с електронни здравни данни, по-специално Регламент (ЕС) 2016/679, Регламент (ЕС) 2018/1725, […] [Акт за управление на данните COM(2020) 767 final] и Регламент […] [Законодателен акт за данните COM(2022) 68 final].

5. Настоящият регламент не засяга Регламент (ЕС) 2017/745 и Регламент […] [Законодателен акт за изкуствения интелект COM(2021) 206 final] по отношение на сигурността на медицинските изделия и системите с ИИ, които взаимодействат със системи за ЕЗД.

6. Настоящият регламент не засяга правата и задълженията, установени в правото на Съюза или в националното право по отношение на обработването на данни за целите на докладването, удовлетворяването на исканията за информация или доказването или проверката на спазването на правните задължения.

Регламент по отношение на създаването на рамка за европейска цифрова самоличност	2021/0136/COD	Предложение

https://secure.ipex.eu/IPEXL-WEB/download/file/082d29087b5998dd017b6371b3a445b4

Правният инструмент има за цел да гарантира при трансгранично ползване:

- достъп до надеждни решения за електронна самоличност с висока степен на сигурност,
- надеждни и сигурни решения за цифрова самоличност, на които публичните и частните услуги могат да разчитат,

- разширяване на възможностите на физическите и юридическите лица да използват решения за цифрова самоличност,
- свързване на тези решения с разнообразни атрибути и възможности за целево споделяне на данни за самоличност, които са ограничени до необходимото за конкретната поискана услуга,
- приемане на квалифицирани удостоверителни услуги в ЕС и равни условия за тяхното предоставяне.

На пазара възниква нова среда, в която акцентът се измества от предоставянето и използването на негъвкава цифрова самоличност към предоставянето и използването на специфични атрибути, свързани с тази самоличност. Налице е повишено търсене на решения за електронна самоличност, които могат да предоставят такива възможности, повишаващи ефективността и осигуряващи високо равнище на доверие в целия ЕС както в частния, така и в публичния сектор, за които е важно да могат да идентифицират и удостоверяват автентичността на потребителите с високо ниво на осигуреност

Регламент относно зачитането на личния живот и защитата на личните данни в електронните съобщения	2017/0003/COD	Предложение

https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1471165&t=d&l=en

Това предложение има за цел да актуализира правната рамка. Той има за цел укрепване на доверието и сигурността в цифровия единен пазар – ключова цел на стратегията за цифровия единен пазар. Проектът на регламент също така привежда в съответствие правилата за електронните съобщителни услуги с новите стандарти от световна класа на Общия регламент за защита на данните на ЕС (Регламент (ЕС) 2016/679).Новият регламент има за цел да подобри защитата на поверителността на електронните съобщения чрез разширяване на обхвата на правния инструмент, за да включи нови функционално еквивалентни електронни съобщителни услуги. Подобно на Европейския кодекс за електронни съобщения, това предложението включва и доставчиците на Over-the-Top (OTT) в своя обхват, за да отрази реалността на пазара.

Предложението:

- съдържа основните разпоредби, гарантиращи ограничените разрешени цели и условия за обработка на такива комуникационни данни: поверителността ще бъде гарантирана както за съдържанието, така и за метаданните, получени от електронните комуникации (напр. време на разговор и местоположение). И двете имат висок компонент на поверителност и съгласно предложените правила ще трябва да бъдат анонимизирани или изтрити, ако потребителите не са дали съгласието си, освен ако данните не се изискват например за целите на таксуването;
- разглежда защитата на крайното оборудване, като (i) гарантира целостта на информацията, съхранявана в него, и (ii) защитава информацията, излъчвана от крайното

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

оборудване, тъй като може да даде възможност за идентифициране на своя краен потребител;

- подробно описва съгласието на крайните потребители, когато е технически възможно и осъществимо, съгласието може да бъде изразено чрез използване на подходящите технически настройки на софтуерно приложение, позволяващо достъп до интернет. На крайните потребители, които са се съгласили с обработването на електронни комуникационни данни, се дава възможност да оттеглят своето съгласие по всяко време и да им се напомня за тази възможност на периодични интервали от 6 месеца, докато обработването продължава;

- налага задължение на доставчиците на софтуер, позволяващ електронни комуникации, да помагат на крайните потребители да направят ефективен избор относно настройките за поверителност.

Права на крайните потребители да контролират изпращането и получаването на електронни съобщения: с оглед на защитата на тяхната поверителност, новият регламент предлага:

- правото на крайните потребители да предотвратят представянето на идентификацията на повикващата линия, за да се гарантира анонимност;

- задължението на доставчиците на обществено достъпна междуличностна комуникация, базирана на номера, да предоставят възможност за ограничаване на приемането на нежелани обаждания;

- регламентирането на условията, при които крайните потребители могат да бъдат включени в публично достъпни директории, и условията, при които могат да се провеждат непоискани съобщения за директен маркетинг.

Надзор и прилагане на настоящия регламент: това се поверява на надзорните органи, отговарящи за GDPR. Правомощията на Европейския комитет по защита на данните се разширяват и механизмът за сътрудничество и съгласуваност, предвиден в GDPR, ще се прилага в случай на трансгранични въпроси, свързани с настоящия регламент.

ГЛАВА 3. Новата европейска директива за мрежова и информационна сигурност NIS 2

3.1. GAP анализ

GAP анализът е инструмент за стратегическо планиране, който подпомага дадена организация да прецени на какъв етап е текущо, какво иска да постигне и по какъв начин. През призмата на новата директива за мрежова информационна сигурност, този анализ обхваща следните показатели и аспекти:

3.1.1. Резюме на Директивата за NIS 2

„Директивата NIS 2“ или просто NIS2 е директива на Европейския съюз, която определя изискванията за киберсигурност, които трябва да бъдат приложени от организации от ЕС, които се считат за критична инфраструктура. Пълното ѝ наименование

е „Директива (ЕС) 2022/2555“ относно мерки за високо общо ниво на киберсигурност в целия Съюз" и е публикувано на 14 декември 2022 г.

Тъй като NIS2 е директива, това означава, че всяка държава от ЕС има ангажимент да транспонира в своето национално право посредством законодателен акт за киберсигурността, основан на изискванията на на NIS2, като NIS2 определя минималното ниво на киберсигурност, което трябва да бъде постигнато. На практика това означава, че задължените субекти, включително компаниите от частния сектор, в някои държави ще трябва да спазват минимум от изисквания, посочен в NIS2, а в други държави ще трябва да спазват по-строги изисквания за киберсигурност, посочени в местните закони.

3.1.2. Досега действащата директива за NIS и новата NIS2

Прегледът на Директива (ЕС) 2016/1148 - NIS[31] показва големи различия в прилагането ѝ от държавите членки, включително във връзка с нейния обхват, чието очертаване в много голяма степен бе оставено на преценката на държавите членки. Директива (ЕС) 2016/1148 предоставя на държавите членки и много широка свобода на преценка по отношение на прилагането на предвидените в нея задължения, свързани със сигурността и докладването за инциденти.

Поради това тези задължения бяха приложени по значително различаващи се начини на национално равнище. Съществуват сходни различия в прилагането на разпоредбите на Директива (ЕС) 2016/1148 относно надзора и правоприлагането. Всички тези различия водят до фрагментирането на вътрешния пазар и могат да имат вредно въздействие върху функционирането му, засягайки по-специално трансграничното предоставяне на услуги и нивото на киберустойчивост поради прилагането на различни мерки. В крайна сметка тези различия могат да доведат до по-голяма уязвимост на някои държави членки спрямо киберзаплахи, което би предизвикало потенциални странични ефекти за целия ЕС. NIS 2 има за цел да премахне тези големи различия между държавите членки, по-специално посредством предвиждането на минимални правила относно функционирането на координирана регулаторна рамка, установяването на механизми за ефективно сътрудничество между отговорните органи във всяка държава членка, актуализирането на списъка със сектори и дейности, подчинени на задълженията за киберсигурност, и предоставянето на ефективни правни средства за защита и правоприлагащи мерки, които са от ключово значение за ефективното правоприлагане на тези задължения.

3.1.3. Срок за влизане в сила на NIS 2

NIS 2 влиза в сила на 18 октомври 2024 г. – това е и крайният срок за страните от ЕС да приведат националното си законодателство в съответствие с с NIS 2.

[31] https://eur-lex.europa.eu/eli/dir/2022/2555

3.1.4. Значение на NIS

Пълното заглавие на старата директива за NIS беше: „Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза“.

Следователно "NIS/МИС" е съкращение от "мрежова и информационна сигурност".

3.1.5. Важност на NIS2

NIS 2 е изключително важна, защото поставя строги изисквания за киберсигурност за голям брой компании и организации в Европейския съюз – според някои оценки повече от 100 000 компании в Европейския съюз ще трябва да изпълнят изискванията на NIS 2.

Въпреки, че не се прилага за толкова много задължени субекти, колкото например ОРЗД на ЕС, NIS 2 със сигурност ще се превърне в de facto стандарт за критична инфраструктура, на който трети (извън ЕС) страни ще подражават – много подобен сценарий се случи вече в страни извън ЕС с регулациите за поверителност на данните, които са много сходни с ОРЗД на ЕС.

3.1.6. Пълен текст на NIS 2

Официалният текст може да се намери тук: https://eur-lex.europa.eu/eli/dir/2022/2555.

3.1.7. Структура на NIS 2

NIS 2 започва с преамбюл, в който в 144 точки се обяснява контекстът и се предоставят някои насоки за основната част от директивата. Основната част на NIS 2 има 46 секции, които са структурирани в следните глави:

Глава I —Общи разпоредби
Глава II— Координирани рамки за киберсигурност
Глава III— Сътрудничество на равнището на Съюза и на международно равнище
Глава IV — Мерки за управление на риска за киберсигурността и задължения за докладване
Глава V —Компетентност и регистрация
Глава VI — Обмен на информация
Глава VII — Надзор и правоприлагане
Глава VIII — Делегирани актове и актове за изпълнение
Глава IX — Заключителни разпоредби
Приложение I — Сектори с висока критичност
Приложение II — Други критични сектори
Приложение III — Таблица на съответствието между NIS 2 и NIS

3.1.8. Основни изисквания за киберсигурност на NIS 2

В глава IV на директивата "Мерки за управление на риска за киберсигурността и задължения за докладване" се определя какво трябва да направят съществените и важни

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

субекти, за да спазят NIS 2. Всички останали глави не са от значение за тези субекти, тъй като в тях се посочват задълженията на държавите членки на ЕС и какво трябва да направят правителствените агенции, за да наложат NIS 2.

Глава IV съдържа следните изисквания:

- Член 20 - Управление
- Член 21 - Мерки за управление на риска в областта на киберсигурността
- Член 22 – Координиране на равнището на Съюза оценка на риска за сигурността на критични вериги за доставка
- Член 23 - Задължения за докладване
- Чл.24 - Използване на европейски схеми за сертифициране на киберсигурността
- Чл.25 –Стандартизация

3.1.9. Организации, които трябва да изпълнят изискванията на NIS 2

Директивата за NIS 2 ясно изброява всички сектори и подсектори (отрасли), които трябва да отговарят на изискванията на тази европейска регламентация за киберсигурност. Има, обаче, много изключения от този списък и разликата между съществени и важни субекти не е много лесна за установяване, така че този раздел изяснява кой трябва да бъде съвместим и с какъв статус. Има три общи критерия, които определят кои организации трябва да отговарят на NIS 2:

1) Местоположение – ако предоставят услуги или извършват дейности в която и да е държава в Европейския съюз (независимо дали са базирани в ЕС или не), и
2) Размер – ако са категоризирани като средни или големи организации (виж критериите в раздела по-долу), и
3) Отрасъл – ако работят в някой от 18-те сектора, изброени в таблица 2 по-долу.

3.1.10. Съществени и важни субекти

NIS 2 определя основните субекти, както следва:

- Компании, които са категоризирани като големи предприятия (вижте критериите в следващия раздел) и са в един от 11-те критични сектора (изброени в таблицата по-долу).
- Доставчици на удостоверителни услуги.
- Доставчици на DNS услуги.
- Обществени електронни съобщителни мрежи.
- Органи на държавната власт.
- Всеки критичен субект съгласно Директива (ЕС) 2022/2557 относно устойчивостта на критичните субекти.
- Други субекти, определени от държавите-членки.
- Важни субекти са всички други организации, които не са категоризирани като съществени субекти, но които попадат в обхвата на 3-те критерия, споменати в предишния раздел.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

3.1.11. Разделение по сектори на съществените и важните субекти

Таблицата по-долу показва кои организации трябва да спазват NIS 2 и дали са класифицирани като съществени или важни субекти. За пояснение, ето как ЕС класифицира компаниите според техния размер:

- Микро и малки организации – ако имат по-малко от 50 служители и по-малко от 10 милиона евро годишни приходи.
- Средни организации - ако имат 50 до 250 служители и 10 до 50 милиона евро годишни приходи.
- Големи организации – ако имат повече от 250 служители и повече от 50 милиона евро годишни приходи.

Таблица 2. *Организации, които трябва да спазват NIS 2 и класификация като съществен или важен субект*

Сектор	Подсектор	Вид на обекта	Микро и малки организации*	Средни организации	Големи организации
Сектори с висока критичност					
1. Енергия	а) Електричество	Електроенергийни предприятия, които изпълняват функцията "снабдяване"	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на разпределителни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на преносни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Производители	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Номинирани оператори на пазара на електроенергия Участници на пазара Оператори на зарядна точка	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
	б) Централно отопление и охлаждане	Оператори на районни отоплителни или охладителни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
	в) Масло	Оператори на нефтопреносни тръбопроводи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на съоръжения за производство, рафиниране и третиране на нефт, съхранение и пренос	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Централни структури за поддържане на запаси	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

	г) Газ	Предприятия за доставка	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на разпределителни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на преносни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на системи за съхранение	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на системи за ВПГ	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Предприятия за природен газ	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на съоръжения за рафиниране и третиране на природен газ	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

	д) Водород	Оператори на производство, съхранение и пренос на водород	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
2.Транспорт	а) Въздух	Въздушни превозвачи, използвани за търговски цели	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Органи за управление на летища, летища, включително основните летища, и субекти, опериращи спомагателни инсталации, съдържащи се в летищата	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори по контрол на управлението на движението, предоставящи услуги по контрол на въздушното движение (КВД)	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

	б) Железници	Управители на инфраструктура	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Железопътни предприятия, включително оператори на обслужващи съоръжения	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
	в) Вода	Дружества за вътрешен, морски и крайбрежен пътнически и товарен воден транспорт, без да се включват отделните плавателни съдове, експлоатирани от тези дружества	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Управителни органи на пристанищата, включително техните пристанищни съоръжения, и образувания, които извършват дейности и оборудване, намиращи се в пристанищата	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Оператори на служби по корабния трафик (VTS)	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
	г) Път	Пътни органи, отговарящи за контрола на управлението на движението, с изключение на публични субекти, за които управлението на трафика или експлоатацията на интелигентни транспортни системи е несъществена част от общата им дейност	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Оператори на интелигентни транспортни системи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
3. Банкиране	(Подсектор не е посочен)	Кредитни институции	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
4. Инфраструктури на финансовите пазари	(Подсектор не е посочен)	Оператори на места на търговия	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Централни контрагенти (ЦК)	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
5. Здраве	(Подсектор не е посочен)	Доставчици на здравни услуги	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Референтни лаборатории на ЕС	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Субекти, извършващи научноизследователска и развойна дейност в областта на лекарствените продукти Субекти, произвеждащи основни фармацевтични продукти и фармацевтични препарати Субекти, произвеждащи медицински изделия, считани за критични по време на извънредна ситуация в областта на общественото здраве (списък на критичните устройства за спешни случаи в областта на общественото здраве)	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

6. Питейна вода	(Подсектор не е посочен)	Доставчици и дистрибутори на води, предназначени за консумация от човека, с изключение на дистрибуторите, за които разпределението на вода за консумация от човека е несъществена част от общата им дейност по разпределение на други стоки и стоки	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

7. Отпадъчни води	(Подсектор не е посочен)	Предприятия, които събират, заустват или пречистват градски отпадъчни води, битови отпадъчни води или промишлени отпадъчни води, с изключение на предприятия, за които събирането, заустването или пречистването на градски отпадъчни води, битови отпадъчни води или промишлени отпадъчни води е несъществена част от общата им дейност	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
8. Цифрова инфраструктура	(Подсектор не е посочен)	Доставчици на точки за обмен в интернет	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект

		Доставчици на DNS услуги, с изключение на операторите на root сървъри за имена	Основен субект	Основен субект	Основен субект
		Регистри на имена на TLD	Основен субект	Основен субект	Основен субект
		Услуги по регистрация на имена на домейни	Важен субект	Важен субект	Важен субект
		Доставчици на услуги за изчисления в облак	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Доставчици на услуги за центрове за данни	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Доставчици на мрежи за доставка на съдържание	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
		Доставчици на удостоверителни услуги	Основен субект	Основен субект	Основен субект
		Доставчици на обществени електронни съобщителни мрежи	Важен субект	Основен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Доставчици на обществено достъпни електронни съобщителни услуги	Важен субект	Основен субект	Основен субект
9. ИКТ услуга управление (бизнес-къмбизнес)	(Подсектор не е посочен)	Доставчици на управлявани услуги Доставчици на управлявани услуги за сигурност	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
10. Публична администрация	(Подсектор не е посочен)	Структури на държавната администрация на централни правителства, както са определени от държава членка в съответствие с националното право	Основен субект	Основен субект	Основен субект
		Субекти на държавната администрация на регионално равнище, както са определени от държава членка в съответствие с националното право	Основен субект	Основен субект	Основен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Органи на държавната администрация на местно равнище	(ако член на ЕП Държавата решава)	(ако а Член Държавата решава)	(ако а Член Държавата решава)
11. Пространство	(Подсектор не е посочен)	Оператори на наземна инфраструктура, притежавана, управлявана и експлоатирана от държавите членки или от частни лица, които подпомагат предоставянето на космически услуги, с изключение на доставчиците на обществени електронни съобщителни мрежи	(Не се изисква съответствие с NIS 2)	Важен субект	Основен субект
Други критични сектори					
1. Пощенски и куриерски услуги	(Подсектор не е посочен)	Доставчици на пощенски услуги, включително доставчици на куриерски услуги	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

2. Отпадъци управление	(Подсектор не е посочен)	Предприятия, извършващи управление на отпадъци, с изключение на предприятия, за които управлението на отпадъците не е основната им икономическа дейност	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
3. Производство, производство и Дистрибуция на химикали	(Подсектор не е посочен)	Предприятия, извършващи производството на вещества и разпространението на вещества или смеси, и предприятия, извършващи производството на изделия от вещества или смеси	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект

4. Производство, преработка и Раздаване на храна	(Подсектор не е посочен)	Хранителни предприятия, които се занимават с дистрибуция на едро и промишлено производство и преработка	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
5. Производство	а) Производство на медицински изделия и медицински изделия за инвитро диагностика	Предприятия, произвеждащи медицински изделия и субекти, произвеждащи медицински изделия за инвитро диагностика, с изключение на субектите, произвеждащи медицински изделия	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
	б) Производство на компютърни, електронни и оптични продукти	Предприятия, извършващи някоя от икономическите дейности	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
	в) Производство от електрически оборудване	Предприятия, извършващи някоя от икономическите дейности	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

	г) Производство на машини и оборудване н.в.д.	Предприятия, извършващи някоя от икономическите дейности	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
	д) Производство на автомобили, ремаркета и полуремаркета Ремаркета	Предприятия, извършващи някоя от икономическите дейности	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
	е) Производство от други Транспортно оборудване	Предприятия, извършващи някоя от икономическите дейности	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
6. Дигитални доставчици	(Подсектор не е посочен)	Доставчици на онлайн пазари	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
		Доставчици на онлайн търсачки	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
		Доставчици на платформи за услуги за социални мрежи	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект
7. Изследвания	(Подсектор не е посочен)	Научноизследователски организации	(Не се изисква съответствие с NIS 2)	Важен субект	Важен субект

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

		Образователни институции, по-специално когато извършват критични научноизследователски дейности	(ако член на ЕП Държавата решава)	(ако а Член Държавата решава)	(ако а Член Държавата решава)

*Съгласно член 2, параграф 2 микро и малките организации също трябва да бъдат в съответствие с директива, ако:

б) субектът е единственият доставчик в държава членка на услуга, която е от съществено значение за поддържането на особено важни обществени или икономически дейности;

в) прекъсването на услугата, предоставяна от субекта, би могло да има значително въздействие върху обществената безопасност, обществената сигурност или общественото здраве;

г) прекъсването на услугата, предоставяна от субекта, би могло да породи значителен системен риск, по-специално за секторите, в които това смущение би могло да има трансгранично въздействие;

д) субектът е от решаващо значение поради специфичното си значение на национално или регионално равнище за конкретния сектор или вид услуга или за други взаимозависими сектори в държавата членка;"

Ако държава членка е определила този субект като "критичен субект" съгласно Директива (ЕС) 2022/2557 относно устойчивостта на критичните субекти.

3.1.12. Съществени и важни субекти в NIS 2

Ето най-важните разлики в начина, по който NIS 2 третира съществени и важни субекти:

В член 32 се определят по-строги мерки за надзор и правоприлагане за съществени субекти от посочените в член 33 важни субекти.

В член 32 също така се посочва, че висшето ръководство на основни субекти може да бъде подведено под отговорност за нарушаване на техните задължения, за да се гарантира спазването на МИС 2. Това изискване не съществува за важни субекти.

В член 34 се определят по-високи глоби за съществени и важни субекти, като информация за това може да намерите в точка 3.5.8 Глоби и отговорност .

Тук е мястото да отбележим, че държавната администрация е посочена като съществен субект.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

3.2. Състояние на страните членки за съответствие на NIS 2

Тази част от изследването е тясно свързано с Директивата на Европейския съюз за мрежова и информационна сигурност 2 (МИС/NIS 2/Директивата), и представя основните факти и насоки за тази нова директива. Частта от изследването обхваща следните теми:

Транспонирането е процесът, който всяка държава-членка на ЕС приема, за да постигне целите и изискванията на дадена директива на ЕС и да приведе националното законодателство в съответствие със законодателството на ЕС.

Среща се и т.нар. и регулаторен арбитраж (практика, прилагана от организациите, с цел да се потърси "вратичка" в даден нормативен акт или да се насочи дейността към юрисдикция с по-лек регулаторен режим). Поради това съществуват различия и несъответствия в прилагането на европейското законодателството в държавите-членки на ЕС, както и важни регулаторни различия.

Всички страни от ЕС трябва да транспонират директивите в националното си законодателство. Някои държави се придържат към по-стриктно прилагане (и увеличават разходите за осигуряване на спазването на регулаторните изисквания), а други други държави са по- по-малко стриктни при прилагането на задължителните регулации (и минимизират разходите за спазване).

Международните компании често правят „регулаторно пазаруване" и установяват присъствието си в ЕС в страни, където спазването на изискванията е по-евтино. Това може да доведе до конкурентно неизгодно положение за страните, които прилагат по-правилно регулациите, което коства повече разходи.

Държавите, които правят по-малко и дори не изпълняват целите на дадена директива, могат да имат предимства и да предложат по-висока възвръщаемост на собствения капитал за компаниите, само защото цената за спазване е по-ниска. Тези практики не следва да бъдат толерирани по никакъв начин, тъй като повишеното въздействие и вероятността от кибер-рискове, особено на фона на продължаваща война между Русия и Украйна, не може да оправдае по никакъв план регулаторен арбитраж.

Изискването на директивата е представено в член 41: „ *До 17 октомври 2024 г. държавите членки приемат и публикуват необходимите мерки, за да се съобразят с настоящата директива. Те незабавно информират Комисията за това. Те прилагат тези мерки от 18 октомври 2024 г.*

Когато държавите-членки приемат мерките, посочени в параграф 1, те съдържат позоваване на настоящата директива или са придружени от такова позоваване при официалното им публикуване. Методите за такова позоваване се определят от държавите-членки."

За целите на проучването е направен преглед за състоянието на транспонирането на Директивата NIS 2 във всяка държава от ЕС, въз основа на информация, предоставена от всяка държава членка[32]. Това са резултатите, актуални към 10 февруари 2024 г.:

[32] https://www.nis-2-directive.com/NIS_2_Directive_Transposition.html

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

Таблица 3. *Състоянието на транспонирането на Директивата NIS 2*

Австрия	Директивата NIS 2 не е транспонирана в националното законодателство
Белгия	Директивата NIS 2 не е транспонирана в националното законодателство
България	Директивата NIS 2 не е транспонирана в националното законодателство
Хърватия	Директивата NIS 2 не е транспонирана в националното законодателство
Кипър	Директивата NIS 2 не е транспонирана в националното законодателство
Чешка Република	Директивата NIS 2 не е транспонирана в националното законодателство
Дания	Директивата NIS 2 не е транспонирана в националното законодателство
Естония	Директивата NIS 2 не е транспонирана в националното законодателство
Финландия	Директивата NIS 2 не е транспонирана в националното законодателство
Франция	Директивата NIS 2 не е транспонирана в националното законодателство
Германия	Директивата NIS 2 не е транспонирана в националното законодателство
Гърция	Директивата NIS 2 не е транспонирана в националното законодателство
Унгария	Директивата NIS 2 не е транспонирана в националното законодателство

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Ирландия	Директивата NIS 2 не е транспонирана в националното законодателство
Италия	Директивата NIS 2 не е транспонирана в националното законодателство
Латвия	Директивата NIS 2 не е транспонирана в националното законодателство
Литва	Директивата NIS 2 не е транспонирана в националното законодателство
Люксембург	Директивата NIS 2 не е транспонирана в националното законодателство
Малта	Директивата NIS 2 не е транспонирана в националното законодателство
Холандия	Директивата NIS 2 не е транспонирана в националното законодателство
Полша	Директивата NIS 2 не е транспонирана в националното законодателство
Португалия	Директивата NIS 2 не е транспонирана в националното законодателство
Румъния	Директивата NIS 2 не е транспонирана в националното законодателство
Словакия	Директивата NIS 2 не е транспонирана в националното законодателство
Словения	Директивата NIS 2 не е транспонирана в националното законодателство
Испания	Директивата NIS 2 не е транспонирана в националното законодателство
Швеция	Директивата NIS 2 не е транспонирана в националното законодателство

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

3.3. Връзка на NIS 2 с други актове за мрежова и информационна сигурност

3.3.1. Връзка на NIS 2 с ISO 27001

NIS 2 не изисква внедряване на ISO 27001. Въпреки това, Директивата реферира към серията ISO/IEC 27000 в преамбюла си като начин за прилагане на мерки за управление на риска за киберсигурността, а основната част от NIS 2 насърчава използването на международни стандарти.

При по-тясно сравняване на NIS 2 с ISO 27001 става ясно, че ISO 27001 предоставя подходяща рамка за спазване на мерките за управление на риска за киберсигурността, изисквани от NIS 2. ISO 27001 предоставя ясно ръководство за това как да се дефинира процесът на управление на риска, как да се комбинира техническото изпълнение с обучение и други въпроси, свързани с човешките ресурси, как да се включи висшето ръководство и т.н.

3.3.2. Разлика между NIS 2 и EU GDPR/ОРЗД

Пълното заглавие на EU GDPR е "Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните)". Въпреки че и NIS 2, и GDPR се фокусират върху защитата на данните, те са доста различни:

Таблица 4. *Разлика между NIS 2 и EU GDPR/ОРЗД*	МИС 2	ЕС ОРЗД
Вид	Директива (организациите спазват местното законодателство, а)	Регламент (пряко приложим за дружествата)
Отнася се за	Организации, които се считат за съществени и важни субекти	Всяка организация, която обработва лични данни
Закрила	Мерките за киберсигурност се прилага за всички данни в рамките на компанията	Мерките за киберсигурност се прилагат само за лични данни; съществува и правен аспект на защитата на лични данни

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Приложимост от от	октомври 18, 2024	25 май 2018

3.3.3. Разлика между NIS 2 и DORA

Пълното заглавие на DORA е "Регламент (ЕС) 2022/2554 относно цифровата оперативна устойчивост на финансовия сектор". Въпреки че NIS 2 и DORA са публикувани в един и същи ден (27 декември 2022 г.), има съществени разлики между тях:

Таблица 5. *Разлика между NIS 2 и DORA*

	МИС 2	ДОРА
Вид	Директива (компаниите спазват местното законодателство, което се публикува)	Регламент (пряко приложим за финансовите институции)
Отнася се за	Организации, които се считат за съществени и важни субекти	Финансови институции
Закрила	Акцент върху мерките за киберсигурност	Освен мерките за киберсигурност, акцентът е и върху цялостната устойчивост
Ефективен от	октомври 18, 2024	януари 17, 2025

3.3.4. Разлика между NIS 2 и Директивата за устойчивост на критичните субекти (CER)

Пълното заглавие на CER е "Директива (ЕС) 2022/2557 относно устойчивостта на критичните субекти". Въпреки че NIS 2 и CER са публикувани в един и същи ден (27 декември 2022 г.), те имат различен фокус:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Таблица 6. *Разлика между NIS 2 и Директивата за устойчивост на критичните субекти (CER)*

	МИС 2	CER
Вид	Директива (компаниите спазват местното законодателство, което се публикува)	Директива (компаниите спазват местното законодателство, което се публикува)
Отнася се за	Организации, които се считат за съществени и важни субекти	Организации, които се считат за критични съгласно решението на държавата-членка
Закрила	Акцент върху мерките за киберсигурност	Акцент върху устойчивостта и непрекъснатостта на бизнеса
Ефективен от	октомври 18, 2024	18 октомври 2024 г.; Въпреки това, критичните субекти трябва да станат съвместими в рамките на 10 месеца от деня, в който са определени като критични

МИС 2, CER Директивите и Регламентът DORA следва да се имплементират по начин, въвеждащ съгласуван подход за осигуряване на критичните инфраструктури на държавите-членки на ЕС и в нашата страна. При отчитане на обхвата на трите нормативни акта, и трите засягат в различна степен органите на държавната администрация на Република България.

3.4 Очаквани действия, ефект, рискове и срокове за транспониране на NIS 2

Направен е анализ кои държавни органи са определени в NIS 2. Ето какво определя NIS 2:

- Държавите членки трябва да публикуват свои собствени закони и разпоредби за киберсигурност въз основа на NIS 2.
- Компетентните органи са определени от държавите членки да упражняват надзор върху съществените и важни субекти, които трябва да спазват NIS 2 и местното законодателство в областта на киберсигурността.
- Държавите членки създават „единни звена за контакт", за да се даде възможност за трансгранично сътрудничество между органите.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- "Органи за управление на киберкризи" са компетентни органи, определени от държавите членки, които отговарят за управлението на мащабни инциденти и кризи в областта на киберсигурността.
- „Екипите за реагиране при инциденти с компютърната сигурност“ (CSIRT) се определят от държавите-членки, за да се справят с инциденти в съответствие с определени процеси.
- „Европейската мрежа от организации за връзка при киберкризи“ (EU-CyCLONe) подпомага координираното управление на широкомащабни инциденти и кризи в областта на киберсигурността.
- „Групата за сътрудничество“ улеснява стратегическото сътрудничество и обмена на информация между държавите членки.
- Агенцията на Европейския съюз за киберсигурност (ENISA) създава база данни за уязвимости, изготвя двугодишен доклад за състоянието на киберсигурността в Съюза, поддържа регистър на субектите със специален статут, изготвя насоки относно техническите области и съществуващите стандарти и др.

3.4.1. Транспониране на NIS2

Държавите членки на ЕС трябва да публикуват местните закони и разпоредби, свързани с Директивата за NIS 2, до 17 октомври 2024 г. Към датата на анализа нито една от държавите членки не е транспонирала NIS 2.

3.4.2 Сертифициране по NIS 2

NIS 2 не изисква съществените и важни субекти да бъдат сертифицирани.

Държавите членки (или Комисията на ЕС) обаче могат да изискват от тези субекти да използват конкретни ИТ продукти или услуги, които са сертифицирани в съответствие с европейската схема за сертифициране на киберсигурността съгласно Закона за киберсигурността (Регламент (ЕС) 2019/881).

3.5. Основни изисквания на NIS 2 и подход за изпълнение несъответствието

От 46 члена в Директивата за NIS 2 само членове 20—25 са от значение за организациите (т.е. съществени и важни субекти), които трябва да бъдат приведени в съответствие с NIS 2; Повечето от другите разпоредби уточняват изискванията към държавните органи, които регулират киберсигурността.

Тези най-важни изисквания са поставени в глава IV и гравитират около две основни теми: управление на риска за киберсигурността и задължения за докладване. Освен глава IV, има само няколко изисквания, свързани със съществени и важни субекти.

Ето и най-важните изисквания на NIS 2, с които трябва да сте наясно:

3.5.1. Отговорности на висшето ръководство

Съгласно член 20 висшето ръководство на съществени и важни субекти:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- трябва да одобри мерките за киберсигурност, които трябва да бъдат приложени в организацията,
- трябва да контролира тяхното изпълнение
- може да бъде подведено под отговорност, ако киберсигурността не се прилага правилно.

Член 32 допълнително подчертава отговорността на законните представители на съществени субекти.

3.5.2. Значение на обучението

Съгласно член 20 членовете на висшето ръководство трябва да преминат през обучение по киберсигурност и трябва да дадат възможност на служителите си да посещават редовно такова обучение.

NIS 2 изисква обучение, което да обхване идентифицирането на рисковете, оценката на практиките за киберсигурност и как тези мерки за киберсигурност помагат на компанията да предоставя услугите си.

3.5.3 Основан на риска подход към киберсигурността

Член 21 изисква мерките за киберсигурност да бъдат подходящи за свързаните с тях рискове; при оценката на рисковете NIS 2 изисква от дружествата да вземат предвид следното:

- Излагане на рискове
- Размер на организацията
- Вероятност от възникване на инциденти и тяхната сериозност
- Социални и икономически последици от инциденти

3.5.4 Киберсигурността като комплекс от технически, оперативни и организационни мерки

Член 21 изисква от дружествата да "*предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи, които тези субекти използват при своите операции или при предоставяне на своите услуги, както и за предотвратяване или свеждане до минимум на въздействието на инцидентите върху получателите на услугите им и върху други услуги*"

Освен това член 21 изисква подход на всички опасности, което основно означава, че организациите трябва да се подготвят за широк спектър от потенциални заплахи.

В член 21 се определят и редица документи и мерки за киберсигурност, които са изброени по-долу.

3.5.5. Сигурност на веригата на доставки

В член 21 от дружествата се изисква да обръщат специално внимание на рисковете, свързани с преките доставчици и доставчиците на услуги, и по-специално:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

- Уязвимости, специфични за всеки директен доставчик и доставчик на услуги
- Цялостното качество на продуктите и практиките за киберсигурност на доставчиците и доставчиците на услуги
- Сигурни процедури за развитие на доставчиците и доставчиците на услуги

3.5.6. Докладване на значими инциденти

Член 23 изисква от субектите да докладват за всички значителни инциденти на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и на потребителите на техните услуги.

3.5.7. Използване на сертифицирани ИТ продукти и услуги

NIS 2 не изисква съществените и важни субекти да бъдат сертифицирани. Директивата за NIS 2, обаче позволява на държавите от ЕС (държавите членки) или на Комисията на ЕС да изискват от тези субекти да използват ИТ продукти или услуги, които са сертифицирани. Към момента няма изисквания за използване на сертифицирани ИТ продукти или услуги, но има потенциална възможност това да стане задължително.

Тези ИТ продукти и услуги ще трябва да бъдат сертифицирани в съответствие с европейската схема за сертифициране на киберсигурността.

3.5.8. Глоби и отговорност

За компании, които не отговарят на изискванията на NIS 2, глобите са следните:

- За съществени субекти – до 10 милиона евро или 2% от общия годишен оборот.
- За важни субекти – до 7 милиона евро или 1,4% от общия годишен оборот.

Важно е да се отбележи, че член 20 изисква висшето ръководство на съществени и важни субекти да одобрява мерките за управление на риска за киберсигурността и да наблюдава тяхното изпълнение, и в него се посочва, че висшето ръководство може да бъде подведено под отговорност, ако киберсигурността не е в съответствие с член 21.

Има предвидени и непарични санкции :

- предупреждения при нарушение на настоящата директива от засегнатите субекти;
- обвързващи указания или разпореждане, с които се изисква от засегнатите субекти да поправят установените пропуски или нарушението на настоящата директива;
- да разпореждат на засегнатите субекти да преустановяват поведение, което нарушава настоящата директива, и да се въздържат от повтарянето на такова поведение и др.

3.6. Документи за съответствие с директивата NIS 2

Административните структури трябва да спазва директивата NIS 2, поради което трябва да генерират определен брой документи, за да се покрият изискванията за

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

киберсигурност и докладване. Този раздел представя всички документи, които организациите трябва да напишат съгласно NIS 2 Глава IV "Мерки за управление на риска за киберсигурността и задължения за докладване". Причината, поради която акцентът е само върху тази глава, е че тя е единствената, която уточнява какво трябва да направят съществените и важни субекти, за да спазват настоящата директива.

3.6.1. Списък на необходимите документи и записи

Таблицата по-долу показва изискванията за NIS 2, съответните членове от глава IV от настоящата директива и най-добрата практика за документиране на тези изисквания.

Таблица 7. *Списък на необходимите документи и записи съобразно изискванията на NIS 2*

Какво трябва да се документира	NIS 2 изискване	Генериран документ
Управителните органи трябва да одобрят мерките за управление на риска за киберсигурността	Член 20, параграф 1	План за третиране на риска
Управителните органи трябва да упражняват надзор върху прилагане на мерки за управление на риска за киберсигурността	Член 20, параграф 1	Отчет за мониторинг + доклад от вътрешен одит + Протокол за преглед на ръководството
От членовете на управителните органи се изисква да преминат обучение и трябва редовно да предлагат подобно обучение на своите служители	Член 20, параграф 2	План за обучение и осведоменост Доказателства за обучение
Субектите трябва да предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете	Член 21, параграф 1	Методика, оценка и план за третиране на риска Регламенти за внедряване на организационни и технологични решения

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

При оценката на пропорционалността на мерките надлежно се вземат предвид степента на излагане на риска на субекта, размерът на субекта и вероятността от възникване на инциденти и тяхната тежест, включително тяхното обществено и икономическо въздействие	Член 21, параграф 1	Методология за оценка на риска, резултати от оценка на риска
Политика за анализ на риска	Член 21, параграф 2, буква а)	Методология за оценка на риска
Политика за мрежова и информационна сигурност	Член 21, параграф 2, буква а)	Политика за мрежова и информационна сигурност
Обработка на инциденти	Член 21, параграф 2, буква б)	Процедура за управление на инциденти Регистър на инциденти
Непрекъснатост на бизнеса	Член 21, параграф 2, буква в)	План за непрекъснатост на бизнеса
Управление на архивирането	Член 21, параграф 2, буква в)	Политика (схема) за архивиране
Възстановяване след бедствие	Член 21, параграф 2, буква в)	План за възстановяване при бедствия
Управление на кризи	Член 21, параграф 2, буква в)	План за управление на кризи

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Сигурност на веригата на доставки, включително аспекти, свързани със сигурността, свързани с взаимоотношенията между всеки субект и неговите преки доставчици или доставчици на услуги	Член 21, параграф 2, буква г)	Политика за сигурност на доставчика Декларация за поверителност
Сигурност при придобиване, разработване и поддръжка на мрежи и информационни системи	Член 21, параграф 2, буква д)	Политика за сигурност при разработване и поддържане на мрежи и информационни системи Спецификация на изискванията към информационната система
Политики и процедури за оценка на ефективността на мерките за управление на риска за киберсигурността	Член 21, параграф 2, буква е)	Методология на мониторинг Резултати от мониторинг Вътрешен одит Преглед от топ мениджмънта
Основни практики за киберхигиена	Член 21, параграф 2, буква ж)	Политика за ИТ сигурност
Обучение по киберсигурност	Член 21, параграф 2, буква ж)	План за обучение и осведоменост Доказателства за обучение
Политики и процедури относно използването на криптография и криптиране	Член 21, параграф 2, буква з)	Политика за използване на криптиране
Сигурност на човешките ресурси	Член 21, параграф 2, буква и)	Политика за сигурност на човешките ресурси

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Политики за контрол на достъпа	Член 21, параграф 2, буква и)	Политика за контрол на достъпа
Управление на активи	Член 21, параграф 2, буква и)	Процедура за управление на активи Инвентаризация на активите
Използване на решения за многофакторно удостоверяване или непрекъснато удостоверяване	Член 21, параграф 2, буква й)	Политика за удостоверяване
Защитени гласови, видео и текстови комуникации	Член 21, параграф 2, буква й)	Политика за трансфер на информация Политика за сигурна комуникация
Защитени системи за аварийна комуникация в рамките на предприятието	Член 21, параграф 2, буква й)	Политика за сигурна комуникация
Да се вземат предвид уязвимостите, специфични за всеки пряк доставчик на доставчици и услуги, и цялостното качество на продуктите и практиките в областта на киберсигурността на техните доставчици и доставчици на услуги, включително техните сигурни процедури за разработване	член 21, параграф 3	Политика за сигурност на доставчика Управление на риска Доклад за оценка и третиране на рискове
Предприемане на подходящи и пропорционални коригиращи мерки	член 21, параграф 4	Процедура за коригиращи действия Записи за управление на коригиращи действия
Уведомяване на ЕРИКС или компетентния орган за значителен инцидент	Член 23, параграф 1	Процедура за уведомяване за значителен инцидент за CSIRT/компетентен орган

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Уведомяване на получателите на услугите за значителни инциденти, които има вероятност да се отразят неблагоприятно на предоставянето на тези услуги	Член 23, параграф 1	Процедура за уведомяване за значителен инцидент за получатели на услуги
Съобщаване на получателите на услуги, които са потенциално засегнати от значителна киберзаплаха, всички мерки или средства за правна защита, които тези получатели са в състояние да предприемат в отговор на тази заплаха; също така да информират тези получатели за самата значителна киберзаплаха;	Член 23, параграф 2	Процедура за уведомяване за значителен инцидент за получатели на услуги
Ранно предупреждение, което показва дали се подозира, че значимият инцидент е причинен от незаконни или злонамерени действия или би могъл да има трансгранично въздействие	Член 23, параграф 4, буква а)	Процедура за ранно предупреждение за значителен инцидент
Уведомление за инцидент, в което се посочва първоначална оценка на значимия инцидент, включително неговата тежест и въздействие, както и, когато са налични, показателите за компромис	Член 23, параграф 4, буква б)	Процедура за уведомяване за значителен инцидент за CSIRT/компетентен орган
Междинен отчет за съответните актуализации на състоянието	Член 23, параграф 4, буква в)	Доклад за значителен инцидент
Окончателен доклад не по-късно от един месец след подаване на уведомлението за инцидента	Член 23, параграф 4, буква г)	Доклад за значителен инцидент

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Доклад за напредъка — в случай на продължаващ инцидент към момента на представяне на окончателния доклад	Член 23, параграф 4, буква д)	Доклад за напредъка при значителни инциденти

3.6.2. Общоприложими документи за киберсигурност, които не се изискват от NIS 2

Освен необходимите документи, изброени по-горе, се препоръчва да се разработят и следните документи:

- Политика за класификация на информацията – предоставя ясни правила за това как да се класифицират документи и друга информация и как да се защитят тези активи според нивото на класификация.
- Политика за мобилни устройства, работа от разстояние и работа от дома – определя правилата за използване на лаптопи, смартфони и други устройства извън помещенията на компанията.
- Правила за носене на собствено устройство (BYOD) – указва аспекти на сигурността, ако служителите използват личните си устройства за работа.
- Политика за обезвреждане и унищожаване – определя как да се изхвърлят устройства и носители, за да се изтрият всички чувствителни данни и да се избегне нарушаването на правата върху интелектуалната собственост.
- Процедури за работа в защитени зони – дефинира правила за сигурност за центрове за данни, архиви и други зони, които се нуждаят от специална защита.
- Политика за управление на промените – дефинира правила за това как да се извършват промени в производствените системи, за да се намалят рисковете за сигурността.
- Clear Desk и Clear Screen Policy – определя правила за всеки служител за това как да защити своето работно пространство.
- Процедури за сигурност за ИТ отдела – осигурява оперативни процедури за сигурност за дейности, които не са обхванати в други документи.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ГЛАВА 4. Примерен модел за адаптиране на държавната администрация в контекста на внедряване на новите изисквания по мрежова и информационна сигурност

4.1.Подход за прилагане на мерки за управление на риска за киберсигурността

Спазването на сложни разпоредби, като тези, съдържащи се в Директивата NIS 2 никога не е лесно, но наличието на ясен план как да се направи това, улеснява процеса. По-долу е посочено предложение за най-добрите практики по отношение на стъпките, които следва да се спазват, с цел постигане на пълно пълно съответствие с NIS 2, глава IV "Мерки за управление на риска за киберсигурността и задължения за докладване". Стъпките се фокусират върху тази глава, тъй като тя представя ключови изисквания за NIS 2, с които организациите (т.е. съществени и важни субекти) трябва да спазват.

4.1.1. Получаване на подкрепа от висшето ръководство

Вероятен е изводът, че задължителният характер на NIS 2 ще доведе до автоматичното и гладко осъществяване на процеса по изпълнение на тази директива със или без ангажимент от страна на висшето ръководство. За съжаление, реалността е различна - ако висшето ръководство не подкрепи активно такъв проект, той ще бъде бавен, недофинансиран и блокиран на всяка възможна стъпка.

Така че, въпреки че NIS 2 е задължителна, от ключова важност е нейното припознаване като висок приоритет за изпълнение от страна на ръководството на организацията.

4.1.2. Създаване на управление на проекти

NIS 2 е сложна за въвеждане, за да се възложи само на ИТ администратор, надявайки се, че всичко ще се оправи. На първо място, не може да се очаква някой без формална власт да успее с такъв голям проект и второ – трябва да има ясна представа за стъпките за изпълнение, етапите, основните резултати, отговорностите и т.н. С други думи, проектният подход е необходима предпоставка за успех.

4.1.3. Извършване на първоначално обучение

NIS 2 поставя акцент върху провеждането на обучение по сигурност и трябва да се извърши първоначално обучение на много ранна фаза от въвеждането на директивата. По този начин всички участници ще имат добра представа за това какво е NIS 2, какво трябва да се направи, защо е необходимо и т.н.

4.1.4. Създаване политика на най-високо ниво за сигурност на мрежовата и информационна сигурност

Въпреки че NIS 2 не изисква конкретно документ от най-високо стратегическо ниво в организацията, който да определи посоката на киберсигурността, такъв документ е най-

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

добрата практика според международните стандарти поради следния факт: ако не знаете къде отивате, вероятно ще се изгубите. Затова е необходим такъв документ от най-високо ниво – той ясно да показва какво трябва да се постигне с киберсигурността, какви са основните роли и отговорности и как ще се измерва успехът.

4.1.5. Определяне на методологията за управление на риска

Управлението на риска обикновено е най-сложната стъпка в процеса на съответствие и освен това NIS 2 има някои специфични изисквания за това как трябва да се извършва управлението на риска.

За да е сигурно, че организацията е в съответствие с NIS 2 и за да е сигурно, че всички в тази организация разбират как трябва да се управляват рисковете, трябва да се създаде документ/методология, който определя ясни правила за управление на риска.

4.1.6. Извършване на оценка на риска и третиране на рисковете

По време на оценката на риска трябва да се установи какво би могло да застраши информационните системи – това обикновено се прави чрез изброяване на активи и свързаните с тях заплахи и уязвимости. Освен това трябва да се разбере колко големи са тези рискове, като се оценят вероятността и тежестта (въздействието).

След като е готов списъкът с рискове, трябва да се разбере как да се третират (т.е. да се смекчат) най-високите рискове – за повечето от тях ще се приложат мерките за киберсигурност, определени в член 21. По този начин има киберсигурност, която се основава на задълбочен анализ, а не на хаотично прилагане на различни мерки.

4.1.7. Създаване и одобряване на план за третиране на риска

След като има пълна представа какви са рисковете и какво би било тяхното въздействие, следва да се да създаде конкретен план за това как да се приложат мерки за киберсигурност – и, което е още по-важно, да се получи одобрението на висшето ръководство за такъв план.

Планът за третиране на риска всъщност е план за изпълнение и обикновено включва списък на всички мерки за киберсигурност (т.е. дейности, процеси и технологии), които трябва да бъдат изпълнени, заедно с информация за това кой е отговорен, какви са сроковете и т.н.

4.1.8. Прилагане на мерки за киберсигурност

Разбира се, ключовото изискване на NIS 2 е да се прилагат различни мерки (контроли) за киберсигурност. На практика това означава, че ще трябва да се въведат нови процеси за сигурност, дейности и в някои случаи нови технологии, всички въз основа на резултатите от оценката на риска. Във всеки случай ще трябва да се изготвят различни политики и процедури за киберсигурност, за да определят ясни правила за тези нови процеси, дейности и технологии. В раздела по-долу са посочени необходимите документи, визиращи необходимите мерки за киберсигурност.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

4.1.9. Създаване на сигурност на веригата за доставки

NIS 2 установява, че все по-голям брой инциденти, свързани със сигурността, са свързани с нарушения с доставчиците – това изисква да се обърне по-голямо внимание на взаимоотношенията с доставчиците на услуги, което включва оценка на техните уязвимости и проучване на техните процедури за разработка на софтуер.

Това става чрез официална оценка на риска на доставчиците, като се избират само надеждни доставчици, с които да се работи, включително клаузи за сигурност в споразумения с тях, и се следи тяхната позиция по отношение на сигурността.

4.1.10. Създаване на оценка на ефективността на киберсигурността

NIS 2 изисква висшето ръководство да наблюдава прилагането на мерките за киберсигурност – най-добрата практика е това да става по три начина:

(1) чрез непрекъснато измерване и наблюдение на киберсигурността, за да може да се забележат всякакви отклонения,

(2) чрез въвеждане на периодични вътрешни одити за откриване на несъответствия и

(3) чрез въвеждане на периодичен преглед от ръководството, за да има официална сесия за преглед на всички факти, свързани с киберсигурността.

За да се регулират тези дейности, се изисква създаване на няколко ключови документа: Методология на измерване, Процедура за вътрешен одит и Процедура за преглед на управлението.

4.1.11. Докладване на инциденти

Едно от ключовите изисквания за NIS 2 е уведомяването на CSIRT (или компетентния орган) и получателите на услуги за значителни инциденти. Субектите трябва да представят няколко вида доклади на CSIRT: ранно предупреждение, уведомление за инцидент, междинен доклад, окончателен доклад и доклад за напредъка.

4.1.12. Подход за непрекъснато обучение по киберсигурност

NIS 2 е много специфична по отношение на за създаването на капацитет за киберсигурност сред всички служители, включително висшето държавни служители. Предизвикателството тук е как да се изберат правилните теми и каква форма на обучение да бъде избрана, за да се получи правилният трансфер на знания, без да влагат твърде много време или пари.

4.1.13. Провеждане на периодичен вътрешен одит

Вярно е, че вътрешният одит не е споменат в NIS 2; ISO 27001 и други международни стандарти, обаче предлагат вътрешния одит, като най-добрата практика за висшето ръководство, за да може да наблюдава прилагането на мерките за киберсигурност.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Без да идентифицира несъответствията по време на вътрешния одит, висшето ръководство никога няма да има пълна картина за състоянието на киберсигурността, което може да доведе до инциденти и отговорност.

4.1.14. Периодичен преглед на управлението

Прегледът от ръководството е официална среща, на която висшето ръководство трябва да получи цялата съответна информация относно киберсигурността (напр. Доклад за измерване, доклад за вътрешен одит и т.н.), за да вземе ключови решения относно киберсигурността.

По време на прегледа от ръководството висшето ръководство може да повиши коригиращите действия, да промени ключови роли и отговорности, да определи нови цели в областта на сигурността, да определи бюджета за сигурност и т.н.

4.1.15. Коригиращи действия

Коригиращите действия са систематичен начин за отстраняване на несъответствията – по време на тяхното изпълнение формално се анализира причината за несъответствието и се определят и изпълняват дейностите по отстраняване на тази причина.

С други думи, целта на коригиращите действия е да се гарантира, че подобни несъответствия няма да се случат отново.

4.2. Оценка на риска за сигурността на критични вериги за доставка

Директивата за NIS 2 изисква да се оценяват рисковете за сигурността на критичните вериги за доставка. Налични са много международни стандарти, които дават насоки за управление на рисковете при взаимоотношения с доставчиците. По-долу предлагаме добри практики от международния стандарт ISO/IEC 27002:2022, които се отнасят до всяка структура от държавната администрация.

Всяка структура от публичната информация може да идентифицира и внедри процеси и процедури за справяне с рисковете за сигурността, свързани с използването на продукти и услуги, предоставяни от доставчици. Това трябвало да се отнася и за използваните от структурата ресурси на доставчиците на облачни услуги. Процесите и процедурите трябвало да включват както тези, които трябва да бъдат внедрени от организацията, така и тези, които организацията изисква да се внедрят от доставчика, за да започне използването на продукти или услуги на доставчика или за прекратяване на използването на продукти и услуги на доставчика, като например:

4.2.1 идентифициране и документиране на видовете доставчици (например на ИКТ услуги, логистика, комунални услуги, финансови услуги, компоненти на ИКТ инфраструктура), които могат да окажат влияние върху конфиденциалността, интегритета и наличността на информацията на организацията;

4.2.2. определяне на това как да се оценяват и избират доставчиците в зависимост от чувствителността на информацията, продуктите и услугите (например чрез пазарен анализ, препоръки от клиенти, преглед на документи, оценявания на място, сертифициране);

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

4.2.3. оценяване и подбор на продукти или услуги на доставчика, които имат подходящи механизми за контрол за сигурността на информацията и преглеждането им; по-специално, точността и пълнотата на механизмите за контрол, въведени от доставчика, които осигуряват интегритета на информацията и на обработването на информацията от доставчика и следователно сигурността на информацията на организацията;

4.2.4. определяне на информацията на организацията, ИКТ услугите и физическата инфраструктура, до които доставчиците могат да имат достъп, да извършват мониторинг, да контролират или да използват;

4.2.5. определяне на видовете компоненти и услуги на ИКТ инфраструктурата, предоставяни от доставчици, които могат да засегнат конфиденциалността, интегритета и наличността на информацията на организацията;

4.2.6. оценяване и управление на рисковете за сигурността на информацията, свързани с:

1. използването от доставчиците на информацията и другите свързани активи на организацията, включително рисковете, произтичащи от потенциално злонамерен персонал на доставчика;
2. неправилно функциониране или уязвимости на продуктите (включително софтуерни компоненти и подкомпоненти, използвани в тези продукти) или услугите, предоставяни от доставчиците;

4.2.7. следене на съответствието с установените изисквания за сигурност на информацията за всеки тип доставчик и тип достъп, включително преглед от трета страна и валидиране на продукта;

4.2.8. смекчаване на несъответствието на доставчика, независимо дали то е било открито чрез мониторинг или по друг начин;

4.2.9. обработване на инциденти и непредвидени ситуации, свързани с продукти и услуги на доставчиците, включително отговорностите на организацията, така и на доставчиците;

4.2.10. еластичност и ако е необходимо мерки за възстановяване при извънредни ситуации, за да се осигури наличността и обработването на информацията на доставчика, а следователно и наличността на информацията на организацията;

4.2.11. осведоменост и практически упражнения на персонала на организацията, който взаимодейства с персонала на доставчиците по отношение на съответните правила за включване, специфични политики, процеси, процедури и поведение, базирани на типа на доставчика и нивото на достъп на доставчика до системите и информацията на организацията;

4.2.12. управление на необходимия пренос на информация, на другите свързани активи и на всичко друго, което трябва да бъде променяно, и гарантиране, че сигурността на информацията се поддържа през целия период на пренос;

4.2.13. изисквания за осигуряване на безопасно прекратяване на взаимоотношенията с доставчика, включително:

1. отнемане на правата за достъп;
2. обработване на информацията;

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

3. определяне на притежанието върху интелектуалната собственост, разработена по време на ангажимента;
4. преносимост на информацията в случай на смяна на доставчик или поемане на дейностите от самата организация;
5. управление на записите;
6. връщане на активи;
7. сигурно унищожаване на информация и други свързани активи;
8. текущи изисквания за конфиденциалност;

4.2.14. нивото на сигурност на персонала и физическата сигурност, очаквани от персонала и съоръженията на доставчика.

Информацията може да бъде изложена на риск от доставчици с неподходящо управление на сигурността на информацията. Трябва да се определят и прилагат механизми за контрол за управление на достъпа на доставчика до информацията и другите свързани активи. Например, ако има специална нужда от конфиденциалност на информацията, може да се ползват споразумения за неразкриване на информация или криптографски техники. Друг пример са рисковете за защита на личните данни, когато споразумението с доставчика включва трансграничен пренос или достъп до информация. Организацията трябва да е наясно, че законовата или договорната отговорност за защита на информацията си остава на организацията.

Освен това, рисковете могат да бъдат причинени и от неподходящи механизми за контрол на компонентите на ИКТ инфраструктурата или услугите, предоставяни от доставчиците. Неправилно функциониращи или уязвими компоненти или услуги могат да причинят пробиви в сигурността на информацията в организацията или на друг субект (например те могат да причинят заразяване със злонамерен софтуер, атаки или други вреди на организации, различни от организацията).

4.3 От киберсигурност към киберустойчивост. Докладване на инциденти

Директивата за NIS 2 определя само задълженията за докладване в член 23, но този член е доста дълъг и доста взискателен. Кои инциденти трябва да се докладват, на кого и как трябва да се докладва?

4.3.1. Значим инцидент

Според NIS 2 инцидент означава събитие, компрометиращо наличността, автентичността, целостта или поверителността на съхранявани, предавани или обработвани данни или на услугите, предлагани от или достъпни чрез мрежови и информационни системи.

NIS 2 изисква докладването само на значими инциденти – определя значим инцидент като “всеки инцидент, който има значително въздействие върху предоставянето” на услугите, които съществени и важни субекти предоставят, ако:

а) е причинил или е в състояние да причини сериозни смущения в експлоатацията на услугите или финансови загуби за съответния субект;

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

б) засегнало е или е в състояние да засегне други физически или юридически лица, като е причинило значителни имуществени или неимуществени вреди.

В съображение 101 от NIS 2 се казва: "Показатели като степента, в която е засегнато функционирането на услугата, продължителността на инцидента или броя на засегнатите получатели на услуги, биха могли да играят важна роля при определянето на това дали оперативното прекъсване на услугата е сериозно".

Освен това, не са публикувани насоки за това какво би означавало „тежка финансова загуба" или какви биха били „значителни материални или нематериални щети".

Както съществените, така и важните субекти трябва да докладват за значителни инциденти, докато няма изисквания за докладване на други видове инциденти.

4.3.2. Докладване на инциденти

NIS 2 изисква съществените и важни субекти да уведомяват следните страни за значителни инциденти:

- Екипът за реагиране при инциденти с компютърната сигурност (CSIRT) или компетентен орган (тези органи са определени от държавите членки да отговарят за киберсигурността и за надзорните задачи).
- Получатели на услуги от съществени или важни субекти, които са потенциално засегнати от значителния инцидент.

4.3.3. Механизъм за докладване на инциденти

Член 23 изисква от дружествата да докладват за значителни инциденти по следните начини:

Таблица 8. *Механизъм за докладване на инциденти*

Изискване за NIS 2	Съответна статия от NIS 2	Кога да докладвате	Какво да докладвате	Предложено име на документ
Уведомление (за получателите на услуги, които са потенциално засегнати от значителна киберзаплаха)	Член 23, параграф 2	Без неоправдано забавяне	всички мерки или средства за правна защита, които тези получатели са в състояние да предприемат в отговор на тази заплаха; също така информира тези получатели за значителната киберзаплаха	Значителен инцидент Уведомление за Получатели на Услуги

Ранно предупреждение (за ЕРИКС или компетентен орган)	Член 23, параграф 4, буква а)	Без неоправдано забавяне и във всеки случай в рамките на 24 часа от узнаването за значимия инцидент	Посочва се дали се подозира, че значимият инцидент е причинен от незаконни или злонамерени действия или би могъл да има трансгранично въздействие	Ранно предупреждение за значителен инцидент
Уведомление за инцидент (за CSIRT или компетентен орган)	Член 23, параграф 4, буква б)	Без неоправдано забавяне и във всеки случай в рамките на 72 часа от узнаването за значимия инцидент	Посочва първоначална оценка на значимия инцидент, включително неговата тежест и въздействие, както и, когато са налични, показателите за компромис	Значителен инцидент Уведомление за CSIRT/компетентен авторитет
Междинен доклад (за CSIRT или компетентен орган)	Член 23, параграф 4, буква в)	По искане на ЕРИКС или на компетентния орган	Съответни актуализации на състоянието	Значителен инцидент Междинен Доклад

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Окончателен доклад (за CSIRT или компетентен орган)	Член 23, параграф 4, буква г)	Не по-късно от един месец след подаване на уведомлението за инцидента	(1) Подробно описание на инцидента, включително неговата тежест и въздействие; (2) вида на заплахата или първопричината, която е вероятно да е предизвикала инцидента; (3) прилагани и текущи мерки за смекчаване на последиците; iv) когато е приложимо, трансграничното въздействие на инцидента	Окончателен доклад за значителен инцидент
Доклад за напредъка (за ЕРИКС или компетентен орган)	Член 23, параграф 4, буква д)	В случай на продължаващ инцидент	(не е посочено)	Доклад за напредъка при значителни инциденти

4.4 Европейски схеми за сертифициране

Схемите на Европейския съюз за сертифициране на киберсигурността ще повлияят значително на пазара на ИКТ решения, като осигурят хармонизирано ниво на доверие в Съюза и извън него. ИКТ екосистемата, т.е. разработчици, доставчици на услуги, потребители на ИКТ, но и регулатори, оценители и национални органи, е необходимо да разберат предстоящите промени, за да бъдат подготвени. Освен извършената работа по разработването на схеми за сертифициране, Европейската агенция за киберсигурност ENISA има за цел да предостави подкрепа на екосистемата с насоки и кампании за повишаване на осведомеността .

Схемата на Европейския съюз за сертифициране на киберсигурността представлява изчерпателен набор от правила, технически изисквания за киберсигурност,

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

стандарти и процедури за оценка, определени на ниво Европейски съюз и приложими към сертифицирането на конкретни ИКТ продукти, услуги или процеси. Сертификатът на Европейския съюз за киберсигурност удостоверява, че ИКТ продукт, процес или услуга са сертифицирани в съответствие с такава схема и че отговарят на определените изисквания и правила за киберсигурност. Сертифицирането се извършва от орган за оценка на съответствието (CAB) , който може да одитира и/или тества и/или сертифицира. Всички сертификати ще бъдат публикувани от ENISA на специален уебсайт.

Член 24 от директивата NIS2 посочва, че за да се докаже съответствие за спазване на изискванията за внедряване на мерки за управление на риска в областта на киберсигурността, всяка държава от Европейския съюз може да изиска от съществените и важните субекти да използват конкретни ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от съществените или важните субекти или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност. Директивата дава насоки, че държавите членки могат, като се консултират с групата за сътрудничество и Европейската група за сертифициране на киберсигурността, да насърчават използването на съответните европейски и международни стандарти от съществените и важните субекти или да изискват от субектите да използват сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси.

Планира се и се очаква до края на първото тримесечие на 2024 г. Европейската агенция за киберсигурност ENISA да изготви схема за сертифициране съгласно член 48, параграф 2 от Регламент (ЕС) 2019/881 относно ENISA и сертифицирането на киберсигурността на информационните и комуникационните технологии.

Какъв е прогресът в разработването на схемите за сертифициране в ENISA? Няколко са основните схеми, по които се работи на различни етапи:

1. EUCC. Първата Европейска схема за сертифициране на киберсигурност по общи критерии, която е насочена към хардуерни и софтуерни продукти и компоненти. Очаква се до края на първото тримесечие на 2024 г. Европейската комисия да публикува акта за изпълнение, с който да се стартира схемата за сертифициране.

2. EUCS. Европейска схема за сертифициране на облачни услуги се изготвя с подкрепата на специална работна група и държави-членки. Очаква се становище по текста на схемата.

3. EU5G. Европейска схема за сертифициране на киберсигурност за 5G, която се разработва на две фази. По време на първата фаза, която приключи през есента на 2022 г., ENISA, експертите, събрани в рамките на специална работна група с Европейската комисия и държавите членки, са анализирали съществуващите оценки и

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

схеми за сертифициране и техните необходими актуализации, за да се съобразят с Директивата за киберсигурност. Очаква се първият проект на схема да бъде предоставен за обществено обсъждане.

4. Изкуствен интелект. С оглед на приемането на проекта на Регламент на ЕС относно изкуствения интелект ENISA оценява дали и как изкуственият интелект може да бъде обект на сертифициране за киберсигурност, както и как схемите в процес на разработване могат да бъдат използвани повторно. Тази дейност е подготвителна, тъй като ENISA не е получила официално нареждане за разработване на схема за сертифициране от Европейската комисия.

Кои са организациите, които се интересуват от Европейските схеми за сертифициране? Това са:

1. Доставчици на продукти и услуги. Сертифицирането на киберсигурността ще донесе нови пазарни възможности в Европейския съюз чрез унифициране на усилията за демонстриране на съответствие с изискванията. Решенията ще могат да се открояват на пазара, а извършената работа ще подпомогне развитието на вътрешна експертиза. За тези, които вече са сертифицирани по съществуващи схеми, ENISA и държавите-членки ще предоставят насоки за улесняване на процеса на преход и ще сравнят изискванията от съществуващите схеми с тези на ЕС, за да улеснят прехода.

2. Национални органи за сертифициране на киберсигурността. Както се изисква от Директивата за киберсигурност, всяка държава-членка трябва да определи национални органи за сертифициране на киберсигурността, които ще отговарят за надзора, сертифицирането и мониторинга на сертифицирането на киберсигурността на Европейския съюз на национално ниво и за обмена на ниво Европейски съюз.

3. Органи за оценяване на съответствието. Схемите на Европейския съюз за сертифициране на киберсигурността се разработват от ENISA с подкрепата на експерти от държавите членки и от индустрията, включително от общността за оценка на съответствието. Тези схеми са предназначени да отговорят на нуждите на държавите-членки, индустрията и да отговарят на изискванията на европейското законодателство, което ги прави ценен инструмент на европейско ниво за насърчаване на сигурността на продуктите и услугите. Тази нова стойност представлява значителна възможност за органите за оценяване на съответствието, които ще бъдат акредитирани да издават сертификати или да извършват дейности по оценка (тестове, одити) за тези схеми.

4. Потребители на сертификати. Сертификатите на Европейския съюз за киберсигурност се предоставят за сертифицирани ИКТ продукти и услуги срещу приложени схеми за сертифициране. Те демонстрират, че тестваните решения са устойчиви на определени нива на атаки, задават процеси за отстраняване, като

същевременно вземат предвид най-новите най-съвременни разработки. Те са признати в целия Съюз и позволяват на търговците на продукти и доставчиците на услуги да покажат съответствието на своето решение с конкретна схема, ниво на сигурност, обхват и потенциално разширение или профили за сигурност. Сертификатите ще са валидни за ограничен период от време, който може да бъде удължен чрез повторна оценка.

4.5 Прилагане на национални и международни стандарти за мрежова и информационна сигурност в държавната администрация

Една от насоките за развитие на мрежовата и информационна сигурност, заложена в NIS2, е свързана с прилагането на международните и национални стандарти. В настоящата част представяме важността от разбирането и прилагането на международни стандарти в областта на мрежовата и информационна сигурност.

В последните години на международно и европейско ниво се създават и приемат много стандарти, свързани с мрежовата и информационна сигурност. Важна роля в тази дейност играе Международната организация за стандартизация ISO - независима, неправителствена и международна, в която членуват 170 национални органи за стандартизация. Нейната цел е чрез своите членове да бъдат обединени експерти в различни области на знанието за споделяне, разработване и утвърждаване на доброволни, базирани на консенсус и подходящи за пазарните механизми международни стандарти, които подкрепят иновациите и предоставят решения за глобални предизвикателства.

Организацията има 75-годишна история. В началото са организирани 67 технически комитета с включени фокусни групи от експерти, като към настоящия момент функционират 802 технически комитета и подкомитета, ангажирани с разработването на стандарти. Техническият комитет представлява работен орган, който отговаря за определени области на стандартизация.

Към 31 декември 2023 г. Международната организация за стандартизация е генерирала 25111 международни стандарта[33], покриващи всички технически и производствени аспекти на бизнеса. Топ 5 технически сектори, за които са публикувани стандарти, са:

- 21,2 % Информационни технологии, графика и фотография
- 14,2 % Машиностроене
- 12,8 % Транспорт
- 8,5 % Неметални материали
- 7.3 % Здравеопазване, медицина и лабораторно оборудване

Националният орган за стандартизация, признат на национално ниво, на който е дадено право да бъде национален член Международната организация за стандартизация и други международни и регионални организации по стандартизация, е Българският институт за стандартизация. Към края на 2023 г. в него активно работят 77 технически комитета в

[33] https://www.iso.org/iso-in-figures.html

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

различни сектори на индустрията, като припокриват около 80% от техническите комитети на CEN, CENELEC, ISO и IEC[34].

Международните стандарти, създадени от ISO, са документи, създадени чрез консенсус и одобрени от признат орган, който определя за общо и повтарящо се прилагане правила, насоки или характеристики за дейности или техни резултати с цел постигане на оптимален ред в дадена съвкупност от обстоятелства. Освен това, общият термин „стандарт“ се прилага за всички международни, регионални и национални нормативни актове, като стандарти, технически доклади, технически спецификации, технически нормативни актове, ръководства, кодекси за добра практика и др., както и проектите на документи.

Стандартите и брандът ISO са разпознаваеми на световно ниво. Организацията работи в тясно сътрудничество с различни технически и професионални организации, като Международната електротехническа комисия IEC, Международния съюз по далекосъобщения ITU, Институт на инженерите по електротехника и електроника IEEE и много други.

През 1987 г. Международната организация за стандартизация и Международният електротехнически комитет създават JTC1[35] – съвместен технически комитет за разработване на стандарти в областта на информационните и комуникационните технологии за бизнеса и потребителски приложения. Комитетът функционира съгласно директивите и на двете организации и целта е да се избегне дублирането на усилията им при разработване на стандарти. След създаването на JTC1 настъпват големи промени на пазара на информационни технологии и комуникации. Към края на 2021 г. комитетът е публикувал 3175 стандарта, разработени от 22 подкомитета с включени около 4500 технически експерти от цял свят. Комитетът има глобално въздействие върху индустрията на световно ниво.

Един от подкомитетите JTC1 SC27 „Сигурност на информацията, киберсигурност и защита на лична информация“ разработва международни стандарти, технически доклади и технически спецификации в областта на мрежовата и информационна сигурност. Обхватът на дейност на подкомитета е свързан с разработване на методологии и техники за сигурност, управление на сигурността, в т.ч. на процеси, контроли и услуги, изисквания към криптографията, ръководства, документи, речници и процедури за компонентите на сигурността, критерии за оценка на сигурността и др. Огледален технически комитет на JTC1 в Българския институт за стандартизация е ТК 57 „Информационни и комуникационни технологии“.

Както всеки подкомитет, и JTC1 SC27 има своя работна програма. В таблица 9 е представена работната програма на подкомитета за 2024 г., в която са включени общо 91 стандарта от серията ISO 27000, които или са в процес на разработване, или са вече публикувани. Всички стандарти са в областта на сигурността на информацията, киберсигурността и защитата на личната информация. Стандартите са взети от електронния

[34] https://bds-bg.org/bg/committee
[35] https://jtc1info.org/

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

каталог на подкомитет JTC1 SC27[36] и от каталога на Международната класификация на стандартите ICS.

Във втората колона на таблицата е записан поредният номер на стандарта. Във третата колона е записан статусът на стандарта в зависимост от етапа, на който се намира. Четвъртата колона представя името на стандарта, а следващите колони указват към коя оперативна група стандарти може да бъде причислен конкретният стандарт:

- Управление
- Управление на активи
- Защита на информацията
- Сигурност на човешките ресурси
- Физическа сигурност
- Сигурност на системи и мрежи
- Сигурност на Приложения
- Сигурност на конфигурации
- Идентичност и управление на достъпа
- Управление на заплахи и уязвимости
- Непрекъснатост
- Сигурност при взаимоотношения с доставчици
- Правно съответствие
- Управление на събития
- Осигуряване на сигурността на информацията

Таблица 9. *Работна програма на подкомитет, и JTC1 SC27*

Като в таблицата колоните от 1-15 са както следва :

1. Governance
2. Asset Management
3. IS Protection
4. HR Security
5. Physical Security
6. System&Network Security
7. Application Security
8. Secure Configuration
9. Identity&Access Management
10. Treat&VM
11. Continuity
12. Supllier relationship
13. Legal&compliance
14. IS EventManagement
15. IS Assurance

[36] https://www.iso.org/committee/45306/x/catalogue/p/0/u/1/w/0/d/0

o	Standards Number	Published / Under Development / Under Update	Title										0	1	2	3	4	5
	ISO/IEC 27000	2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary															
	ISO/IEC 27001	2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements															

	ISO/IEC 27002	2022	Information security, cybersecurity and privacy protection — Information security controls															
	ISO/IEC 27003	2017	Information technology — Security techniques — Information security management systems — Guidance															
	ISO/IEC 27004	2016	Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation															

	ISO/IEC 27005	2022	Information security, cybersecurity and privacy protection — Guidance on managing information security risks															
	ISO/IEC 27006	2015	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems															

	ISO/IEC TS 27006-1	Draft	Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General															
	ISO/IEC TS 27006-2	2021	Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems															

0	ISO/IEC 27007	2020	Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing															
1	ISO/IEC TS 27008	2019	Information technology — Security techniques — Guidelines for the assessment of information security controls															
2	ISO/IEC 27010	2015	Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications															

3	ISO/IEC 27011	2016	Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations																
4	ISO/IEC 27013	2021	Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1																
5	ISO/IEC 27014	2020	Information security, cybersecurity and privacy protection — Governance of information security																

6	ISO/IEC TR 27016	2014	Information technology — Security techniques — Information security management — Organizational economics																
7	ISO/IEC 27017	2015	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services																

8	ISO/IEC 27018	2019	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors																
9	ISO/IEC 27019	2017	Information technology — Security techniques — Information security controls for the energy utility industry																
0	ISO/IEC 27021	2017	Information technology — Security techniques — Competence requirements for information security management systems professionals																

1	ISO/IEC TS 27022	2021	Information technology — Guidance on information security management system processes															
2	ISO/IEC TR 27024	Draft	ISO/IEC 27001 family of standards references list — Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements															
3	ISO/IEC 27028	Draft	Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes															

4	ISO/IEC 27031	2011	Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity															
5	ISO/IEC 27032	2023	Cybersecurity — Guidelines for Internet security															
6	ISO/IEC 27033-1	2015	Information technology — Security techniques — Network security — Part 1: Overview and concepts															

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

7	ISO/IEC 27033-2	2012	Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security															
8	ISO/IEC 27033-3	2010	Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues															

9	ISO/IEC 27033-4	2014	Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways															
0	ISO/IEC 27033-5	2013	Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)															

1	ISO/IEC 27033-6	2016	Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access																
2	ISO/IEC 27033-7	2023	Information technology – Network security — Part 7: Guidelines for network virtualization security																
3	ISO/IEC 27034-1	2011	Information technology — Security techniques — Application security — Part 1: Overview and concepts																

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

4	ISO/IEC 27034-2	2015	Information technology — Security techniques — Application security — Part 2: Organization normative framework															
5	ISO/IEC 27034-3	2018	Information technology — Application security — Part 3: Application security management process															
6	ISO/IEC 27034-5	2017	Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure															

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

7	ISO/IEC TS 27034-5-1	2018	Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas															
8	ISO/IEC 27034-6	2016	Information technology — Security techniques — Application security — Part 6: Case studies															
9	ISO/IEC 27034-7	2018	Information technology — Application security — Part 7: Assurance prediction framework															

0	ISO/IEC 27035-1	2023	Information technology — Information security incident management — Part 1: Principles and process																
1	ISO/IEC 27035-2	2023	Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response																
2	ISO/IEC 27035-3	2020	Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations																

3	ISO/IEC 27035-4	Draft	Information technology — Information security incident management — Part 4: Coordination																
4	ISO/IEC 27036-1	2021	Cybersecurity — Supplier relationships — Part 1: Overview and concepts																
5	ISO/IEC 27036-2	2022	Cybersecurity — Supplier relationships — Part 2: Requirements																
6	ISO/IEC 27036-3	2023	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security																

7	ISO/IEC 27036-4	2016	Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services															
8	ISO/IEC 27037	2012	Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence															
9	ISO/IEC 27038	2014	Information technology — Security techniques — Specification for digital redaction															

0	ISO/IEC 27039	2015	Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)																
1	ISO/IEC 27040	2024	Information technology — Security techniques — Storage security																
2	ISO/IEC 27041	2015	Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method																

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

3	ISO/IEC 27042	2015	Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence																
4	ISO/IEC 27043	2015	Information technology — Security techniques — Incident investigation principles and processes																
5	ISO/IEC 27050-1	2019	Information technology — Electronic discovery — Part 1: Overview and concepts																

6	ISO/IEC 27050-2	2018	Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery																
7	ISO/IEC 27050-3	2020	Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery																
8	ISO/IEC 27050-4	2021	Information technology — Electronic discovery — Part 4: Technical readiness																

9	ISO/IEC 27070	2021	Information technology — Security techniques — Requirements for establishing virtualized roots of trust																
0	ISO/IEC 27071	2023	Cybersecurity — Security recommendations for establishing trusted connections between devices and services																
1	ISO/IEC 27090	Draft	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems																

2	ISO/IEC 27091	Draft	Cybersecurity and Privacy — Artificial Intelligence — Privacy protection															
3	ISO/IEC 27099	2022	Information technology — Public key infrastructure — Practices and policy framework															
4	ISO/IEC TS 27100	2020	Information technology — Cybersecurity — Overview and concepts															
5	ISO/IEC 27102	2019	Information security management — Guidelines for cyber-insurance															

6	ISO/IEC TR 27103	2018	Information technology — Security techniques — Cybersecurity and ISO and IEC Standards																
7	ISO/IEC TR 27109	Draft	Cybersecurity education and training																
8	ISO/IEC TS 27110	2021	Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines																
9	ISO/IEC TS 27115	Draft	Cybersecurity evaluation of complex systems — Introduction and framework overview																

0	ISO/IEC 27400	2022	Cybersecurity — IoT security and privacy — Guidelines																
1	ISO/IEC 27402	2023	Cybersecurity — IoT security and privacy — Device baseline requirements																
2	ISO/IEC 27403	Draft	Cybersecurity – IoT security and privacy – Guidelines for IoT-domestics																
3	ISO/IEC 27404	Draft	Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT																

4	ISO/IEC TR 27550	2019	Information technology — Security techniques — Privacy engineering for system life cycle processes															
5	ISO/IEC 27551	2021	Information security, cybersecurity and privacy protection — Requirements for attribute-based unlikable entity authentication															
6	ISO/IEC 27553-1	2022	Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 1: Local modes															

7	ISO/IEC 27553-2	Draft	Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Remote modes															
8	ISO/IEC 27555	2021	Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion															

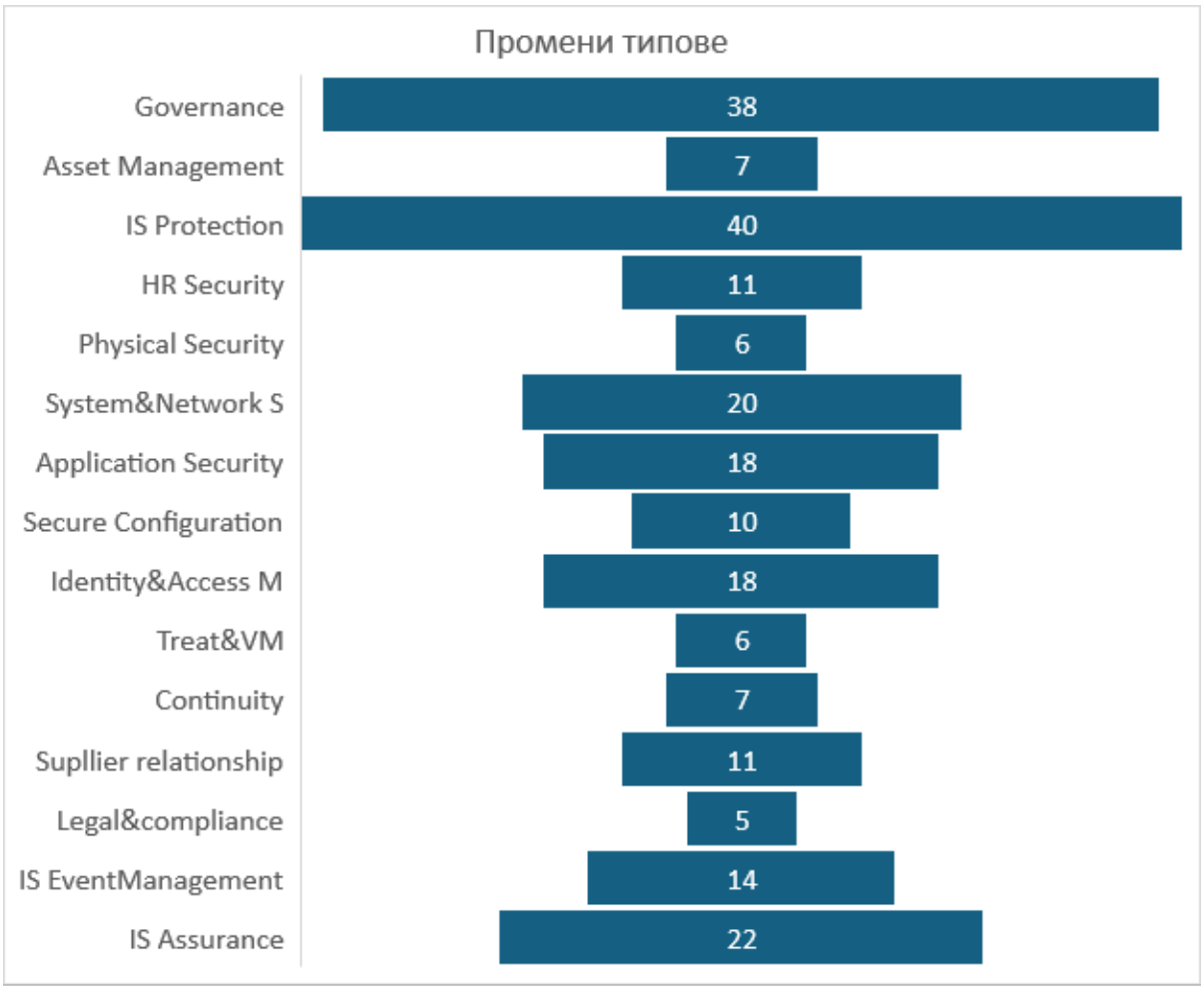
9	ISO/IEC 27556	2022	Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework															
0	ISO/IEC 27557	2022	Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management															
1	ISO/IEC 27559	2022	Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework															

2	ISO/IEC TS 27560	2023	Privacy technologies — Consent record information structure															
3	ISO/IEC 27561	Draft	Information security, cybersecurity, and privacy protection — Privacy operationalisation model and method for engineering (POMME)															
4	ISO/IEC 27562.2	Draft	Privacy guidelines for fintech services															
5	ISO/IEC TR 27563	2023	Security and privacy in artificial intelligence use cases — Best practices															

6	ISO/IEC 27565.3	Draft	Guidelines on privacy preservation based on zero knowledge proofs																
7	ISO/IEC 27566-1	Draft	Information security, cybersecurity and privacy protection — Age assurance systems — Framework — Part 1: Framework																
8	ISO/IEC 27566-2	Draft	Age assurance systems — Part 2: Benchmarks for benchmarking g analysis																
9	ISO/IEC 27566-3	Draft	Age assurance systems — Part 3: Interoperability ty, technical architecture and guidelines for use																

0	ISO/IEC TS 27570	2021	Privacy protection — Privacy guidelines for smart cities															
1	ISO/IEC 27701	2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines															

Данните могат да бъдат представени и в съответната графика:



Международните стандарти са ключов инструмент в борбата срещу киберпрестъпността, тъй като съдържат всеобхватни мерки за сигурност, базирани на добри практики от експерти от целия свят. Стандартите за оценяване на съответствието като тези за изпитване и сертификация също помагат на организациите да удовлетворят местното законодателство и да демонстрират пред своите заинтересовани страни, че са внедрени сериозни мерки за сигурност.

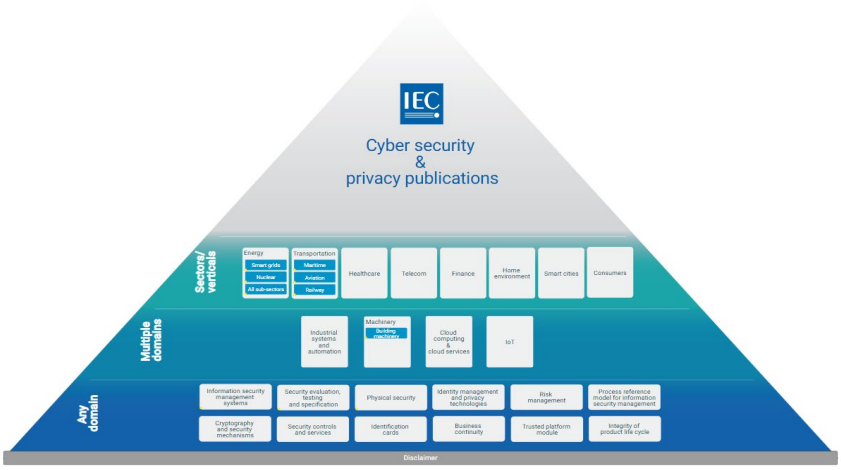
Но тъй като не е възможно един стандарт да бъде приложим за всички, и за организациите е предизвикателството да изберат правилните стандарти за своите нужди, Международната електротехническа комисия (IEC) разработи инструмент за подбор на стандарти[37]. Подготвен от ACSEC, консултативен комитет по информационна сигурност и

[37] https://mapping.iec.ch/#/maps/10

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

поверителност на данните към IEC, инструментът разглежда повече от 300 международни стандарти за киберсигурност, разработени от IEC, ISO и IEEE. По този начин той дава възможност на потребителите да видят бързо кои стандарти могат да посрещнат техните конкретни нужди.

Фигура 17. *Инструмент за търсене на стандарти за мрежова и информационна сигурност.*



Инструментът включва хоризонтални стандарти, които могат да бъдат използвани във всяка област, включително държавната администрация, като системи за управление на сигурността на информацията, оценка на сигурността, изпитване и специфициране, управление на риска, управление на идентичността, технологии за поверителност и защита на данните и много други.

Той изброява също стандарти, които покриват много области като Интернет на нещата (IoT) и изчисления в облака, както и конкретни сектори като здравни грижи, финанси, морски сектор, авиация и енергетика.

Проектният лидер на този инструмент Алиа Фурати заявява: „*С огромния брой стандарти за киберсигурност, които съществуват, този инструмент за подбор ще помогне на потребителите на стандарти да идентифицират бързо кои документи биха посрещнали конкретните им нужди. Той е разработен по начин, който осигурява неутрално и йерархично представяне на съществуващите стандарти въз основа на тяхното поле на приложимост съгласно обхвата и целите им*.“ Инструментът ще бъде редовно актуализиран, за да гарантира, че обхваща всички нови стандарти в сферата.[38]

[38] Източник IEC

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ГЛАВА 5. От оценка на състояние към оценка на готовност. Модел за оценка на технологичната зрялост

Правейки проучването на практиките за оценка на състоянието на киберсигурността на държавната администрация в България и на ниво Европейски съюз, както и на база предоставената до момента информация, може да се идентифицира приемливото ниво на регулаторната рамка, наложено от законодателството на ЕС. Тази нормативна рамка е адаптирана по адекватен начин в националното ни законодателство, като има разписани правила и добри практики за прилагането й. Независимо от наличието на малки пропуски или липса на интегритет между някои от нормативните актове, наличието на условности, даващи възможност за различно тълкуване и интерпретиране на ключови текстове, както и липсата на писмени становища от компетентните органи с цел унифициране на практиката и разрешаване на възникнали казуси, можем да изведем твърдението за достатъчност на регулациите.

В добавка към регулациите, стандартите в областта на информационната и киберсигурност, допринасят за още по-ясното дефиниране на изискванията и критериите за удостоверяване на съответствие.

Пример за това е групата от стандарти ISO 27000, като популярността им е причина да бъдат използвани, като отправна точка при определяне на изискванията по НМИМИС (групата стандарти е спомената в нея).

В зависимост от изпълнението или неизпълнението на така очертаните изисквания, се достига до бинарност на оценката състоянието на дадения оценяван субект: отговарящ или не.

Освен тези две състояния, при оценяването, имаме още и документирани наблюдения, които могат да бъдат обобщени в следните категории "**Препоръки**" (предлага възможност за подобряване на процеса при неговото изпълнение), **Забележка**" (маркира пропуски в изпълненията на дадени изисквания) и "Несъответствие" (установява неизпълнение на дадено изискване).

Реално, наблюденията са в контекста на състоянията и наличието на несъответствия не могат да позволят получаване на документ за изпълнение на изискванията, който да е със статус - съответствие.

Състоянията се удостоверяват с вътрешни, външни или одити от трета страна, които се осъществяват по публикувани методологии, като са подкрепени и от планове и цели за подобряване на съответствието и управлението на информационната и киберсигурност.

Но всички, така изброени, методи за оценка имат дефицити. Дефицитите са още по-критични за малки организации, за такива с ниски бюджети и за тези, които имат липса на капацитет, както и възможност да се ориентират в променящата се среда. Дефицитите, за които ще спомена малко по-долу, водят до формално отчитане на съответствие и фокуса от идентифициране, планиране, имплементира, наблюдение и подобряване се измества върху документално оформление на съответствие и скриване на информация, както и и осъзнато или не пропускане на рискове.

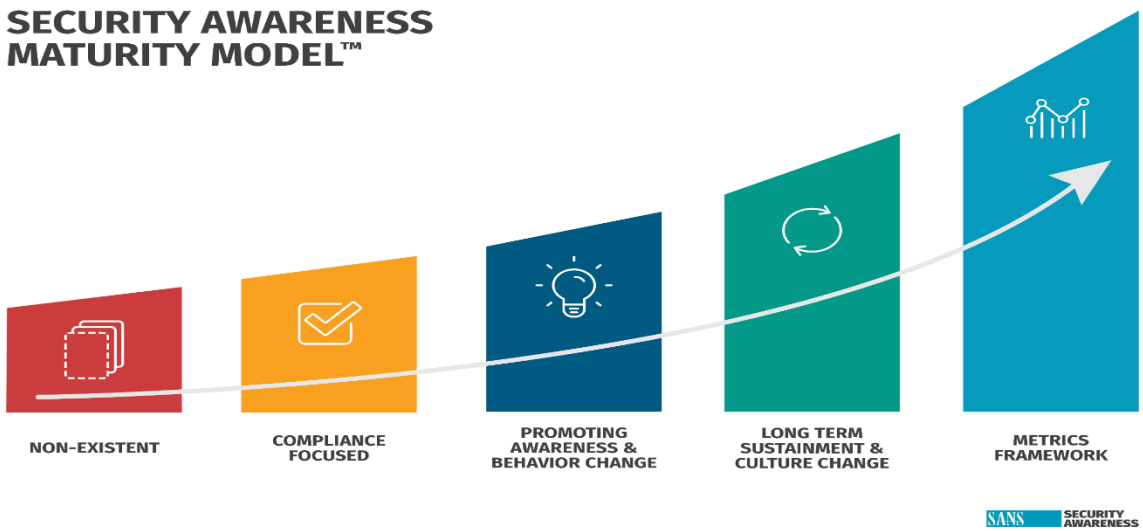
Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

Дефицитите, са както следва:

- различните организации имат различна възможност за подготовка и управление на дейностите в информационната и киберсигурност;
- подходите са различни;
- осъзнаването на реалността е сложен и субективен процес за различните организации;
- Планирането на етап преди да бъде постигнато съответствие и след постигане на съответствие трябва да е общ процес;
- Организациите трябва да имат ясна методика за самооценка, за да могат да се равняват по критериите и нивото си на зрялост;
- Въпросниците трябва да бъдат достъпни онлайн и задължителни за попълване независимо от това дали ще бъда направен одит или не,

Тези и още някои въпроси са идентифицирани в документи на ЕС[39] и определено показват посоката, в която ще се движи Съюзът, а именно да бъде хибриден, т.е съчетаващ рамки за съответствие, сертификационни схеми и схеми за оценка на зрялост. Примерът, показващ интеграцията на ISO 27001 и методология за оценка на зрялост, може да бъде видян в следващата фигура:

Фигура 18. *Методология за оценка на зрялост.*[40]



39 https://media.cert.europa.eu/static/Maturity_EUIBA/IT%20Security%20Maturity%20Analysis%20of%20the%20EU%20institutions,%20bodies%20and%20agencies.pdf

40 https://www.sans.org/blog/strategically-managing-your-human-risk-leverage-the-security-awareness-maturity-model/

В Този модел ясно може да идентифицира, че след осъзнаването и постигането на съответствие, организацията има стратегически цели отвъд отговарянето на изискванията. Планирането и въвеждане на специфична отправна точка за оценка на цифровата зрялост, чрез различни критерии за оценка в зависимост от сектора и размера на организацията, но и с централизирана платформа, интегрираща тази информация за държавната администрация, нейните доставчици и МСП е подход, който вярваме, че ще промени пътя за постигане на по-високо и устойчиво ниво на информационна и киберсигурност.

5.1 Методика за оценка на технологична зрялост на Европейския съюз

Европейският съюз разглежда опита си за оценка на цифровата зрялост на различни институции, организации и агенции в свой анализ IT Security Maturity Analysis of the EU institutions, bodies and agencies [41]. Този анализ е систематичен и изводите в него показват нуждата от прилагане на диференциран подход за оценка на цифровата зрялост. Подходът за анализа е базиран на техника за оценка на зрелостта с източник Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) [42].

Впоследствие този доклад се развива в направление и разработка на Инструмент за оценка на цифровата зрялост на МСП[43] , който е изключително полезен, но след наш тест се оказа, че е приложен от една единствена компания в България.

Идентифицирахме и следните няколко документа, които биха могли да бъдат отнесени към методология за оценка на цифровата зрялост :

- Methodology for Sectoral Cybersecurity Assessments[44]
- CSIRT Maturity Framework[45], както и свързания с него инструмента за оценка на екипите базиран на модела SIM3[46]

Независимо, кой от тези подходи и инструменти изберем, в крайния резултат имаме диаграма на текущото състояние, възможности и план за подобряване и отчитане на прогреса спрямо предишното измерване. Добрата практика предполага и електронно анонимизирано събиране на информацията и предоставяне на информация къде е организацията в рамките на всички организации, в рамките на нейния домейн, спрямо нейния размер и регион. Данните от тези проучвания и помощ може да се приложат за планиране на мерки и създаване на програми за подпомагане и финансиране, както и за поддържане на качеството на вече приложени такива.

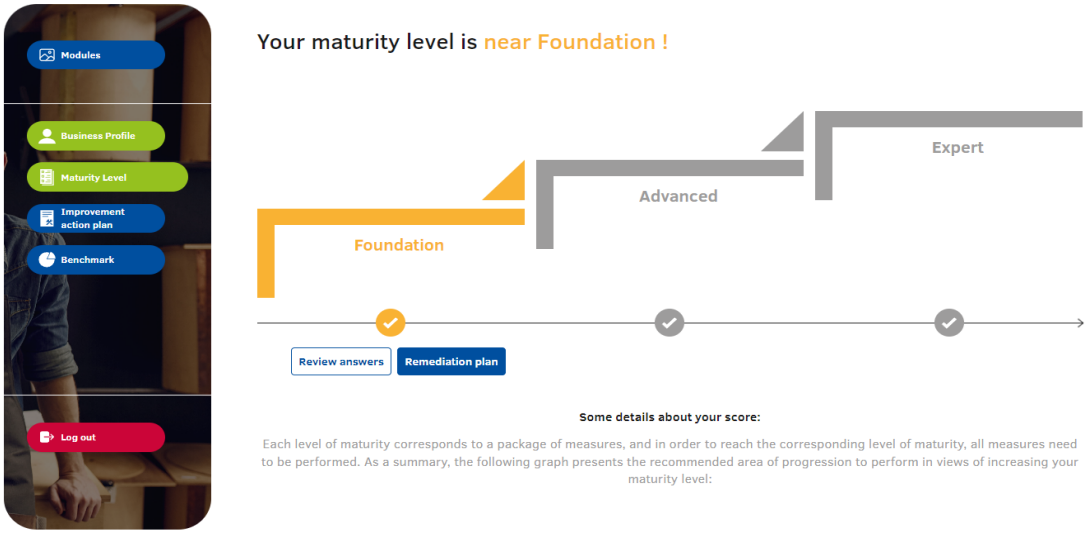
[41] https://media.cert.europa.eu/static/Maturity_EUIBA.pdf
[42] https://www.cyber.gov.au
[43] https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises/#/
[44] https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment
[45] https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity
[46] https://opencsirt.org/csirt-maturity/sim3-and-references/

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

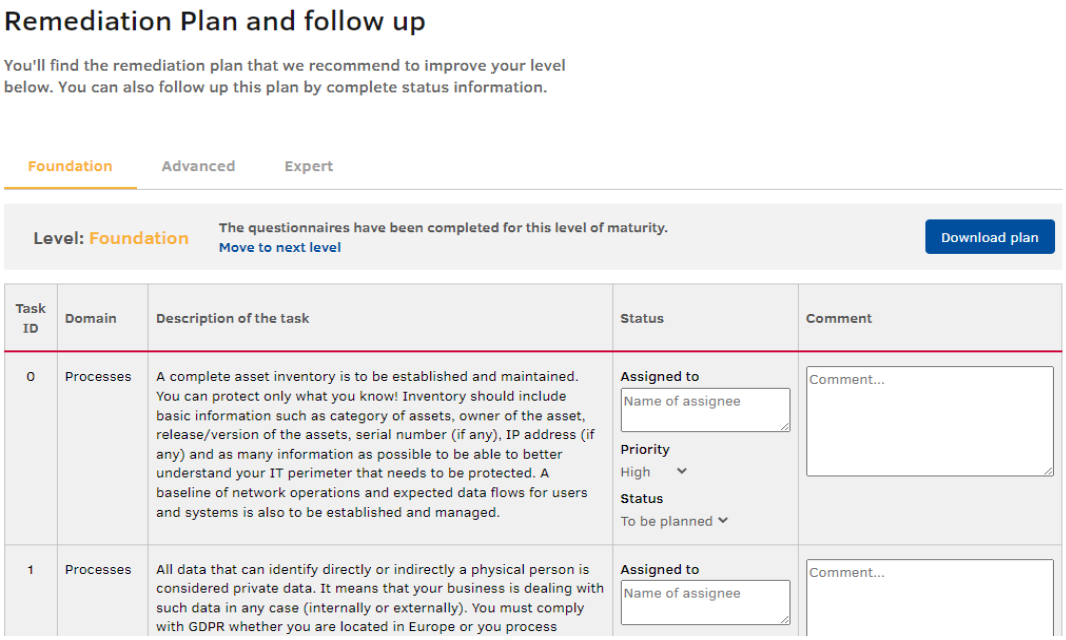
Препоръката ни е да се обсъди стратегическия подход на ЕС, а дори България да опита да предложи въвеждане на оценка на зрелостта на периодична база за всички организации в публичния и частен сектор, работещи с публични ресурси, или бидейки част от веригата за доставка.

5.2. Примерни резултати от оценка на зрялост за МСП

Фигура 19. *Примерни резултати от оценка на зрялост*

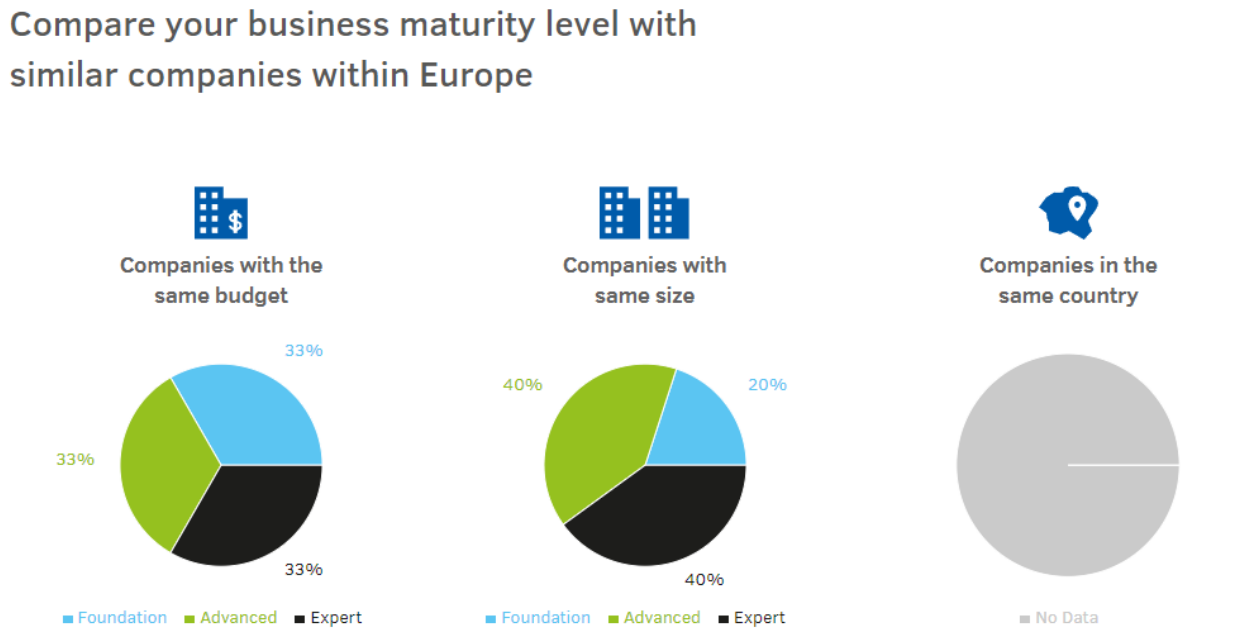


Фигура 20. *План за поправяне и последващи действия*



Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Фигура 21. *Сравнение модела на зрялост със сходни компании в Европа*



5.3 Необходимост от методики за оценка на зрялост в областта на мрежовата и информационна сигурност

В предишния раздел от анализа беше разгледано какво представлява съответствието и какви са референциите и стандартите, спрямо които може да се търси покриване на изискванията в контекста на информационната и киберсигурност. Добрата база, на която това да се прави, предполага и ясни правила за отчитане на постигането му, но административният и дисциплинарен натиск водят до случаи, в които добрите практики биват заменени от административно отчетна формалност.

Разделяйки съответствието и зрелостта и това, че зрелостта продължава да се развива след достигане на съответствие, предлагаме детайлно да разгледаме добрите практики от създаване и прилагане на модел за зрялост в областта на информационната и киберсигурност. Идеята за зрелостта по киберсигурност може да бъде разглеждана като неизменна част от цифровата зрялост.

В следващите страници ще разгледаме и сравним няколко методики като с това ще предоставим достатъчно информация за основите, които можем да използваме, за да изберем и въведем модел на зрялост, приложим за държавната администрация.

Какво е общото за моделите за зрялост, които ще разгледаме. Те са свързани с:

- Опит за събиране на най-добрите практики за киберсигурност;

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Разработени са в сътрудничество на експерти от различни среди;
- Вземат предвид размер, знания, умения, способности и опит на организациите, които ще използват модела;
- Възприемат жизнен цикъл и подход за непрекъснато усъвършенстване на киберсигурността.

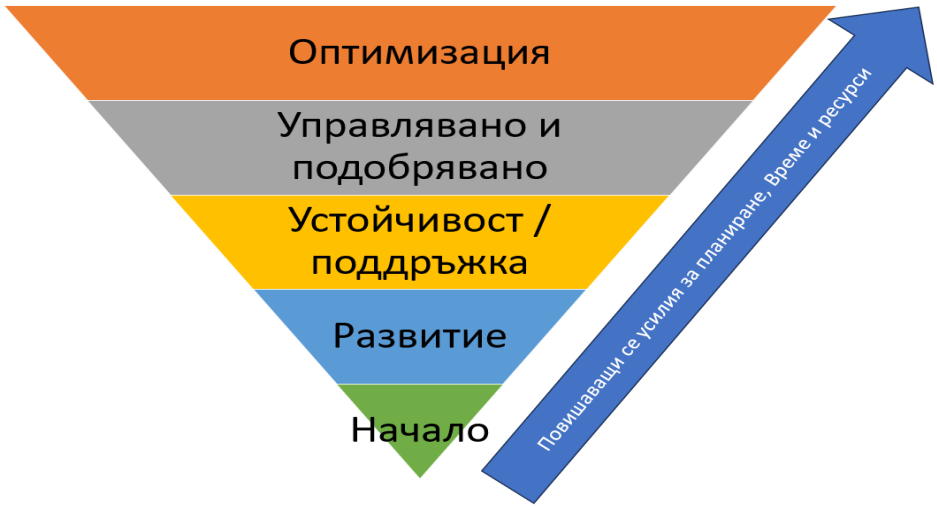
С какво са полезни моделите за зрялост ?

- Позволяват на организациите да продължават да предоставят услуги на своите клиенти без прекъсване;
- защитават чувствителна потребителска и корпоративна информация;
- Подпомагат спазването на законите и разпоредбите, които управляват тяхната дейност;
- Осигуряват структура за организациите в контекста на способностите им в планирането на работната сила в киберсигурността, създавайки основа за последователна оценка и измерване на развитието във времето;
- Предлагат управленски инструмент за лидерство при идентифициране на възможности за растеж и развитие.

Структурата на всички модели може да бъде обобщена графично в обърната пирамида, като с преминаване на всяко следващо по-горно ниво предизвикателствата към организацията са по-големи. При правилното изпълнение и стабилизиране на базовите слоеве, реално ръстът е плавен, защото се надгражда. Моделите за зрялост разчитат на честност и мотивация.

Следваща фигура представя нагледно това.

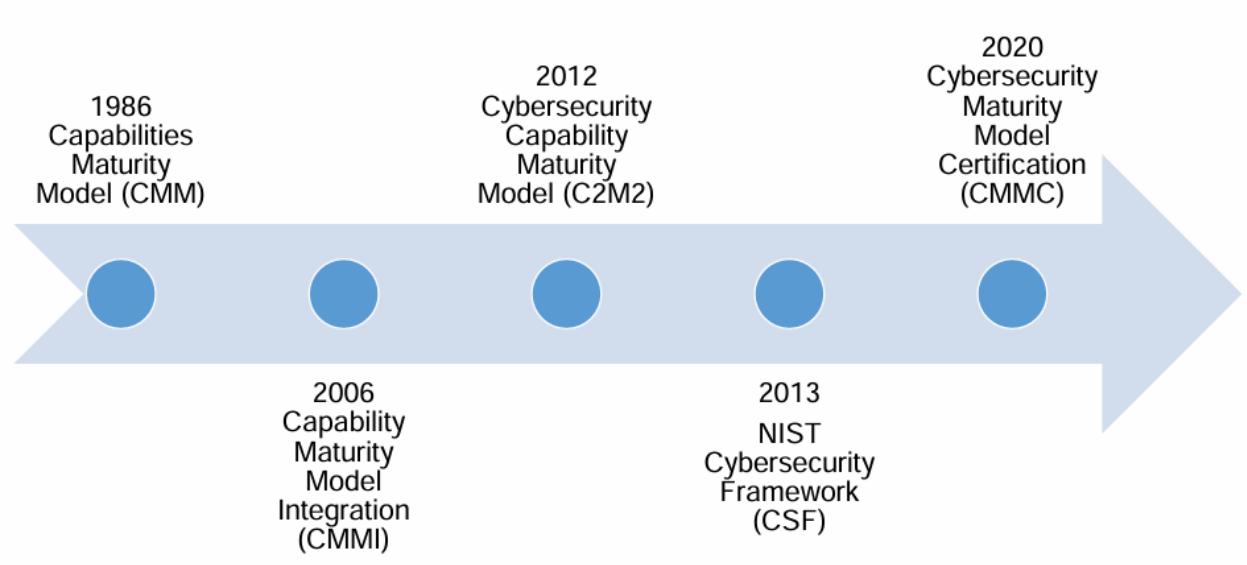
Фигура 22. *Примерна обобщена структурна на моделите за зрялост*



Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

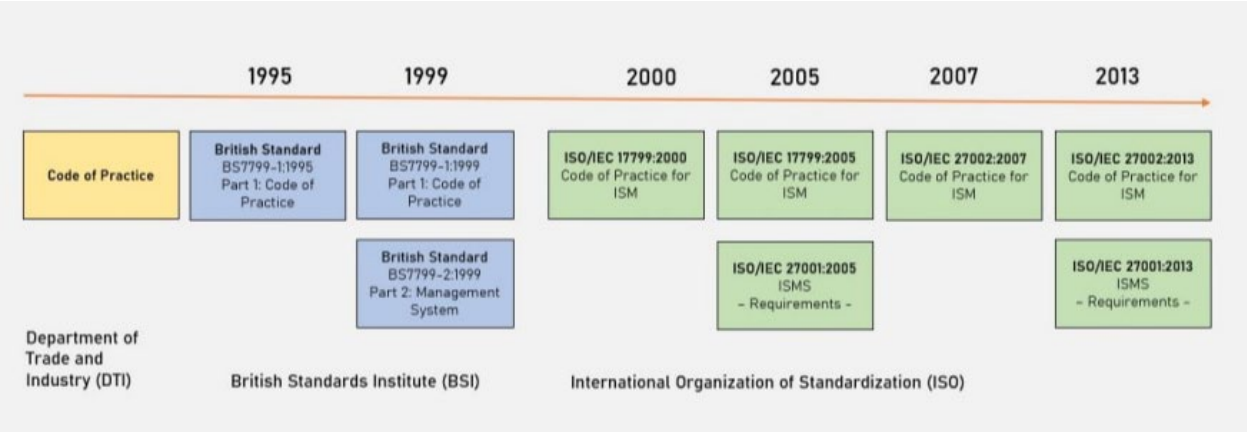
Както системите за съответствие, директивите, регламентите и законодателната рамка и съпровождащите ги спомагателни документи, като подзаконови актове, добри практики и др., така и моделите за зрялост имат своята история. Развитието им е започнало приблизително преди 40 години, като същото може да бъде свързано с момента на стартиране на дигиталната революция в средата на 80-те години на миналия век.

Фигура 23. *Развитие на моделите за зрялост*



За да можем да направим сравнение с периода на възникване на първите стандарти / системи за съответствие, прилагаме графика за историческото развитие на стандарта ISO 27001

Фигура 24. *Сравнение с периода на възникване на първите стандарти/системи за съответствие*



Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Моделът на зрялост е технология за оценка за очакванията за достигане на определено ниво на знания, умения и тяхното приложение в действия, аналогични с житейското развитие на човека, поради което този модел е естествено базиран на усещането ни за човешка зрялост и нейното постигане и поддържане.

При разглеждането на идеята за моделите, а и имайки предвид горната диаграма, със сигурност съществува сходност на подходите и процеса на приложимост. И тази сходност е точно компонентът, който прави възможно добавянето на модел за зрялост толкова естествено и осъзнато да се появява в документите на европейско ниво не само в частта информационна и киберсигурност.

Но преди да продължим с анализа на различните модели нека отговорим на въпроса, който би си задала организацията:

- Защо имам нужда от модел за управлението на зрелостта на информационната и киберсигурност?

И краткият отговор е: защото, използвайки модела, ще имате истината за:

- Текущото ви състояние;
- Къде се намирате спрямо останалите и това ще ви покаже - зрялост, но според кое и в сравнение с кого;
- Имайки реалното състояние и целите ви в дългосрочен план ще можете да решите - кога и в какво да инвестирате, като сте наясно с очакванията, но и коя стъпка какво ще ви донесе;
- Организацията спрямо наличните активи, капацитет и ресурси, но и рисковете, за да може да се балансират ползите от киберзащита и финансова устойчивост с фокус ефективност;
- Създаване на пътна карта за нуждите от реализация на всеки етап заедно със специалистите по мрежова, информационна и киберсигурност и лидерите на организацията.

Процесът е цикличен и моделите се развиват, така че пътя, по който ще вървите, за да постигнете успешно осъществяване на модела, ще се налага да затваряте кръга и да започнете отначало. Но вече по-сигурни и по-устойчиви.

Следващата фигура представя схематично описания отговор на въпроса и цикличността на действията:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Фигура 25. *Схематично описание на цикличността на действията*

Следващата логична стъпка при прилагането на модела след осъзнаването "защо ми е нужен" е "как да го използвам".

Подходът за прилагане е идентичен на подхода за въвеждане на системи за управление на сигурността на информация и управление на проекти, свързани с киберсигурността, а именно: Планирай, Приложи, Провери, Реагирай. Всеки един от тези етапи се характеризира с минимален набор от действия, обобщени в диаграма на етапите и детайли в нея:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

Фигура 26. *Схема на цикъла Планирай, Приложи, Провери, Реагирай*

5.4 Анализ на популярни модели на зрялост

Как да използвам модела на зрялост е логичен въпрос. Ако си задавате този въпрос е естествено да потърсите базова информация за съществуващите модели, които са придобили популярност. В предишната глава засегнахме модела на ЕС за оценка на зрелостта на малки и средни предприятия, както и по-ранен доклад, който реферира към модела за оценка на зрялост, прилаган в Австралия - Essential Eight Maturity Model[47]. Моделите, които ще разгледаме по-долу, не са включени в разглежданите досега, но се

[47] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

смятат за тези с най-широко разпространение и доказана ефективност. Вие като организация може да изберете онзи, който е подходящ за вас до момента в който не бъде приет и наложен един или няколко централизирано. В сравнителния анализ ще бъдат представени данни за следните модели: Cybersecurity Capabilities Maturity Model(C2M2), NIST Cybersecurity Framework (CSF), DOD Cybersecurity Maturity Model Certification

5.4.1. Cybersecurity Capabilities Maturity Model(C2M2)[48]

Cybersecurity Capabilities Maturity Model (C2M2) е разработен с цел да помогне на организациите в различни сектори да управляват своята киберсигурност по ефективен и зрял начин. C2M2 предлага структуриран подход за оценка и подобрение на способностите на организацията в областта на киберсигурността, като се фокусира върху няколко ключови аспекта на управлението на информационната сигурност.

Основни компоненти на C2M2:

1. Модел на Зрялост: C2M2 определя нивата на зрялост на организацията в контекста на киберсигурността, като позволява на организациите да оценят текущото си състояние и да идентифицират стъпки за подобрение. Моделът разделя способностите на организацията в различни домейни, като всяка способност се оценява според определено ниво на зрялост.

2. Домейни на Способности: C2M2 включва редица домейни, като например управление на риска, управление на активи, защита и възстановяване от инциденти, и др., които предоставят структуриран начин за разглеждане на различните аспекти на киберсигурността в организацията. Това позволява на организациите да разберат по-добре своите силни и слаби страни в различните области.

3. Самооценка и Подобрение: C2M2 насърчава организациите да извършват периодични самооценки на своите способности за киберсигурност, за да идентифицират възможности за подобрение. Моделът предоставя инструменти и ресурси за помощ при самооценката, включително ръководства и шаблони.

4. Фокус върху Непрекъснато Подобрение: Основна характеристика на C2M2 е акцентът върху непрекъснатото подобрение на практиките в контекста на киберсигурността. Моделът разбира, че киберсигурността е динамична област, и насърчава организациите да развиват култура на постоянно подобрение и адаптация към новите заплахи и технологии.

5. Универсалност и Гъвкавост: C2M2 е проектиран да бъде приложим за организации от всякакъв размер и от различни сектори, включително енергетика, финанси и здравеопазване. Това го прави универсален инструмент, който може да бъде адаптиран към специфичните нужди и условия на различните организации.

[48] https://c2m2.doe.gov/

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

C2M2 предлага цялостен и гъвкав подход за оценка и подобрение на способностите за киберсигурност в организациите. Чрез фокусирането върху непрекъснатото подобрение и предоставянето на ясни насоки за самооценка, моделът помага на организациите да укрепят своята киберсигурност и да се адаптират към постоянно променящата се среда и заплахи.

5.4.2. NIST Cybersecurity Framework (CSF)[49]

NIST Cybersecurity Framework (CSF) е широко признат стандарт за киберсигурност, разработен от Националния институт за стандарти и технологии (NIST) в САЩ. Той предоставя комплексен набор от насоки, който помага на организациите от всички сектори да управляват и намаляват кибер рисковете. Чрез своята гъвкава и адаптивна структура, CSF насърчава индивидуалния подход към киберсигурността, позволявайки на организациите да прилагат практики, които най-добре отговарят на техните специфични нужди и рискови профили.

Основни компоненти на NIST CSF:

1. Функции за Киберсигурността: CSF е организиран около пет основни функции - Идентифициране, Защита, Откриване, Реагиране и Възстановяване. Тези функции предоставят високо ниво рамка за управление на рисковете от киберсигурност и са приложими във всички типове организации.
2. Категории и Подкатегории: Всяка функция е разделена на категории и подкатегории, които детайлизират конкретни цели и дейности за управление на киберсигурността. Това структурирано разбиване помага на организациите да разработят подробни стратегии и да идентифицират специфични области за подобрение.
3. Профили и Целеви Състояния: CSF насърчава разработването на „профили“, които отразяват текущите практики и амбиции на организацията за подобрение в областта на киберсигурността. Това позволява на организациите да определят целеви състояния и да планират инициативи за развитие.
4. Ръководство за Имплементация: CSF предоставя подробни насоки за имплементация, включително препоръки за идентифициране на приоритети и ресурси. Това помага на организациите да разработват ефективни планове за управление на киберсигурността, които са в съответствие с техните бизнес цели и регулаторни изисквания.
5. Фокус върху Непрекъснатото Подобрение: CSF подчертава значението на непрекъснатия преглед и актуализиране на практиките за киберсигурност. Организациите се насърчават регулярно да преоценяват своите профили и да адаптират своите стратегии, за да отговорят на развиващите се заплахи и технологични промени.

[49] https://www.nist.gov/cyberframework/getting-started

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

NIST Cybersecurity Framework предлага цялостна и гъвкава структура за управление на киберсигурността, която може да бъде адаптирана от организации с различен размер, сектор и специфика. Чрез насърчаване на систематичен подход към идентифициране, защита, откриване, реагиране и възстановяване от инциденти в контекста на киберсигурността, CSF помага на организациите да укрепят своите защити и да подобряват своята устойчивост срещу кибер заплахи.

5.4.3. DOD Cybersecurity Maturity Model Certification[50]

The Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) представлява ключова инициатива, разработена за укрепване на киберсигурността във веригата на доставки на отбранителната индустрия. CMMC има за цел да интегрира множество стандарти за киберсигурност и най-добри практики, за да се създаде единна стандартна рамка за всички доставчици, работещи с DoD. Моделът е проектиран да защитава контролираната некласифициране информация (CUI) и федералната информация за договорите (FCI) в информационните системи и мрежите на подизпълнителите.

Основни компоненти на CMMC:

1. Нива на Зрялост: CMMC обхваща пет нива на зрялост, като всяко ниво представлява по-голяма степен на защита и процеси за управление на киберсигурността. Нивата варират от основна киберхигиена до напреднало управление на риска и процеси, които са необходими за защита на чувствителна информация.

2. Практики и Процеси: В рамките на всяко ниво, CMMC изисква определен набор от практики (действия) и процеси (управление), които трябва да бъдат имплементирани и институционализирани. Това гарантира, че организациите не само прилагат необходимите технически контроли, но и поддържат устойчивост и непрекъснато подобрение в своите усилия за киберсигурност и киберустойчивост.

3. Сертификация: За разлика от други рамки, CMMC изисква независима сертификация от акредитирани органи, за да участват доставчиците в договори с DoD. Това осигурява, че всички доставчици във веригата на доставки на DoD отговарят на установените стандарти за киберсигурност преди да получат или продължат договори.

4. Обхват: CMMC е приложим за всички доставчици, работещи с DoD, включително малки и средни предприятия, което подчертава универсалната нужда от защита на отбранителната информация, независимо от размера на организацията или нейната роля във веригата на доставки.

5. Адаптивност: Моделът е проектиран да бъде адаптивен и да отразява промените в заплахите за киберсигурността, като се актуализира с времето, за да остане релевантен и ефективен в защитата на контролираната информация.

[50] https://dodcio.defense.gov/CMMC/

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Заключение:

DoD Cybersecurity Maturity Model Certification (CMMC) представлява значителна стъпка към постигането на по-високо ниво на киберсигурност във веригата на доставки на отбранителната индустрия. Модела е приложим извън обхвата на създателите.

Таблица 10. *Сравнителна таблица на моделите C2M2, CSF и CMMC*

	Cybersecurity Capabilities Maturity Model (C2M2)	NIST Cybersecurity Framework (CSF)	Cybersecurity Maturity Model Certification (CMMC)
Текуща версия	2.1	1.1	2
Нива на зрялост Функции/нива	3	5/4	5
Домейни/категории за сигурност	10	21	17
Процеси/Подкатегории /Възможности	38	108	44
Практики/контроли (максимум)	210	240	171
Вид на оценката	Самооценка	Самооценка	От трета страна

5.5. Препоръки за модел за зрялост

Заключения за ползата от модели за зрялост и предложение за план за разработване и пилотно стартиране на такъв с паралел на транспониране на директивата МИС2:

5.5.1. Необходимост от моделите за зрялост

Моделите за зрялост са критични за киберсигурността, тъй като предоставят структуриран метод за оценка и непрекъснато подобрение на защитите срещу киберзаплахи. Те помагат на организациите да идентифицират слабости в своите системи

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

за киберсигурност, да определят приоритети на действията си и да насочат ресурсите си по начин, който максимизира защитата. Във време на постоянно развиващи се заплахи и технологии, моделите за зрялост предлагат динамична рамка, която позволява адаптиране към нови рискове, гарантирайки, че мерките за киберсигурност са актуални и ефективни.

5.5.2. Въвеждане на модели на зрялост като добра практика, като разширение на оценката по стандарти

Въвеждането на модели за зрялост в киберсигурността представлява важна стъпка към създаването на по-защитена и устойчива информационна среда. Тези модели не само допълват оценката по стандарти, като предоставят подробен план за действие за подобрения, но също така улесняват организациите да разберат своето текущо състояние и да планират своето бъдещо развитие в областта на киберсигурността. Моделите на зрялост подкрепят културата на непрекъснато подобрение и помагат на организациите да се адаптират към постоянно променящия се пейзаж на заплахите. Те насърчават развитието на персонализирани стратегии, които са специфични за нуждите и рисковите профили на всяка организация, увеличавайки ефективността на усилия за киберсигурни и устойчиви организации.

Пътна карта за въвеждане на оценка на зрелостта в държавната администрация на България (предложение за тест и пилот):

За успешното въвеждане на оценка на зрелостта в държавната администрация на България през следващите 6 месеца, следва да се разработи пътна карта, която включва:

- Месец 1: Идентифициране на ключовите заинтересовани страни и създаване на работна група за киберсигурност. Преглед на съществуващите стандарти и политики за киберсигурност.
- Месец 2: Избор на подходящ модел за зрялост, адаптиран към специфичните нужди и предизвикателства на държавната администрация. Провеждане на първоначална оценка за идентифициране на текущото ниво на зрялост.
- Месец 3-4: Разработване на индивидуализирани планове за подобрение за всяко ведомство, с ясни цели, срокове и отговорности.
- Месец 5: Обучение и повишаване на осведомеността на служителите относно киберсигурността и ролята на модела за зрялост.
- Месец 6: Имплементация на първоначални мерки за подобрение, последвана от мониторинг и оценка на прогреса.

Имплементиране: Установяване на процес за непрекъснато преглеждане и актуализиране на оценката на зрелостта, с цел гарантиране на това, че мерките за киберсигурност остават ефективни срещу новите заплахи и променящите се фактори на контекста на организациите и обществото.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Такава пътна карта ще помогне на държавната администрация на България да изгради здрава основа за киберсигурност, да подобри своята устойчивост на киберзаплахи и да укрепи доверието на гражданите в цифровите услуги.

ГЛАВА 6. Модел за обучение, оценка, адаптиране и развитие на държавната администрация

В Директивата за NIS 2 се посочва много ясно, че всички служители, включително висшето ръководство, трябва да преминат през обучение по киберсигурност. Кои теми трябва да бъдат обхванати и как трябва да бъде организиран целият обучителен процес?

6.1. Теми за обучение и осведоменост по киберсигурност

В глава IV Мерки за управление на риска за киберсигурността и задължения за докладване, NIS 2 определя различни дейности и мерки за сигурност, които трябва да бъдат извършени. Най-добрият подход за определяне на теми за обучение и осведоменост по киберсигурност е, да се обхване всяка от тези дейности и мерки. Въпреки това, не всички от тези теми ще бъдат подходящи за всяка аудитория - затова по-долу ще видите, че темите са разделени според целевата аудитория.

Теми за всички служители (включително средно ниво и висше ръководство)

- Основи на Директивата за NIS 2 (обхващат всички съответни членове)
- Основни практики за киберхигиена (член 21, параграф 2, буква ж)
- Справяне с инциденти (член 21, параграф 2, буква б)
- Архивиране (член 21, параграф 2, буква в)
- Непрекъснатост на дейността (член 21, параграф 2, буква в)
- Използване на решения за многофакторно удостоверяване и непрекъснато удостоверяване на автентичността (член 21, параграф 2, буква й)

Теми за ИТ служители и мениджъри по сигурността

- Политика в областта на сигурността на информационните системи (член 21, параграф 2, буква а)
- Възстановяване при бедствия (член 21, параграф 2, буква в)
- Сигурност при придобиване, разработване и поддръжка на мрежи и информационни системи (член 21, параграф 2, буква д)
- Политики и процедури по отношение на използването на криптография и криптиране (член 21, параграф 2, буква з)
- Контрол на достъпа (член 21, параграф 2, буква и)
- Управление на активи (член 21, параграф 2, буква и)
- Защитени гласови, видео и текстови комуникации (член 21, параграф 2, буква й)
- Защитени системи за аварийна комуникация (член 21, параграф 2, буква й)

Теми, специфични за мениджърите по сигурността

- Стъпки за съответствие с NIS 2 (съответните членове в глава IV)
- Как NIS 2 е свързан с ISO 27001? (преамбюл съображение 79, член 21, параграф 1, член 25)

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Как NIS 2 е свързан с DORA? (Преамбюл съображение 28)
- Как NIS 2 е свързан с CER? (член 2, параграф 3, Член 3, параграф 1, буква е)
- Как NIS 2 е свързана с GDPR на ЕС? (преамбюл съображение 121), Член 35)
- Сертифициране на ИТ продукти и услуги (член 24)
- Държавни органи, определени в NIS 2 (няколко члена)
- Организиране на регулярни обучения по киберсигурност за различни нива служители в една компания (чл.20, ал.2; Член 21, параграф 2, буква ж)
- Как се извършва оценка на риска и лечение съгласно NIS 2 (член 21, параграф 1)
- Оценка на уязвимостта и качеството на доставчиците (член 21, параграф 3)
- Сигурност на човешките ресурси (член 21, параграф 2, буква и)
- Оценка на ефективността на мерките за управление на риска за киберсигурността (член 21 параграф 2, буква е)
- Предприемане на корективни мерки (член 21, параграф 4)

Теми за висшето ръководство и мениджърите по сигурността

- Кои са съществените и важни субекти, които трябва да спазват NIS 2? (Член 3)
- Основни изисквания за киберсигурност на NIS 2 (член 21)
- Одобряване и надзор на мерките за управление на риска за киберсигурността (член 20, параграф 1)
- Управление на кризи (член 21, параграф 2, буква в)
- Сигурност на веригата на доставки (член 21, параграф 2, буква г)
- Задължения за докладване (член 23)
- NIS 2 глоби и задължения (член 20, параграф 1; член 32, параграф 6; Член 34)
- Законодателство в областта на киберсигурността от държавите от ЕС (Чл.41)

6.2. Процес на създаване на обучение по МИС 2

Като цяло, процесът на създаване на обучение по киберсигурност, което е в съответствие с NIS 2, трябва да следва следните стъпки:

1) Оценете рисковете в компанията - това е основата за писане на документи за сигурност и за намиране на това, върху което да се съсредоточите в обучението по киберсигурност.

2) Дефиниране на политики и процедури за киберсигурност – по този начин ролите и отговорностите в киберсигурността стават ясни.

3) Определете целевите групи за обучение в рамките на компанията – групи от служители с различни роли в киберсигурността.

4) Определете теми за обучението – въз основа на рискове, роли и отговорности – които ще се различават за различните целеви групи.

5) Определете колко често ще се провежда обучението, как ще се измерва и кой ще отговаря.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

6.3. Възможности за редовно предоставяне на обучение

Има няколко възможности за предоставяне на обучение по киберсигурност МИС 2:

а) Обучение в класната стая, ръководено от инструктор:

- Професионалисти:
- Обучението може да бъде адаптирано според нуждите.

Минуси:

- Най-скъпият вид обучение
- Не може да се прави много често
- Трудно е да се проведе отделно обучение за различни целеви групи

б) Онлайн обучение, водено от инструктор

- Професионалисти
- Обучението може да бъде адаптирано според нуждите.

Минуси: По-ниска ангажираност

в) Предварително записано онлайн обучение, предоставяно чрез система за управление на обучението (LMS)

- Професионалисти
- Лесно проследяване на посещаемостта и резултатите от тестовете
- Служителите могат да гледат видеа в удобно за тях време
- Най-бюджетният вариант

Минуси: Участниците не могат да задават въпроси директно на инструктора

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ГЛАВА 7. Модел за оценка на дигиталната компетентност за служителите в държавната администрация

Тази глава ще прегледа наличната публична информация за политиката за оценка на дигиталната компетентност на служителите на държавната администрация и доставчиците на стоки и услуги, с които тя е в отношения.

Ще разделим тези два субекта на две части: служители (4.8.1) и доставчици (4.8.2), тъй като изискванията към отделните категории са различни и влиянието на законодателната рамка е от различно естество.

7.1 Изисквания за компетентност на служителите в държавната администрация

Основният документ, който определя изискванията за компетенции при назначаване и мобилност на държавни служители е Наредбата за провеждане на конкурсите и подпора при мобилност на държавните служители[51], приета на основание Закона за държавния служител:

Тази наредба определя още в Чл. 1: процедурата и начините за провеждане на конкурсите за назначаване на държавни служители и реда за извършване на подбор при преминаване на държавна служба в друга администрация (мобилност) по чл. 81а от ЗДСл.

От 01.01.2022 г. Е в сила нова глава четвърта, регламентираща тест за обща компетентност и познания за държавната администрация “Тест за общи компетентности и познания за държавната администрация”, който се провежда в гр. София чрез платформа, поддържана от администрацията на Министерския съвет, в компютърно оборудвани тестови зали в присъствието на квестори. Институтът по публична администрация (ИПА) съдейства на конкурсните комисии за организацията на провеждането на теста.

По-конкретно, съгласно Чл. 72. ал (3), предвидено, че: Тестът включва решаване на различни задачи, разделени в два модула. За решаването на всеки модул времетраенето, което не може да бъде надвишавано, е:

1. за модул "Общи компетентности" - 60 минути;

2. за модул "Познания за държавната администрация" - 30 минути.

Въвеждането на тестове, като форма на оценка, е израз на волята на държавата за подобряване на обективността и качеството на подбора на държавни служители чрез въвеждането на централизиран и децентрализиран етап на конкурса при постъпване на държавна служба, както и развитие на мобилността (провеждането на тестове е централизиран етап). Тестове трябва да се провеждат и в областта на цифровите умения и киберсигурността.

[51] https://lex.bg/bg/laws/ldoc/2137198193

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

7.2. Проблеми, свързани с обучението, и техни възможни решения

Този процес се прилага и към настоящия момент, а в Частична предварителна оценка на въздействието[52] на Администрацията на Министерския съвет са установени проблеми, засягащи въпроса с дигиталната компетентност и необходимостта от обособяването и като отделна част от теста:

Проблем 1: „В рамките на теста за оценка на компетентности не се оценяват компютърните умения на кандидатите“

1.1. Наредбата за провеждане на конкурсите и подбора при мобилност на държавни служители (НПКПМДС) предвижда тестът за компетентности да включва два модула – „Общи компетентности“ и „Познания за държавната администрация“. Съгласно чл. 15 от Наредба за условията и реда за оценяване изпълнението на служителите в държавната администрация (НУРОИСДА), служителите в държавната администрация, с изключение на заемащите технически длъжности, следва да притежават дигитална компетентност и да прилагат в работата си компютърни умения. Към момента липсва нормативно установен механизъм за оценка на дигиталната компетентност на кандидатите за държавна служба, а тестът за компетентности не включва въпроси, чрез които да бъдат оценени компютърните им умения.

Проблем 2: „Разпоредбите на НПКПМДС, свързани с организирането и провеждането на тестове за компетентности, не са достатъчно прецизни.“

Действащата нормативна уредба по отношение на организирането и провеждането на тестове за компетентности не е достатъчно прецизна, което може да създаде неясноти и затруднения при прилагането им като един от начините за провеждане на конкурс за държавни служители. Не е възможно проблемът да бъде решен без изменение на нормативната уредба.

По проблем 1 „В рамките на теста за оценка на компетентности не се оценяват компютърните умения на кандидатите.“

Вариант 1 „Без действие“:

Описание: При този вариант не се предприемат нормативни изменения и допълнения в НПКПМДС.

Положителни (икономически/социални/екологични) въздействия:

При този вариант не се предвиждат положителни въздействия върху заинтересованите страни.

Отрицателни (икономически/социални/екологични) въздействия:

[52] https://strategy.bg/FileHandler.ashx?fileId=29274

Въпреки че от края на 2019 г. дигиталната компетентност и компютърните умения са включени в общата компетентностна рамка на служителите в държавната администрация съгласно НУРОИСДА, ще се запази съществуващото положение, при което тези умения на кандидатите не могат да бъдат оценени обективно, а дигиталната им компетентност не може да бъде установена в рамките на конкурсната процедура. Вариант 2 „Приемане на Постановление за изменение и допълнение на Наредбата за провеждане на конкурсите и подбора при мобилност на държавни служители“:

Описание:

Вариантът предвижда изменения и допълнения на НПКПМДС, с които се въвежда отделен модул в теста за компетентности за оценка на дигиталната компетентност и компютърните умения на кандидатите.

Положителни (икономически/социални/екологични) въздействия:

Ще бъде въведен нормативно установен механизъм за обективна оценка на дигиталната компетентност и компютърните умения на кандидатите за държавна служба, с което ще се гарантира, че новоназначените служители в държавната администрация отговарят на изискванията на чл. 15, ал. 2 от НУРОИСДА. Наличието на компетентни служители ще допринесе за повишаване на ефективността и ефикасността на администрацията, както и за общественото доверие в институциите като цяло.

Отрицателни (икономически/социални/екологични) въздействия:

При този вариант не се предвиждат отрицателни въздействия върху заинтересованите страни.

Институтът за публична администрация е институцията, която най-добре разбира смисъла от способността организациите да учат, да се развиват и да повишават капацитета си в областта на информационните технологии и киберсигурността. Това много ясно може да се види, при запознаване с програмите за обучение и възможността за достъп до безвъзмездни и платени курсове, предоставяни от ИПА.

Чрез провеждането на курсове и оценката на знанията на курсистите, Институтът работи в рамките на задълженията си да повишава дигиталната компетентност и да подпомага заинтересованите служители на държавната администрацията да се развиват и доказват това.

7.3 Модели за оценка на дигиталната компетентност

Темата за оценката на дигиталната компетентност е засегната и в нарочен доклад МОДЕЛИ ЗА ОЦЕНКА НА ДИГИТАЛНАТА КОМПЕТЕНТНОСТ[53], разработен от д-р Теодора Върбанова.

[53] https://www.ipa.government.bg/sites/default/files/digital_competence_final.pdf

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Като в резюмето си д-р Върбанова ясно очертава фокуса на доклада си а именно: *Общата цел на настоящия аналитичен документ е да предложи разработването на модели за самооценка (включващи инструменти като тестове, практически задачи и казуси), с помощта на които държавните служители сами да оценяват нивото си на компетентност, както и модел за обективна независима външна оценка чрез изпит, като анализаторът се основава на рамката DigiComp и на добрите практики в Европейския съюз*"

Докладът в своите 83 страници навлиза в подробности и анализира състоянието на европейското законодателство в контекста на цифрови компетенции и интерпретирането на тези изисквания са съпоставени в контекста на анкета, проведена измежду 1056 служителя на държавната администрация.

Докладът, освен пълен анализ на DigiComp, засяга и въведената от ЕС рамка за електронна компетентност (e-CF)[54] с ясна референция към ESCO (European Skills, Competences, Qualifications and Occupations)[55].

В контекста на доклада, но извън неговото съдържание, считаме, че е важно да се предостави достъп до инструмент, който ще позволи на държавната администрация освен общите компетенции за администрация, да може да идентифицира и изискванията и очакванията за квалифициран ИТ персонал. Тази информация за компетенции може да бъде достъпна чрез инструмента The e-CF Explorer.[56] Докладът приключва с предложение за модел за оценка на дигиталната компетентност и начина за въвеждането му в държавната администрация.

Към момента на приключване на настоящия анализ не успяхме да открием доказателства за въвеждането му. Докато анализирахме данните за политики и проблемите, свързани със създаване на качествени и прозрачни критерии за оценка на нивото за обучение и доказване на квалификация, идентифицирахме скрит проблем, който се оказа блокиращ за образованието в домейн киберсигурност а именно, че в Списъка на професиите за професионално образование и обучение няма обособена цивилна професия в професионално направление 48 „Информатика“ (481 Компютърни науки) или в друга подходяща област, което представлява огромен проблем за ангажираните с развитието на киберсигурността – както в частния сектор, така и в публичния, защото поради този недостатък, не може да се изгради пряка връзка между обученията, предоставяни от различни центрове за професионално обучение и европейските компетентностни модели в сферата на киберсигурността, по които работи ЕЦИХ Тракия" [57]

[54] https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf
[55] https://esco.ec.europa.eu/en/about-esco/what-esco
[56] https://ecfexplorer.itprofessionalism.org/
[57] https://dihtrakia.org/bg/eczih-trakiya-postavi-vaprosa-za-aktualizacziyata-na-spisaka-na-profesiite-za-profesionalno-obuchenie

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Даден е пример за липса на професии в сферата на киберсигурността: "Понастоящем, центровете за обучение са принудени да обучават бъдещите специалисти по киберсигурност в някои от съществуващите алтернативни професии, следвайки утвърдените им учебни планове и програми – подход, който представлява компромис от гледна точка на частичното припокриване на знания и умения между отделните професии. Уменията, които един специалист в сферата на киберсигурността следва да притежава, застъпват, но не припокриват изцяло тези, които един приложен или системен програмист следва да развие в хода на своето обучение. За пример, професията „Старшина за ВМС – киберсигурност и кибероперации" е от безспорна нужда в системата на Българската армия, но не може да претендира за всеобхватно задоволяване на потребностите на частния сектор или тези на държавната администрация отвъд военизираните институции."

Тезата показва, как разбирането ни за киберсигурност и нейното обезпечаването е изоставена административно, независимо от демонстрираната ангажираност по основните европейски проекти за създаване на обща, цифрова и сигурна Европа, както и разграничаването на професиите, свързани с киберсигурността и тези с информационните технологии (виж The e-CF Explorer)

7.4 Обобщение на наличните политики за дигитална компетенция на служителите от публична администрация

- Има ясна европейска рамка за компетенции - умения и знания.
- Тази рамка е разделена в контекста на обща грамотност - DigiComp и рамка за умения и знания - European Cybersecurity Skills Framework (ECSF).[58]
- В двете рамки има зададени роли на учащи се, обучаващи и организации, както и изисквания към тях, както е в примера на DigiComp - European Framework for the Digital Competence of Educators: DigCompEdu.[59]
- Има изрична наредба за провеждане на изпити за приемане на работа и миграция в държавната администрация.
- Направена е оценка на дефицитите в тази наредба и предложение на МС за преодоляването и повишаване на качеството, чрез въвеждане на критерии.
- ИПА води целенасочена политика за обучение на служителите на държавната администрация на новите знания и умения свързани с дигитална компетенция и киберсигурност.
- ИПА изгражда и поддържа активни мрежи за обмен на информация и взаимопомощ.
- Неправителствените организации и организациите на работодателските организации са активни участници с предложение за подобряване на рамката за оценка на компетентността не само за държавната администрация, но и за МСП.

[58] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
[59] https://publications.jrc.ec.europa.eu/repository/handle/JRC107466

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене", финансиран от Оперативна програма „Добро управление", съфинансирана от Европейския съюз чрез Европейския социален фонд

- Оценките за дигиталната грамотност в България от доклада за цифровата декада е с незадоволително и ниско качество,
- Планът за възстановяване и развитие има предвиден ресурс обучение по професионална квалификация и първите инициативи са стартирали по него.[60]

И не на последно място, но от изключително важно значение е фактът, че в България вече съществува контактна точка по инициативата Европейска мрежа и център за компетентност в областта на киберсигурността.

7.5. Мерки за прилагане на рамката за компетенции на служителите от държавната администрация

- Адаптиране и изравняване на рамките за дигитални компетентности за държавната администрация съгласно европейските норми и добрите практики.
- Редовна комуникация и разяснения на ръководството на администрацията за разликата между административен, ИТ, и персонал, ангажиран с информационната и киберсигурност.
- Спешно въвеждане на професии, свързани с киберсигурността, за да могат да се извършват професионални обучения в средното, висше и професионалните обучения в ЦПО.
- Да се приложи The e-CF Explorer и да се провери, нуждата от попълване на дефицитите от знания и умения в държавната администрация, като се създадат персонални обучителни планове в зависимост личностната оценка.
- Да се стартират незабавно портали за анонимна, задължителна самооценка, като се комуникира, че ще се премине към идентифицираща такава.
- В реално време да се следят капацитета, нуждата от обучения и дефицитите.
- Да се премине от статично еднократно обучение, към интерактивно и постоянно.
- Да се въведат нови техники за оценка на знанието чрез симулация на реални събития от обхвата на киберсигурността, чрез добронамерени атаки и симулационни тренировки в кибер полигони. Тези активности и резултатите да бъдат управлявани локално при наличие на капацитет, но докладвани централизирано по шаблон.
- Всички - обучители, обучаващи или подготвящи съдържание за дигитални компетенции да бъдат оценени по създадени правила и рефлектиращи на изискванията минимум на DigiCompEdu.
- Да се разгледа и ясно да се дефинира обучението в детски градини, училища и университети с преобладаваща държавна собственост и критериите за знания и умения, които са приложими за тях.

[60] https://www.mlsp.government.bg/zaeti-i-bezrabotni-shche-poluchavat-vaucheri-za-obuchenie-po-profesionalna-kvalifikatsiya-tsifrovi-i-drugi-klyuchovi-kompetentsii

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Да се разшири рамката за професии и да създаде поддомейн на знанието във висшето образование с фокус киберсигурност в информационни технологии, Национална сигурност.

В заключение, може да се направи изводът, че българската администрация, общество и бизнес притежават основата за изграждане на нужния капацитет, който вече е подкрепен с нормативна база. Онова, което не достига, е приложението им по същество, което е значителен риск поради оформящата се огромна пропаст между дигитално не компетентните и тези със средни и висока оценка на компетентността си. Това ще доведе до дефицит на хора, работещи в държавната администрация, и риск за националната сигурност.

ГЛАВА 8 Анализ в контекста на обучения за осъществяване на политиката за мрежова и информационна сигурност

За да продължим успешно обученията на служителите в държавната администрация и да създадем успешна рамка за развитие на капацитет, умения и знания като финална част от доклада е важно да разбираме очакванията, предизвикателствата и нуждите на публичната администрация. Огромният обем нови директиви и регламенти и ясния фокус на МИС 2 върху дигиталната грамотност дефинират подхода, а именно:

- Създаване на микро обучения по цялата рамка на ЕС, както и такива произтичащи от сегашните нужди.

Тези обучения е нужно да бъдат подредени в последователност съгласно рамката за компетенции в държавната администрация и DigiComp.

- Програмите и курсовете, трябва да бъдат целево ориентирани към следните групи:
  - Обучения за всички (базова грамотност)
  - Ръководители
  - Служители с достъп до чувствителна и секретна информация
  - ИТ персонал
  - Ръководен ИТ персонал (както и отговорници по МИС).
  - Анализирайки последните данни от геополитическите рискове в контекста на информационна и киберсигурност, препоръчваме да създадем и допълнителен класификатор – *оперативно интересни лица за чуждо разузнаване или неприятелски групи в публичната администрация*.

През последната година ИПА е започнал да прилага този подход изпреварващо и на база обратната връзка. В института, за 2022 г. и 2023 г., са били обучени 22 218 държавни служители в 11 курса.

Активната комуникация на ИПА по оста – курсисти-преподаватели, както и обратната връзка са поставили основите на актуализация на каталога за обучения. Основните положителни страни на тези курсове и техните дефицити биха могли да бъдат обобщени в следното:

„Предимства в проведените курсове“:

- Високата компетентност и професионализъм на лекторите
- Конкретни примери от практиката в администрацията
- Преподаден на разбираем материал език, дори за неспециалисти в областта на ИТ
- Модерен, атрактивен и запомнящ се подход на преподаване на лекторите
- Полезни упражнения
- Възможността за дискусии

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Обхванатите актуални теми за оперативната съвместимост и информационната сигурност

„Дефицити и възможност за подобрение“:

- Материалът е много, по-голяма продължителност
- Недостатъчна продължителност на обученията
- По-голяма теоретична насоченост за сметка на практическите упражнения
- Недостатъчно конкретни отговори по прилагане на Наредбата за МИС в администрацията
- Недостатъчно практически примери и упражнения

„Какви са Вашите препоръки?“:

- Да се въведат курсове за киберсигурност за IT-експерти, PEN test и т.н.
- Да има симулации на кибератаки
- Ориентиране на курса към различните целеви групи – ръководители IT звена, IT специалисти и неспециалисти
- По-голяма продължителност на обученията
- По-често провеждане на подобни курсове с актуализиране и представяне на актуални тенденции и примери
- Повече интерактивност в обученията, време за дискусии и обсъждане на казуси

Позовавайки се и на тези данни, както реагирайки с висока степен на гъвкавост ИПА следва да създаде новия каталог за 2024 г. следните курсове:

Информационна и медийна грамотност

Европейската комисия определя медийната грамотност като „всички технически, познавателни, социални, граждански и творчески способности, които ни позволяват да имаме достъп и да имаме критично разбиране и взаимодействие с медиите“. Целта на този курс е да разшири дигитална та компетентност на служителите в администрацията чрез усвояване на ключови знания и умения, свързани с информацията и медиите в дигитална среда, с начини за анализиране на различни гледни точки в мрежата, с правила за преценка на качеството и достоверността на източниците на данни в интернет. Участниците ще се запознаят и с важни етични правила за поведение и комуникация в дигитална среда.

Въведение в цифровите права

Реализацията на съвременния човек все по-силно зависи от познаването на цифровите технологии на комуникация, труд и управление, образование и обучение, култура и забавление. Ориентацията в цифровите технологии все по-малко е въпрос на личен избор и все повече е част от базовите знания и умения, необходими за нормалното функциониране на обществото в цифровото време.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Целта на този курс е да разшири познанията на служителите в администрацията за комуникационните права, като се акцентира върху основни положения, свързани със защитата на личните данни и личния живот, правата на интелектуална собственост и киберсигурността и хибридните заплахи. Отделя се специално внимание върху специфичните общностни стандарти за социалните мрежи.

Противодействие на дезинформацията

За да участват пълноценно в съвременните комуникационни процеси, държавните служители следва да имат базисна ориентация за източниците на информация, идентифицирането на надеждни и ненадеждни източници, проверката на фактите. Освен това, те носят отговорност за точното и стриктно прилагане на мерките на Европейския съюз за противодействие на дезинформацията и хибридните заплахи. Държавната и общинската администрация не трябва да допуска да бъде използвана като проводник на слухове, дезинформация или конспиративни теории. Курсът представя принципите на противодействие на дезинформацията в цифровото общество, мерките, предприети от Европейския съюз и нормативната рамка, към която при необходимост участниците могат винаги да се обърнат за справка. Ще бъде подложено на анализ и поведението в конкретни ситуации.

Въведение в информационната и киберсигурност (за не IT експерти)

През последното десетилетие, всички хора се оказаха виртуално свързани и голяма част от информацията – личните и професионални данни, се съхраняват и в дигиталната среда (киберпространството). Целта на този курс е участниците да се запознаят с актуални заплахи за информацията и за самите тях, както и методите за защита от най-често използваните техники и тактики за хакване на системите и хората. Курсът поставя акцент върху техническите заплахи и специално проектираните за хората – социално инженерство и дезинформация, с фокус киберсигурността. Базовата грамотност по информационна и киберсигурност е по-важна дори от базовите компютърни умения. Защото, дори и да не се ползва електронна поща, текстообработка или електронни таблици, се използват чат, „умен“ телефон и социални медии. Завършвайки този курс, участниците ще повишат знанията си за киберсигурността за себе си, организацията и семейството си.

Методология за оценка на риска и управление на инциденти, свързани с информационната и киберсигурност

Курсът е фокусиран върху теорията за управление на рисковете и управление на инциденти и е предназначен за всички служители в администрацията, които имат интерес да надградят знанията си за оценка на риска и управление на инциденти. По време на обучението се провежда работилница, в която участниците групово разработват планове за управление на риска.

Киберсигурност – заплахи, защита и киберполигон (за IT експерти)

Киберсигурността е знание, оценка на рисковете, управлението му и постоянна готовност да се реагира при атака и да се управляват правилно инциденти. За това е нужно

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

ИТ експертите да тренират заедно и да участват в симулации. В този курс участниците ще бъдат запознати и ще им бъдат демонстрирани реални заплахи, както и ще им бъдат предложени тактики за наблюдение и управление на инциденти и реакция. Предвиждат се тренировки в киберполигон и симулация на атаки и опит за овладяването им.

С цел ускоряване и широко покритие следва да се предвидят и серия от електронни курсове:

Защита на личните данни в дигитална среда

Този е-модул ще ви запознае с правилата за защита на личните данни в дигитална среда. Включва три основни теми: основни положения в правната уредба, спазване на законови задължения за предоставяне/публикуване на информация и насоки за развитие на европейската уредба.

Социални мрежи в публичния сектор - създаване и управление

Модулът е предназначен за всички служители в администрацията. В него се разглеждат основните социални мрежи, които са актуални в момента (Facebook/Meta; Youtube; LikedIN; Twitter - X), какви са техните специфики, какво е необходимо да се знае и на какво да се обръща внимание за добро присъствие в социалните канали.

Киберсигурност: „Троянски кон“ и социален инженеринг

Как могат да бъдат хакнати както компютри, така и хора, и защо тези два аспекта са основен киберриск в дигиталната ера, в която работим? Това са отговорите, които ще откриете в базовия електронен модул за самообучение. В него ще се запознаете с основните характеристики на „Троянския кон“ и на социалния инженеринг като кибер-заплахи и ще получите съвети, какви добри практики да следвате, за да избегнете тези заплахи и да осигурите сигурността на информацията на работното място.

Нови технологии в управлението - облачни технологии

Модулът е за всички служители в администрацията и цели да ги запознае с възможностите, които облачните технологии предоставят в областта на публичното управление. Ще бъдат разгледани различните приложения на облачните технологии, както в частния, така и в публичния сектор, и ще бъдат коментирани усилията на ЕС за развитие на отворените данни.

Нови технологии в управлението - светът на данните

Модулът е предназначен за всички служители в администрацията и има за цел да представи светът на Големите данни (Big Data). Ще бъдат разгледани теми като: значение то на големите данни, вземане на решения, основани на данни решения в публичното управление, както и ще бъдат разгледани различни платформи за отворени данни, които могат да се използват при проучвания и анализи.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Нови технологии в управлението - изкуствен интелект и машинно учене (модул запознаващ с нововъзникващите технологии – ползи и рискове)

Модулът е за всички служители в администрацията, които желаят да разберат каква е същността на моделите на машинно самообучение. В модула се разясняват основни моменти на машинното обучение, а съдържанието е структурирано в следните главни теми: същност на изкуствения интелект; внедряване на изкуствен интелект; приложения на изкуствения интелект.

Създаването на тези курсове с насоченост цифрови компетенции, ще съдейства за развитие на систематичен подход за разработка на обученията.

За да бъдем реалисти обаче е важно да признаем, че преминалите базовите или електронни курсове са малко под 10 % от държавните служители. Какво можем да направим, за да приложим МИС2 и да изпълним условието на МИС за обучение на персонала:

1. Всички държавни служители да преминат през стандартизиран курс за оценка на базова дигитална грамотност DigiComp.
2. Да се въведе предложението за отделен тест по дигитална грамотност DigiComp или подобрена локална версия за всички новоназначени или мобилни служители. Тестовете по т.1 и 2 да се управляват и обслужват централизирано от ИПА или друг орган с компетенции.
3. Всички обучаващи държавната администрация да преминат оценка на знанията по DigiComp или разработел локален тест, като се съобразят уменията и знанията им с DigiCompEdu.
4. Оценката на знания по т. 1, 2, 3 да се извършва периодично на срок не по-дълъг от 3 години.
5. Да се определят минимални нива за съответните длъжности на държавните служители съгласно класифицирането им.
6. За специалистите по ИТ и отговорниците по МИС да се предвидят отделни пътеки за доказване и поддръжка на знанията и компетенциите, в които да бъда ангажирани БАН и университетите, като процесът се координира от ИПА или друг орган с капацитет.
7. Да се предвидят изпити за доказване на компетентност на изнесените/външни за администрацията доставчици на услуги. В зависимост от предоставените услуги да се предвиди и необходимото ниво на компетентност по DigiComp или друг метод за оценка на компетенции за еквивалентни нива.
8. Данните от действията по т. 1-7 да се събират, непосредствено и централизирано за анализ и изводи по позиции, тип публична администрация или външен доставчик, географско местоположение, риск.
9. Да се извършват извадкови одити на резултатите по методика, определена от ИПА, чрез присъствени изпити или интервюта.
10. С цел изпълнение на критериите по МИС да се актуализира нивото на % обучени и преминали служители.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Ако препоръките ни бъдат реализирани, то в не по-малко от 30 % от администрацията ще успее да се повиши дигиталната компетентност. Следва да се разработи и нова серия от микро курсове с висока степен на адаптиране, като целта за 2025 г. би могла да бъде заложена, като:

Персонализиран подход за учене и проверка на знанията чрез обработка на големи обеми от данни и изкуствен интелект.

Примери за нови подходи при водене на обучения в държавната администрация:

1. Серия от микро курсове от 3-5 минути по актуални ежедневни теми и заплахи
2. Месечен аудио подкаст или анимирани видеа с изкуствен интелект.
3. Ежемесечно провеждане на „добронамерени“ фишинг симулации с изпращане на електронна поща до държавните служители и измерване на резултатите.
4. Анализ на трафика на държавната администрация и идентифициране на несигурни услуги използвани от нея – електронни пощи без двуфакторна идентификация, протоколи с ниско ниво на сигурност (FTP, HTTP, telnet,и др.).
5. Създаване на банка от сценарии за киберполигони и достъп за обучение чрез партниране, чрез концепцията за федерирани киберполигони в ЕС [61](в зависимост от типа обучени и разхода).
6. Създаване на банка от оценките на риска в публичната администрация и чрез анонимизиран достъп до данните - идентифициране на най-вероятните или рискове с най-голямо последствие върху индивидите, обществото и бизнеса (публичната администрация има роля на бизнес субект). Създавайки и анализирайки тези данни може да се въведе непосредствено в обученията за цифрови и др. компетенции елементът оценка на риск и планиране за реакция при реализация на риск.

За да представим, част от тези концепции практически и чрез използване на профилиран и фино обучен модел (GPT 4 – cybersecurity architect private trained model) ще дадем примери на т.4 и 5 и примерни програми. Данните са генерирани на английски език и е използван машинен превод.

По т. 4

Ето и топ 5 киберриск за публичната администрация с голямо въздействие и голяма вероятност, съобразени с българския контекст:

1. Фишинг атаки

Въздействие: Фишинг атаките могат да доведат до неоторизиран достъп до чувствителни правителствени бази данни, компрометиране на лични данни на граждани, финансова информация и класифицирани правителствени данни.

[61] https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

Вероятност: Висока, поради нарастващата сложност на фишинг кампаниите и човешкия фактор е последователна уязвимост.

Примерен случай на употреба: Нападателите се представят за правителствен ИТ отдел в имейли до служителите, подмамвайки ги да въведат идентификационни данни на фалшива страница за вход.

Участници в заплахите: Киберпрестъпни групи, насочени към правителствени ресурси за финансова печалба, шпионаж или прекъсване.

2. Рансъмуер атаки

Въздействие: Критичните системи на публичната администрация могат да бъдат криптирани и да станат недостъпни, което нарушава обществените услуги, води до финансови загуби и изисква скъпи усилия за възстановяване.

Вероятност: Висока, като се има предвид глобалното нарастване на рансъмуер атаките срещу субекти от публичния сектор.

Примерен случай на използване: Системите на местната правителствена служба са криптирани от ransomware, спирайки всички цифрови услуги и изисквайки откуп за декриптиране на данни.

Участници в заплахите: Киберпрестъпни синдикати, специализирани в рансъмуер за финансово изнудване или спонсорирани от държавата участници, които се стремят да дестабилизират правителствените операции.

3. Вътрешни заплахи

Въздействие: Злонамерени или небрежни действия от вътрешни лица могат да разкрият чувствителна информация, да улеснят неоторизиран достъп и да компрометират националната сигурност.

Вероятност: Висока, поради огромния набор от фактори, свързани с човека, и потенциала за недоволни служители или тези, принудени от външни участници.

Примерен случай на употреба: Недоволен служител изтича чувствителни фискални данни към неупълномощени страни, което води до масивно нарушение на данните.

Участници в заплахата: Недоволни служители, изпълнители или други вътрешни лица с достъп до мрежите и данните на организацията.

4. DDoS атаки

Въздействие: Разпределените атаки за отказ на услуга (DDoS) могат да направят правителствените уебсайтове и онлайн услуги недостъпни, нарушавайки достъпа на гражданите до информация и услуги.

Вероятност: Висока, тъй като тези атаки изискват сравнително ниски технически умения, но могат да причинят значителни смущения.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Примерен случай на използване: Критичните портали за обществени услуги са претоварени от трафик от координирана DDoS атака, което ги прави недостъпни по време на решаващ период на гласуване.

Участници в заплахите: Хактивистки групи, чуждестранни държавни участници или киберпрестъпници, които искат да нарушат правителствените операции или да протестират срещу политиките.

5. Разширени постоянни заплахи (APT)

Въздействие: APT включват продължителни и целенасочени операции за кибершпионаж, които могат да доведат до кражба на класифицирана информация, шпионаж и дългосрочно компрометиране на правителствени мрежи.

Вероятност: Висока за правителствените субекти поради високата стойност на политическото, военното и икономическото разузнаване.

Примерен случай на употреба: Чуждестранно правителство спонсорира кампания за APT, която прониква в системите за национална сигурност, оставайки незабелязана в продължение на месеци, докато ексфилтрира чувствителни данни.

Участници в заплахите: Спонсорирани от държавата участници или сложни киберпрестъпни групи, участващи в шпионаж или саботаж за стратегическо предимство.

Тези рискове подчертават необходимостта от всеобхватни стратегии за киберсигурност, включително обучение на служителите относно осведомеността за фишинга, строг контрол на достъпа, редовни оценки на сигурността, планиране на реакцията при инциденти и международно сътрудничество по отношение на заплахите за киберсигурността. Като се има предвид стратегическата позиция на България в Европа и интегрирането ѝ в инициативите на ЕС за киберотбрана, сътрудничеството на равнище ЕС може също така да засили националните усилия в областта на киберсигурността.

За да превърнем едната от заплахите в сценарий за киберполигон продължаваме с избрана от нас тема, а именно:

Използвайки следната информация… създай сценарий за киберполигона, като го направиш стъпка по стъпка както е зададено описанието на архитектура – киберполигона.

Сценария е по тематика : Рансъмуер атаки

Фиктивна ситуация

Представете си местната правителствена служба, която управлява критични обществени услуги - от регистрация на граждани до управление на здравеопазването и образованието. Тази инфраструктура е цифровизирана, за да предоставя по-ефективни услуги. Въпреки това, киберпрестъпници от синдикат, специализиран в рансъмуер атаки, са идентифицирали уязвимости в мрежата на правителствената служба. Те планират атака, целяща криптиране на критични системи и изискване на откуп за тяхното декриптиране.

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Атаката започва с внимателно планиране и диагностициране, за да се идентифицират слабите места. След като се получи достъп, зловреднят софтуер се разпространява в цялата мрежа, криптирайки файлове и изключвайки жизненоважни услуги. Публичната администрация е принудена да спре всички цифрови услуги, което води до сериозни обществени и финансови последствия. За да възстанови достъпа до своите системи, тя трябва или да плати откуп, или да вложи значителни ресурси във възстановяването на данните.

MITRE ATT&CK рамка

1. **Разузнаване**:
   - **Техника**: Публично събрана информация (T1590)
   - **Описание**: Атакуващите използват отворени източници, за да наблюдават и анализират системите и мрежите на целта, идентифицирайки уязвимости.
2. **Развитие на ресурси**:
   - **Техника**: Придобиване на зловреден софтуер (T1587)
   - **Описание**: Атакуващите разработват или придобиват рансъмуер за използване в атаката.
3. **Първоначален достъп**:
   - **Техника**: Фишинг през електронна поща (T1566)
   - **Описание**: Атакуващите изпращат зловредни електронни писма на служители в правителствената агенция, за да получат достъп.
4. **Изпълнение**:
   - **Техника**: Скриптове (T1059)
   - **Описание**: Зловреднят код се изпълнява в засегнатите системи, започвайки процеса на криптиране.
5. **Установяване на устойчиво присъствие**:
   - **Техника**: Използване на автостарт техники (T1547)
   - **Описание**: Рансъмуерът се конфигурира да се стартира при всяко стартиране на системата, за да се гарантира постоянството на криптирането.
6. **Ескалация на привилегиите**:
   - **Техника**: Експлоатация на уязвимост (T1068)
   - **Описание**: Атакуващите експлоатират уязвимости в софтуера, за да получат повишени привилегии.
7. **Избягване на защита**:
   - **Техника**: Обфускация (T1027)
   - **Описание**: Зловреднят софтуер е обфускиран, за да избегне откриването от антивирусни програми.
8. **Достъп до потребителски данни**:
   - **Техника**: Кражба на удостоверения (T1056)

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- **Описание**: Атакуващите събират кредeнции, за да разширят достъпа си в мрежата.

9. **Откриване**:
   - **Техника**: Сканиране на мрежата (T1046)
   - **Описание**: Атакуващите сканират мрежата, за да идентифицират допълнителни цели за криптиране.
10. **Хоризонтално движение**:
    - **Техника**: Пасивно проследяване (T1021)
    - **Описание**: Използват се съществуващи мрежови връзки, за да се разпространи рансъмуерът в мрежата.
11. **Събиране**:
    - **Техника**: Данни от информационни панели (T1213)
    - **Описание**: Атакуващите събират важни файлове преди криптирането, за да увеличат натиска за плащане на откуп.
12. **Командване и контрол**:
    - **Техника**: Мултиплексиран протокол (T1095)
    - **Описание**: Управлението на зловредния софтуер се осъществява през шифровани канали.
13. **Извличане на инфорамция**:
    - **Техника**: Ексфилтрация чрез приложение (T1567)
    - **Описание**: Чувствителни данни се изпращат към атакуващите преди криптирането.
14. **Въздействие**:
    - **Техника**: Деструктивен малуер (T1485)
    - **Описание**: Криптирането на файлове води до недостъпност на критични системи и услуги.

Продължавайки с подготовката на симулацията в киберполигона получаваме и данни за нужните активи за обучението:

Инвентарен лист за симулационната среда

За създаване на реалистична симулационна среда на кибер полигон, където може да се проведе обучение по сценарий за рансъмуер атака, ще са необходими следните елементи:

1. **Виртуални машини (ВМ)**:
   - Сървъри за имитация на публични административни услуги.
   - Работни станции за служители на публичната администрация.
2. **Софтуер**:
   - Операционни системи (Windows/Linux) за ВМ.
   - Електронна поща и офис приложения за имитация на работен процес.
   - Защитен софтуер (антивирусна програма, фаеруол) за демонстрация на методи за защита и евентуално заобикаляне.
   - Инструменти за мониторинг и анализ на мрежовия трафик.
3. **Мрежова инфраструктура**:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

- Суичове, рутери и фаеруоли за създаване на сегментирана мрежа.
- VPN за симулиране на отдалечен достъп.

4. **Уязвимости**:
   - Настройки на уязвим софтуер и операционни системи, които могат да бъдат експлоатирани.

И като финал на проекта за полигонен сценарий ще поискаме примерен скрипт за инициализиране на виртуалната среда :

Симулационна среда на кибер полигон

За създаването на виртуална структура на кибер полигон, която да позволява провеждането на обучение по описания сценарий, е необходим скрипт за Terraform. Скриптът ще автоматизира процеса на разгръщане на виртуалните машини, мрежовите компоненти и настройките за сигурност, които са необходими за симулацията.

```
# Примерен Terraform скрипт за симулационна среда
provider "aws" {
  region = "eu-central-1"
}

resource "aws_instance" "public_admin_server" {
  ami           = "ami-0c02fb55956c7d316" # Примерен AMI за Linux
  instance_type = "t2.medium"
  key_name      = "public-admin-keypair"
  security_groups = ["public_admin_sg"]

  tags = {
    Name = "Public Admin Server"
  }
}

resource "aws_security_group" "public_admin_sg" {
  name        = "public_admin_sg"
  description = "Allow inbound traffic for public admin services"

  ingress {
    from_port   = 80
    to_port     = 80
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}
```


Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

За да успеем да обобщим ефекта от такъв сценария са важни познанията за придобити умения и знания, като скриптът на обучения генеративен интелект, дава следните:

Обучение и умения

След завършване на обучението, участниците ще придобият следните умения и знания:

- Разбиране на тактики, техники и процедури (TTPs) използвани от киберпрестъпниците при рансъмуер атаки.
- Умения за идентифициране и анализ на уязвимости, които могат да бъдат експлоатирани.
- Практически умения за използване на инструменти за защита и мониторинг.
- Опит в реагирането на инциденти и възстановяването след атаки.
- Знания за подходящи стратегии за защита и предотвратяване на бъдещи атаки

Извод: с придобиване на повече информация, успешното обучение на моделите и въвеждането на общ федеративен формат за киберполигони ще можем да развием частните модели и да прилагаме индивидуален подход за всяко обучение в контекста на информационната и кибер сигурност след валидация от експерт.

т.5.Задача:

Избери три актива софтуер, хардуер и човешки ресурси и идентифицирай по една заплаха за всеки от тях. Опитай да идентифицираш по три слабости, които могат да я реализират, като вземеш предвид контекста: Разширени постоянни заплахи (APT) Въздействие: APT включват продължителни и целенасочени операции за кибершпионаж, които могат да доведат до кражба на класифицирана информация, шпионаж и дългосрочно компрометиране на правителствени мрежи. Вероятност: Висока за правителствените субекти поради високата стойност на политическото, военното и икономическото разузнаване. Примерен случай на употреба: Чуждестранно правителство спонсорира кампания за APT, която прониква в системите за национална сигурност, оставайки незабелязана в продължение на месеци, докато ексфилтрира чувствителни данни. Участници в заплахите: Спонсорирани от държавата участници или сложни киберпрестъпни групи, участващи в шпионаж или саботаж за стратегическо предимство.

Подреди активите, заплахите и слабостите в таблица, като предложиш стойност за оценка на въздействие и ефект и изчислиш риск по формулата Риск = Вероятност * Ефект / 10.

На база тази стойност реализирай качествена оценка на риска в нова колона, като сам определиш нисък, среден и висок и обясниш границите.

Генерираният табличен резултат е:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

Актив	Слабост	Вероятност	Ефект	Риск	Риск (числово)
Софтуерен актив: Система за управление на бази данни	Неправилно управление на сесии	7	8	Среден	5.6
Софтуерен актив: Система за управление на бази данни	Некриптиран трафик	6	9	Среден	5.4
Софтуерен актив: Система за управление на бази данни	Използване на стандартни администраторски пароли	8	7	Среден	5.6
Хардуерен актив: Мрежови устройства	Физически достъп до устройството	4	9	Нисък	3.6
Хардуерен актив: Мрежови устройства	Уязвимости във фърмуера	5	8	Нисък	4.0
Хардуерен актив: Мрежови устройства	Неактуализирани устройства	7	6	Среден	4.2
Човешки ресурс: IT Администратор	Липса на обучение по сигурност	7	8	Среден	5.6
Човешки ресурс: IT Администратор	Преумора и претоварване	8	7	Среден	5.6
Човешки ресурс: IT Администратор	Ползване на слаби пароли	9	6	Среден	5.4

А критериите за оценка на качествения риск са :

- **Нисък риск**: Резултат до 4.0
- **Среден риск**: Резултат между 4.1 и 6.0
- **Висок риск**: Резултат над 6.0

За да можем да реализираме качествен процес на усещане и пресъздаване на риска, би било подходящо всички теми в контекста на придобиване на умения и знания да бъдат подкрепени с визуализацията, в анимация или видео. Към момента тази технология е ограничена, но ще дадем пример с автоматично генериран комикс по горния сценарий в 5 страници:

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд


CYBERGUARDIANS
THE UNITY PROTOCCOL
TOGETHER, WE SECURE TOMORROW

ЗАКЛЮЧЕНИЕ

Сред държавите членки има значителни опасения и дискусии относно обхвата на преразгледаните правила, критериите за определяне на съществените и важните субекти и последиците от новото правно основание на МИС2. Директивата е приета и България трябва да я транспонира в националното си право до 17 октомври 2024 г.

България е изправена пред предизвикателството да се адаптира към по-взискателните и всеобхватни изисквания на директивата за МИС2. Подготвеността на държавата ще зависи от способността и ефективно да прилага по-строги мерки, да хармонизира националното си законодателство с разширения обхват и изисквания и да отстрани установените недостатъци и несъответствия на предишната директива. В заключение прилагаме някои от основните стъпки, които биха били ключови по отношение на по-добра система за киберсигурност в България:

Пълна ангажираност и подкрепата на висшето ръководство във всяка една структура: Признаване на важността на директивата и осигуряване на активна ангажираност от най-високите нива в организацията ще позволи да се избегнат бавни, недостатъчно финансирани и затруднени процеси на изпълнение.

Установяване на управление на проекта по въвеждане на МИС2: Подчертаване на сложността на внедряването на NIS 2, което изисква формализиран проектен подход с ясни стъпки, фази, резултати и отговорности за успешно изпълнение.

Провеждане на първоначално обучение: Необходимостта от обучение по киберсигурност на ранен етап за всички участници, за да се осигури цялостно разбиране на изискванията и целите на NIS 2.

Създаване на политики за сигурност на високо ниво: Разработване на вътрешна политика, определяща насоките на киберсигурността, основните роли, отговорности и показатели за успех, в съответствие с международните стандарти.

Определяне на методология за управление на риска: Разглеждане на сложните и специфични изисквания за управление на риска съгласно NIS 2, като се гарантира, че цялата организация разбира и спазва тези протоколи.

Оценка и намаляване на риска: Идентифициране на заплахите и уязвимостите на информационните системи, оценяване на рисковете и приоритизиране на мерките за намаляване на риска въз основа на задълбочен анализ, а не на ad-hoc прилагане.

Създаване и одобряване на план за управление на риска: Разработване и получаване на одобрение от ръководството на подробен план за справяне с идентифицираните рискове с конкретни мерки за киберсигурност, отговорности и срокове.

Прилагане на мерки за киберсигурност: Прилагане на различни мерки за контрол въз основа на резултатите от оценката на риска, което изисква създаването на нови процеси, дейности, а в някои случаи и технологии.

Защита на веригата на доставчици на услуги: Признаване на нарастващия брой инциденти, свързани с пробиви в сигурността, стандартизация (сертифициране) на

Проект BG05SFOP001-2.017-0001/28.11.2019 г. „Дигитална трансформация в обучението - дигитална компетентност и учене“, финансиран от Оперативна програма „Добро управление“, съфинансирана от Европейския съюз чрез Европейския социален фонд

доставчиците на IT услуги и подчертаване на необходимостта от строга оценка на рисковете от доставчици на услуги, осигуряване на сигурни практики за сътрудничество и мрежи.

Мониторинг и оценка на ефективността на киберсигурността: Наблюдение на прилагането на мерките за сигурност чрез непрекъснато измерване, периодични вътрешни одити и прегледи от ръководството.

Подход за непрекъснато обучение по киберсигурност: Гарантиране, че целият персонал на всяка административна структура, включително висшите държавни служители, получават подходящо, ефективно и ресурсно ефективно обучение по теми, свързани с киберсигурността, които са от значение за техните роли и отговорности.