Рамка за подобряване на киберсигурността на критичната инфраструктура

Версия 1.1

Национален институт по стандарти и технологии

16 април 2018 г.

Превод: проф. Владимир Димитров, ФМИ, СУ „Св. Климент Охридски".

Научен редактор: проф. Калинка Калоянова, ФМИ, СУ „Св. Климент Охридски".

Преводът е финансиран от Национална научна програма ИКТвНОС, Компонент 3.

Translation: Prof. Vladimir Dirnitrov, FMI, University of Sofia "St. Kliment Ohridski".

Scientific editor: Prof. Kalinka Kaloyanova, FMI, University of Sofia "St. Kliment Ohridski".

Translation is funded by the National Scientific Program "Information and Communication Technologies for Digital Single Market in Science, Education and Security", Component 3.

Бележки за читателите относно актуализираната информация

Версия 1.1 на настоящата Рамка за киберсигурност детайлизира, изяснява и подобрява Версия 1.0, която излезе през февруари 2014 г. В нея са отразени коментарите, получени за двете проектоверсии на Версия 1.1.

Версия 1.1 е предназначена да бъде изпълнявана както от нови, така и от вече налични нейни потребители. Последните ще могат да изпълняват Версия 1.1 с минимални или никакви затруднения; съвместимостта с Версия 1.0 беше една от изрично поставените цели.

Следната таблица обобщава направените промени между Версия 1.0 и Версия 1.1.

Таблица NTR: Обобщение на промените при сравнение на Версия 1.0 и Версия 1.1.

Актуализация	Описание на актуализацията
Изяснено е, че термини като „съвместимост“ могат да доведат до объркване, тъй като означават нещо много различно за различните заинтересовани страни от Рамката	Добавено е пояснение, че Рамката е полезна като структура и език за организиране и изразяване на съвместимост със собствените изисквания за киберсигурност на дадена организация. Разнообразните начини, по които Рамката може да бъде използвана от дадена организация обаче означават, че изрази като „съвместимост с Рамката“ могат да бъдат объркващи.
Нов раздел за самооценка	Добавен е Раздел 4.0, *Самооценка на свързания с киберсигурността риск с помощта на Рамката*, за да се изясни начина, по който Рамката може да бъде използвана от организациите за разбиране и оценяване на свързания с киберсигурността риск, включително използването на измервания.
Значително е разширено обяснението за използване на Рамката за целите на управлението на риска за киберсигурността във веригите на доставки	Разширеният Раздел 3.3, *Уведомяване на заинтересованите страни относно изискванията за киберсигурност,* помага на потребителите по-добре да разберат управлението на риска за киберсигурността във веригите на доставки (Supply Chain Risk Management (SCRM)), а новият Раздел 3.4, *Решения за покупка,* поставя ударение върху използването на Рамката в разбирането на риска, свързан с предлаганите на пазара готови продукти и услуги. Добавени са и допълнителни критерии за Кибер SCRM към Нивата на изпълнение. И най-накрая, към Ядрото на Рамката е добавена Категория, „Управление на риска във веригите на доставки", включваща няколко Подкатегории.
Усъвършенстване с цел подобряване на отчетността при удостоверяване, разрешаване и доказване на идентичността	Текстът на Категорията „Контрол на достъпа“ е усъвършенстван с цел подобряване на отчетността при удостоверяване, разрешаване и доказване на идентичността. Това включва добавяне на Подкатегории за удостоверяване и доказване на идентичността. Също така самата Категория е преименувана на „Управление на идентичността и контрол на достъпа“, за да бъде представен по-добре обхватът на Категорията и на съответните ù Подкатегории.
Подобрено е изясняването на връзката между Нивата на изпълнение и Профилите	Добавен е текст към Раздел 3.2, *Установяване или подобряване на програма за киберсигурност,* за използване на Нивата на Рамката при изпълнение на Рамката. Добавен е текст към Нивата на Рамката за отразяване на интеграцията на мерките

	на Рамката с програмите за управление на риска на организациите. Концепциите за Нивата на Рамката също са усъвършенствани. Фигура 2.0 е актуализирана така, че да включва действия от Нивата на Рамката.
Съображения за координирано разкриване на уязвимости	Добавена е Подкатегория, свързана с жизнения цикъл на разкриването на уязвимости.

Както и при Версия 1.0, така и при Версия 1.1, потребителите се насърчават да персонализират Рамката за постигане на максимална стойност за всяка отделна организация.

Благодарности

Тази публикация е резултат от непрекъснато сътрудничество между индустрията, академичните среди и държавата. Националният институт по стандарти и технологии (The National Institute of Standards and Technology (NIST)) стартира проекта, като събира организации от частния и публичния сектор и отделни експерти през 2013 г. Публикувана през 2014 г. и ревизирана през 2017 г. и 2018 г., тази *Рамка за подобряване на киберсигурността на критичната инфраструктура* е базирана на обсъждания на 8 публични работни срещи, в множество заявки за коментар или информация и хиляди директни разговори със заинтересовани страни от всички сектори на Съединените щати, както и с много индустриални сектори от целия свят.

Тласъкът за изменение на Версия 1.0 и промените, които се направиха във Версия 1.1, се базира на:

- Обратната връзка и често задавани въпроси към NIST след излизането на Версия 1.0 на Рамката;
- 105-те отговора на Искането за предоставяне на информация (Request For Information (RFI)) от декември 2015 г., *Виждания за Рамката за подобряване на киберсигурността на критичната инфраструктура (Views on the Framework for Improving Critical Infrastructure Cybersecurity)*;
- Повече от 85 коментара върху предложената втора проектоверсия на Версия 1.1 от 5 декември 2017 г.;
- Повече от 120 коментара върху предложената първа проектоверсия на Версия 1.1 от 10 януари 2017 г.;
- Мненията от над 1200 участници в работните срещи за обсъждане на Рамката през 2016 г. и 2017 г.

Освен това преди това издадената от NIST Версия 1.0 на Рамката за киберсигурност със съпровождащ документ *Пътна карта на NIST за подобряване на киберсигурността на критичната инфраструктура (NIST Roadmap _for Improving Critical Infrastructure Cybersecurity)*. Тази пътна карта обръща внимание на „ключови области за подобрение“ за по-нататъшно развитие, привеждане в съответствие и сътрудничество. С усилията на частния и публичния сектор, някои области на подобрение бележат достатъчно голям напредък, за да бъдат включени във Версия 1.1 на Рамката.

NIST е признателен и благодари на всички, които допринесоха за разработването на тази Рамка.

Изпълнително резюме

Съединените щати зависят от надеждното функциониране на критичната инфраструктура. Заплахите за киберсигурността се възползват от повишената сложност и свързаност на системите на критичните инфраструктури и излагат на риск националната сигурност, икономика, обществена безопасност и здраве. Подобно на финансовите рискове и рисковете за репутацията, рисковете за киберсигурността влияят върху нетните приходи на компаниите. Те могат да увеличат разходите и да засегнат приходите. Рисковете за киберсигурността могат да повлияят отрицателно върху способността на организациите да иновират, да привличат и да задържат клиенти. Киберсигурността може да бъде важен компонент с нарастващо значение за цялостното управление на риска за организацията.

За да справи по-добре с тези рискове, законът за подобряване на киберсигурността (Cybersecurity Enhancement Act (CEA)) от 2014 г.[1] актуализира ролята на Националния институт по стандарти и технологии (NIST), като добави рамки за идентифициране и разработване на рискове за киберсигурността, за да бъдат използвани доброволно от собственици и оператори на критични инфраструктури. С помощта на CEA, NIST трябва да представи „приоритизиран, гъвкав, повторяем, базиран на изпълнението и ефективен по отношение на разходите подход, включващ мерки за информационна сигурност и начини на контрол, които могат да бъдат възприети доброволно от собствениците и операторите на критични инфраструктури, който да им помогне да идентифицират, оценяват и управляват рисковете за киберсигурността“. Така се формализира предходната работа на NIST при разработването на Версия 1.0 на Рамката на базата на Изпълнителна заповед 13636 (Executive Order (EO) 13636), „Подобряване на киберсигурността на критичната инфраструктура“ ("Improving Critical Infrastructure Cybersecurity") (февруари 2013 г.) и се дават насоки за бъдещо развитие на Рамката. Рамката, която беше разработена на базата на EO 13636, и продължава да се развива на базата на CEA, използва общ език за адресиране и управление на риска за киберсигурността по рентабилен начин, базиран на нуждите на бизнеса и организациите, без да поставя допълнителни регулаторни изисквания към бизнеса.

Рамката се фокусира върху използването на двигатели на бизнеса, които да ръководят дейностите по киберсигурността, и разглежда рисковете за киберсигурността като част от процесите за управление на риска на организацията. Рамката се състои от три части: Ядро на Рамката, Нива на изпълнение и Профили на Рамката. Ядрото на Рамката представлява съвкупност от дейности по киберсигурността, резултати и Информативни референтни източници, които са общи за секторите и критичната инфраструктура. Елементите от Ядрото съдържат подробни указания за разработване на индивидуални Профили на организациите. Чрез използването на Профили Рамката помага на дадена организация да хармонизира и приоритизира своите дейности по киберсигурността съгласно изискванията на своя бизнес/мисия, толерантност към риска и ресурси. Нивата предоставят на организациите механизъм, с помощта на който ще могат да видят и да разберат характеристиките на техния подход към управлението на рисковете за киберсигурността, което ще им помогне да приоритизират и постигнат нейните цели.

Въпреки, че този документ беше разработен с цел подобряване на управлението на риска за киберсигурността в критичната инфраструктура, Рамката може да се използва от организации във всички сектори и общности. Тя позволява на организациите – независимо от размера, степента на риска за киберсигурността или нивото

[1]Вижте 15 U.S.C. § 272(e)(1)(A)(i). Законът за подобряване на киберсигурността (The Cybersecurity Enhancement Act) от 2014 г. (S.1353) става закон 113-274 на 18 декември 2014 г. и може да бъде намерен на: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

на сложност на киберсигурността – да прилагат принципите и най-добрите практики за управление на риска за подобряване на сигурността и устойчивостта.

Рамката предоставя обща организационна структура за множество подходи към киберсигурността, като съчетава стандарти, насоки и практики, които действат ефективно в момента. Нещо повече, понеже се позовава на широко признати стандарти за киберсигурност, Рамката може да служи като модел за международно сътрудничество за укрепване на киберсигурността не само в критичната инфраструктура, но и в други сектори и общности.

Рамката предлага гъвкав подход към справяне с проблемите на киберсигурността, включително и ефекта на киберсигурността върху физическите, кибер и човешките измерения. Тя е приложима за организации, базирани на технологиите, независимо дали фокусът им върху киберсигурността е насочен основно към информационните технологии (IT), системите за промишлен контрол (ICS), кибер-физичните системи (CPS) или свързаните устройства в по-общ смисъл, включително и Интернет на нещата (IoT). Рамката може да помогне на организациите да се справят с проблемите на киберсигурността, тъй като тя влияе върху поверителността на клиентите, служителите и трети страни. Освен това, резултатите от Рамката служат като цели на дейностите за развитие и еволюция на работната сила.

Рамката не е един, подходящ за всички, подход,към управлението на риска за киберсигурността за критичната инфраструктура. Организациите ще продължат да се срещат с уникални рискове – различни заплахи, различни уязвимости и различна толерантност към риска. Те също така ще се различават и по начините, по които ще персонализират практиките, описани в Рамката. Организациите могат да определят дейности, които са важни за доставката на услуги от критично значение, и могат да приоритизират инвестициите, за да постигнат максимална ефективност от всеки похарчен долар. В крайна сметка, Рамката е насочена към намаляване на рисковете за киберсигурността и по-доброто им управление.

За да бъдат отчетени уникалните потребности от киберсигурност на организациите, се използват много разнообразни начини на приложение на Рамката. Решението за начина, по който тя трябва да се прилага, се предоставя на прилагащата я организация. Например една организация може да реши да използва Нивата на изпълнение на Рамката, за да формулира предвидените практики за управление на риска. Друга организация може да използва петте Функции на Рамката, за да анализира цялото си портфолио за управление на риска, като този анализ може да бъде или да не бъде базиран на по-подробни придружаващи насоки като каталози на контролите. Понякога има дискусии относно „съвместимостта“ с Рамката, която е средство със структура и език за организиране и изразяване на съвместимост със собствените изисквания за киберсигурност на организацията. Но разнообразието от начини, по които Рамката може да бъде използвана от дадена организация, означава, че изрази като „съвместимост с Рамката“ могат да бъдат объркващи и да означават нещо много различно за различните заинтересовани страни.

Рамката е жив документ и ще продължи да бъде актуализирана и подобрявана чрез обратната връзка, която индустрията ще предоставя за нейното изпълнение. NIST ще продължи координацията с частния сектор и правителствените агенции на всички нива. С разширяването на практиката на прилагането на Рамката, допълнителните уроци, които ще бъдат научени, ще бъдат интегрирани в бъдещите версии. Това ще гарантира, че Рамката удовлетворява потребностите на собствениците и операторите на критична инфраструктура в една динамична и пълна с предизвикателства среда от нови заплахи, рискове и решения.

Разширеното и по-ефективно използване на Рамката и споделянето на най-добрите практики при доброволното ѝ прилагане са следващите стъпки в подобряването на киберсигурността на нашата национална критична инфраструктура. Рамката предоставя развиващи се насоки за отделните организации, като същевременно увеличава силата на киберсигурността на критичната инфраструктура на страната и на икономиката и обществото в по-общ смисъл.

Таблица на съдържанието

Списък на фигурите

Списък на таблиците

1.0 Въведение в Рамката

Съединените щати зависят от надеждното функциониране на критичната си инфраструктура. Заплахите за киберсигурността се възползват от повишената сложност и свързаност на системите на критичните инфраструктури и излагат на риск националната сигурност, икономика, обществена безопасност и здраве. Подобно на финансовите рискове и рисковете за репутацията, рисковете за киберсигурността влияят върху нетните приходи на компаниите. Те могат да увеличат разходите и да засегнат приходите. Рисковете с киберсигурността могат да повлияят отрицателно върху способността на организациите да иновират, да привличат и да задържат клиенти. Киберсигурността може да бъде важен компонент с нарастващо значение в цялостното управление на риска в организацията.

За да укрепи устойчивостта на тази инфраструктура, законът за подобряване на киберсигурността (Cybersecurity Enhancement Act (CEA)) от 2014 г.[2] актуализира ролята на Националния институт по стандарти и технологии (National Institute of Standards and Technology (NIST)) с цел „улеснение и подпомагане разработването на“ рамки за риска за киберсигурността. С помощта на CEA, NIST трябва да представи „приоритизиран, гъвкав, повторяем, базиран на изпълнението и ефективен по отношение на разходите подход, включващ мерки за информационна сигурност и начини на контрол, които могат да бъдат възприети доброволно от собствениците и операторите на критични инфраструктури, който да им помогне да идентифицират, оценяват и управляват рисковете за киберсигурността“. Така се формализира предходната работа на NIST при разработването на Версия 1.0 на Рамката на базата на Изпълнителна заповед 12636 (Executive Order 13636), „Подобряване на киберсигурността на критичната инфраструктура“ ("Improving Critical Infrastructure Cybersecurity"), публикувана през февруари 2013 г.[3], и се дават насоки за бъдещо развитие на Рамката.

Критичната инфраструктура[4] е дефинирана в американския Патриотичен акт (Patriot Act) от 2001 г.[5] като „системи и активи, физически или виртуални, толкова жизненоважни за Съединените щати, че непригодността или разрушаването на тези системи и активи биха оказали омаломощаващо въздействие върху сигурността, сигурността на националната икономика, националното обществено здраве или безопасност, или всяка комбинация от тях“. Поради нарастващия натиск от външни и вътрешни заплахи, организациите, отговорни за критичната инфраструктура, трябва да имат цялостен и итеративен подход към идентифицирането, оценяването и управляването на рисковете за киберсигурността. Този подход е необходим, независимо от размера на организацията, излагането ѝ на заплахи или нивото на сложност на киберсигурността днес.

Общността на критичната инфраструктура включва публични и частни собственици, оператори и други субекти с роля в осигуряването на националната инфраструктура. Членове от всеки сектор на критичната инфраструктура изпълняват функции, които са поддържани от широката категория на технологиите включително информационните технологии (IT), системите за промишлен контрол (ICS), кибер-физичните

[2] Виж 15 Код на САЩ № 272(д)(1)(А)(и). Законът за подобряване на киберсигурността от 2014 г. (S.1353) става публичен закон 113-274 на 18 декември 2014 г. и може да бъде намерен на: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Изпълнителна заповед № 13636, *Подобряване на киберсигурността на критичната инфраструктура*, DCPD-201300091, 12 февруари 2013 г. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] Програмата за критичната инфраструктура на Департамента за вътрешна сигурност (DHS) предоставя списък със секторите и асоциираните с тях критични функции и вериги на стойността. http://www.dhs.gov/critical-infrastructure -sectors

[5] Вижте 42 Код на САЩ № 5195в(д)). Американският Патриотичен акт от 2001 г. (H.R.3162) става публичен закон 107-56 на 26 октомври 2001 г. и може да бъде намерен на: https://www.congress.gov/bill/107th-congress/house-bill/3162

системи (CPS) и свързаните устройства в по-общ смисъл, включително Интернет на нещата (IoT). Тази зависимост от технологиите, комуникациите и взаимосвързаността промени и разшири потенциалните уязвимости, и увеличи потенциалния риск за операциите. Така например, тъй като технологиите и данните, които те произвеждат и обработват, все повече се използват за предоставянето на услуги от критично значение и в подкрепа на решенията за бизнеса/мисията, трябва да се вземат под внимание потенциалните въздействия на инцидентите, засягащи киберсигурността, върху организацията, здравето и безопасността на отделните лица, околната среда, общностите и икономиката и обществото в по-широк смисъл.

За да бъдат управлявани рисковете за киберсигурността, се изисква ясно разбиране за двигателите на бизнеса на организацията и съображенията за сигурността, които са специфични за начина, по който тя използва технологиите. Тъй като рисковете, приоритетите и системите на всяка една организация са уникални, използваните инструменти и методи за постигане на резултатите, описани от Рамката, ще бъдат различни.

Признавайки ролята, която защитата на неприкосновеността и гражданските свободи играе за създаването на по-голямо обществено доверие, Рамката включва методология за защита на личната неприкосновеност и гражданските свободи при провеждането на дейности по киберсигурността от организациите от критичната инфраструктура. Много организации вече разполагат с процеси, адресиращи поверителността и гражданските свободи. Предназначението на методологията е да допълни такива процеси и да осигури насоки за улесняване на управлението на риска за поверителността, съответни на подхода на организацията към управлението на риска за киберсигурността. Интегрирането на поверителността с киберсигурността може да бъде от полза за организациите, тъй като увеличава доверието на клиентите чрез възможността за по-стандартизирано споделяне на информация и чрез опростяване на операциите при правните режими.

Рамката остава ефективна и поддържа техническите иновации, понеже е технологично неутрална и едновременно с това се позовава на многообразие от съществуващи стандарти, насоки и практики, които еволюират с технологиите. Основавайки се на тези глобални стандарти, насоки и практики, разработени, управлявани и актуализирани от индустрията, наличните за постигане на резултатите на Рамката инструменти и методи ще преминат границите, ще признаят глобалната природа на рисковете за киберсигурността и ще еволюират заедно с технологичния напредък и изискванията на бизнеса. Използването на съществуващи и възникващи стандарти ще позволи икономии от мащаба и ще стимулира разработването на ефективни продукти, услуги и практики, които ще удовлетворят идентифицирани нужди на пазара. Пазарната конкуренция също стимулира по-бързото разпространение на тези технологии и практики и реализирането на много ползи от заинтересованите страни в тези сектори.

Градейки върху тези стандарти, насоки и практики, Рамката предоставя обща таксономия и механизъм на организациите, за да:

1) опишат текущото състояние на своята киберсигурност;
2) опишат целевото състояние на своята киберсигурност;
3) идентифицират и приоритизират възможности за подобрения в контекста на непрекъснат и повторяем процес;
4) оценят прогреса към целевото състояние;
5) комуникират с вътрешни и външни заинтересовани страни по въпроси на риска за киберсигурността.

Рамката не е универсален, подходящ за всички подход,към управлението на риска за киберсигурността за критичната инфраструктура. Организациите ще продължат да се срещат с уникални рискове – различни заплахи, различни уязвимости и различна толерантност към риска. Те също така ще се различават и по начините, по които ще прилагат практиките, описани в Рамката. Организациите могат да определят дейности, които са важни за доставката на услуги от критично значение, и могат да приоритизират инвестициите с цел

постигане на максимална ефективност от всеки похарчен долар. В крайна сметка, Рамката е насочена към намаляване на рисковете за киберсигурността и по-доброто им управление.

За да бъдат отчетени уникалните потребности от киберсигурност на организациите, се използват разнообразни начини на приложение на Рамката. Решението за начина, по който тя трябва да се прилага, е предоставено на прилагащата я организация. Например една организация може да използва Нивата на изпълнение на Рамката, за да формулира предвидените практики за управление на риска. Друга организация може да използва петте Функции на Рамката, за да анализира цялото си портфолио за управление на риска, като този анализ може да бъде или да не бъде базиран на по-подробни придружаващи насоки като каталозите на контролите. Понякога има дискусии относно „съвместимостта“ с Рамката, която е средство със структура и език за организиране и изразяване на съвместимост със собствените изисквания за киберсигурност на организацията. Но разнообразието от начини, по които Рамката може да бъде използвана от дадена организация, означава, че изрази като „съвместимост с Рамката“ могат да бъдат объркващи и да означават нещо много различно за различните заинтересовани страни.

Рамката допълва, а не замества процеса на управление на риска и програмата за киберсигурност на дадена организация. Тя може да използва текущите си процеси и да използва Рамката за идентифициране на възможности за укрепване и комуникиране на своето управление на риска за киберсигурността, докато се привежда в съответствие с индустриалните практики. Като алтернатива, организация без съществуваща програма за киберсигурност може да използва Рамката като референтна информация за установяването на такава.

Въпреки че Рамката е разработена с цел подобряване на управлението на риска за киберсигурността във връзка с критичната инфраструктура, тя може да бъде използвана от организации във всеки сектор на икономиката или обществото. Тя е замислена така, че да бъде полезна на компании, правителствени агенции и организации с нестопанска цел, независимо от тяхната насоченост или размер. Общата таксономия от стандарти, насоки и практики, които тя предоставя, също не са специфични за дадена страна. Организации извън Съединените щати също могат да използват Рамката за укрепване на собствените си усилия в областта на киберсигурността, и Рамката може да допринесе за разработването на общ език за международно сътрудничество в областта на киберсигурността на критичната инфраструктура.

1.1 Преглед на Рамката

Рамката е основан на риска подход към управлението на риска за киберсигурността и се състои от три части: Ядро на Рамката, Нива на изпълнение на Рамката и Профили на Рамката. Всеки компонент на Рамката засилва връзката между двигателите на бизнеса/мисията и дейностите по киберсигурността. По-долу следва обяснение на тези компоненти.

- *Ядрото на Рамката* представлява съвкупност от дейности по киберсигурността, желани резултати и приложими референтни източници, които са общи за секторите на критичната инфраструктура. Ядрото представя индустриалните стандарти, насоки и практики по начин, който позволява комуникиране на дейностите и резултатите в областта на киберсигурността в цялата организация – от ръководното ниво до нивото на изпълнение/операциите. Ядрото на Рамката се състои от пет едновременни и непрекъснати Функции: Идентифициране, Защита, Откриване, Отговор и Възстановяване. Когато се разглеждат заедно, тези Функции осигуряват стратегически поглед от високо ниво към жизнения цикъл на управлението на риска за киберсигурността на организацията. И така, Ядрото на Рамката определя базови ключови Категории и Подкатегории – които са отделни резултати – за всяка Функция, и ги съчетава с примерни Информативни референтни източници като съществуващи стандарти, насоки и практики за всяка Подкатегория.

- *Нивата на изпълнение на Рамката* („Нива“) осигуряват контекста за това как организацията вижда риска за киберсигурността и наличните процеси за управление на този риск. Нивата описват степента, до която практиките за управление на риска за киберсигурността на организацията представят характеристиките, дефинирани в Рамката (напр. осведоменост за рисковете и заплахите, повторяемост и адаптивност). Нивата характеризират практиките на организацията в интервала от Частично (Ниво 1) до Адаптивно (Ниво 4). Тези Нива отразяват преминаването от неформални, реактивни отговори към подходи, които са гъвкави и информирани на базата на риска. В процеса за избиране на Ниво организацията трябва да вземе под внимание текущите си практики в управлението на риска, средата на заплахи, правните и регулаторни изисквания, целите на бизнеса/мисията и ограниченията на организацията.
- *Профилът на Рамката* („Профил“) представя резултатите, базирани на бизнес нуждите, които организацията е избрала от Категориите и Подкатегориите на Рамката. Профилът може да се определи като хармонизиране на стандартите, насоките и практиките към Ядрото на Рамката в конкретен сценарий на изпълнение. Профилите могат да бъдат използвани за идентифициране на възможностите за подобряване на състоянието на киберсигурността чрез сравняване на „Текущ“ профил (състоянието „такова каквото е“) с „Целеви“ профил (състоянието „такова каквото ще бъде"). За да разработи даден Профил, организацията може да разгледа всички Категории и Подкатегории и, на базата на двигателите на бизнеса/мисията и на оценката на риска, да определи кои са най-важните; тя може да добави Категории и Подкатегории, според необходимостта, за да адресира рисковете за самата нея. След това Текущият профил може да се използва в подкрепа на приоритизирането и измерването на напредъка към Целевия профил, като същевременно се отчитат и други потребности на бизнеса, включително ефективността на разходите и иновациите. Профилите могат да се използват за провеждане на самооценка и комуникиране в рамките на организацията или между организациите.

1.2 Управление на риска и Рамката за киберсигурност

Управлението на риска е непрекъснат процес на идентифициране, оценяване и реагиране на рискове. За да управляват риска, организациите трябва да разбират вероятността от случване на дадено събитие и възможните последици от него. С тази информация, организациите могат да определят приемливото ниво на риска по отношение на постигането на техните организационни цели и могат да изразяват това като своя толерантност към риска.

Имайки разбиране за толерантността към риска, организациите могат да приоритизират дейностите по киберсигурността, което ще им позволи да вземат информирани решения за разходите за киберсигурността. Изпълнението на програми за управление на риска предлага на организациите възможността да квантифицират и комуникират корекциите към своите програми за киберсигурност. Организациите могат да изберат да се справят с риска по различни начини, включително чрез смекчаване на риска, прехвърляне на на риска, избягване на риска или приемане на риска, в зависимост от потенциалното въздействие върху доставката на услуги от критично значение. Рамката използва процесите за управление на риска, за да даде възможност на организациите да информират и приоритизират решенията си за киберсигурността. Тя поддържа повтарящи се оценки на риска и валидиране на двигателите на бизнеса, за да помогне на организациите да избират целевите състояния за дейностите по киберсигурността, които отразяват желаните резултати. Така Рамката дава на организациите възможността динамично да избират и насочват подобренията в управлението на риска за киберсигурността за средите на техните информационни технологии (IT) и системите за промишлен контрол (ICS) .

Рамката е адаптивна, за да може да осигури гъвкаво и базирано на риска изпълнение, което може да бъде използвано с широк спектър от процеси за управление на риска за киберсигурността. Сред примерите за такива процеси за управление на риска за киберсигурността са Международната организация по стандартизация (International Organization for Standardization (ISO)) 31000:2009[6], (ISO/Международната електротехническа комисия (ISO/International Electrotechnical Commission (IEC)) 27005:2011[7], Специалната публикация на Националния институт по стандарти и технологии (NIST Special Publication (SP)) 800-39[8] и Насока за *процеса на управление на риска за киберсигурността в електроенергийния подсектор* (*Electricity Subsector Cybersecurity Risk Management Process* (RMP)[9]).

1.3 Преглед на документа

Останалата част от този документ съдържа следните раздели и приложения:

- В Раздел 2 се описват компонентите на Рамката: Ядрото на Рамката, Нивата и Профилите.
- В Раздел 3 се дават примери за начините, по които Рамката може да бъде използвана.
- В Раздел 4 се описва начинът на използване на Рамката за самооценка и демонстриране на киберсигурността чрез измервания.
- Приложение А представя Ядрото на Рамката в табличен вид: Функциите, Категориите, Подкатегориите и Информативните референтни източници.
- Приложение Б съдържа кратък речник с избрани термини.
- Приложение В съдържа списък с използваните акроними в този документ.

[6] Международна организация по стандартизация (International Organization for Standardization), *Управление на риска – Принципи и насоки (Risk management - Principles and guidelines)*, ISO 31000:2009, 2009. http://www.iso. org/iso/home/standards/iso31000. htm

[7] Международна организация по стандартизация/Международна електротехническа комисия (International Organization for Standardization/International Electrotechnical Commission), Информационни технологии – *Методи за сигурност – Управление на риска за сигурността на информацията (Information technology - Security techniques - Information security risk management)*, ISO/IEC 27005:2011, 2011. https ://www. iso.org/standard/56742. html

[8] Съвместна работна група за инициатива за преобразуване (Joint Task Force Transformation Initiative), *Управление на риска за сигурността на информацията: от гледна точка на организациите, мисиите и информационните системи* (*Managing Information Security Risk: Organization, Mission, and Information System View)*, Специална публикация 800-39 на NIST, март 2011 г. https://doi.org/10.6028/NIST.SP.800-39

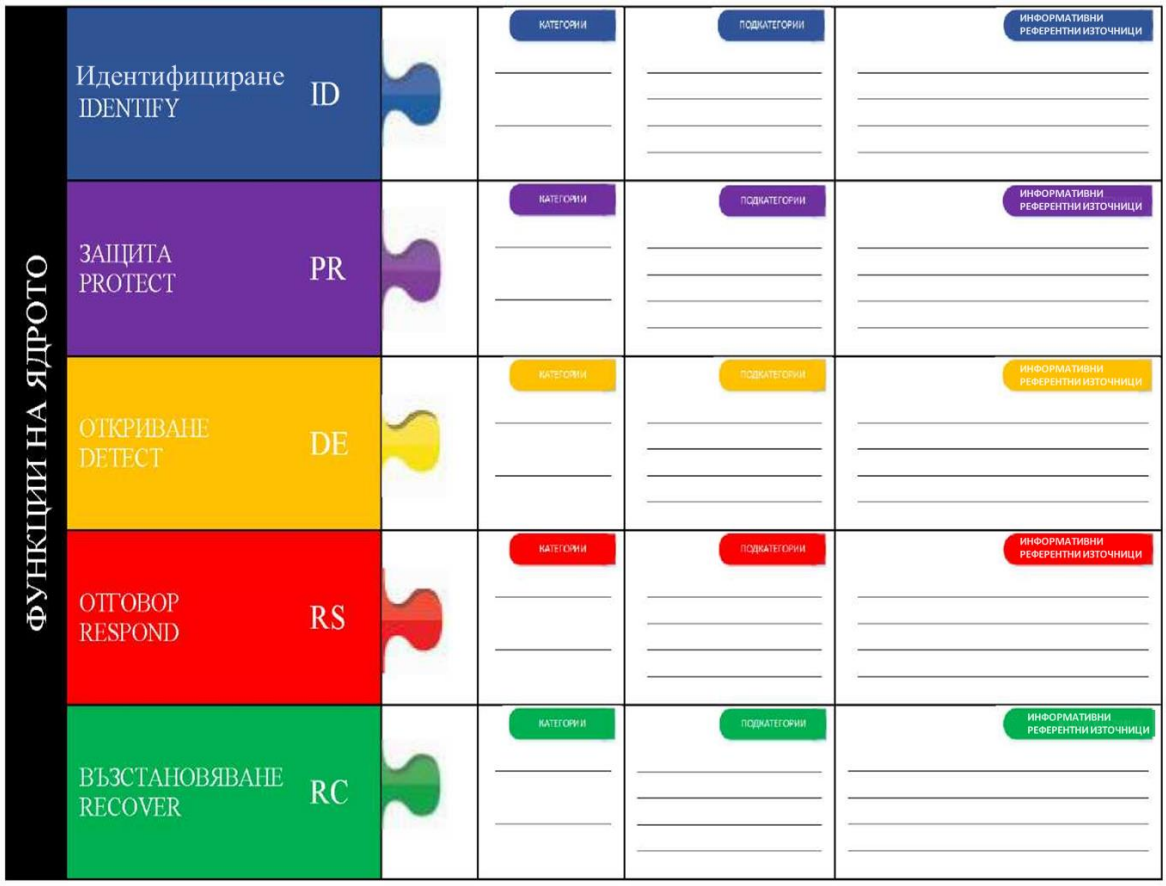
[9] Департамент по енергетика на САЩ, *Процес на управление на риска за киберсигурността в електроенергийния подсектор (Electricity Subsector Cybersecurity Risk Management Process)*, DOE/OE-0003, май 2012 г. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Основни елементи на Рамката

Рамката предоставя общ език за разбиране, управление и изразяване на риска за киберсигурността за вътрешните и външните заинтересовани страни. Тя може да се използва за подпомагане идентифицирането и приоритизирането на действия за намаляване на риска за киберсигурността, и е инструмент за хармонизиране на политическите, бизнес и технологичните подходи към управлението на този риск. Тя може да бъде използвана за управление на риска за киберсигурността в цели организации или да бъде фокусирана върху доставката на услуги от критично значение в дадена организация. Различни видове субекти –включително секторни координационни структури, асоциации и организации – могат да използват Рамката за различни цели, включително и за създаването на общи Профили.

2.1 Ядро на Рамката

Ядрото на Рамката предлага съвкупност от дейности за постигане на специфични *резултати за* киберсигурността и референтни примери на насоки за постигането на тези резултати. Ядрото не е контролен списък от действия за изпълнение. То представя ключови резултати за киберсигурността, идентифицирани от заинтересованите страни като полезни за управлението на риска за киберсигурността. Ядрото се състои от четири елемента: Функции, Категории, Подкатегории и Информативни референтни източници, изобразени на **Фигура 1**:



Фигура 1: Структура на Ядрото на Рамката.

Елементите на Ядрото на Рамката функционират заедно както следва:

- **Функциите** служат за организиране на основните дейности по киберсигурността на най-високото им ниво. Тези функции са: Идентифициране, Защита, Откриване, Отговор и Възстановяване. Те помагат на организацията да изрази своето управление на риска за киберсигурността, като съдействат за организирането на информацията, правят възможно вземането на решения за управление на риска, справянето със заплахи и подобряването на работата, вземайки предвид наученото от предишните действия. Функциите се съгласуват също и със съществуващите методологии за управление на инциденти и помагат да се демонстрира влиянието на инвестициите в киберсигурността. Така например инвестициите в планиране и тренировки поддържат навременни действия на отговор и възстановяване, което води до намаляване на въздействието върху доставката на услуги.

- **Категориите** са подразделения на Функциите, организирани в групи от резултати за киберсигурността, тясно свързани с програмни нужди и конкретни дейности. Като примери на Категории могат да се посочат: „Управление на активите“, „Управление на идентичността и контрол на достъпа“, „Процеси на откриване“.

- **Подкатегориите** допълнително разделят дадена Категория на специфични резултати от техническите и/или управленските дейности. Те предоставят съвкупност от резултати, които, макар и да не са изчерпателни, подпомагат поддръжането на постигането на резултатите във всяка Категория. Като примери на Подкатегории могат да се посочат: „Каталогизиране на външните информационни системи“, „Защита на данните в покой“, „Изследване на уведомленията от системите за откриване“.

- **Информативните референтни източници** представляват специфични раздели от стандарти, насоки и практики, общи за секторите на критичната инфраструктура, които илюстрират метод за постигане на резултатите, свързани с всяка Подкатегория. Информативните референтни източници, представени в Ядрото на Рамката, са илюстративни и не са изчерпателни. Те се базират на междусекторни насоки, които са били най-често реферирани в процеса на разработването на Рамката.

Петте Функции на Ядрото на Рамката са дефинирани по-долу. Предназначението на тези Функции не е да формират серийна пътека или да доведат до статично крайно желано състояние. По-скоро Функциите трябва да бъдат изпълнявани едновременно и непрекъснато, за да формират оперативна култура, която адресира динамичния риск за киберсигурността. Вижте Приложение А за пълния списък на Ядрото на Рамката.

- **Идентифициране –** Развиване на организационно разбиране за управлението на риска за киберсигурността за системи, хора, активи, данни и способности.

  Дейностите във Функцията „Идентифициране“ са основополагащи за ефективното използване на Рамката. Разбирането на контекста на бизнеса, ресурсите, които поддържат критични функции, и свързаните с това рискове за киберсигурността позволяват на организацията да се фокусира и да приоритизира усилията си в съгласие със своята стратегия за управление на риска и нуждите на бизнеса. Ето примери за Категории на резултати в тази Функция: „Управление на активи“, „Бизнес среда“, „Ръководство“, „Оценка на риска“, „Стратегия за управление на риска“.

- **Защита** – Разработване и изпълнение на подходящи предпазни мерки за гарантиране на доставката на услуги от критично значение.

  Функцията „Защита“ поддържа способността за ограничаване или задържане на влиянието на потенциалните събитие, засягащи киберсигурността. Ето примери за Категории на резултати в тази Функция: „Управление на идентичността и контрол на достъпа“, „Осведоменост и обучение“, „Сигурност на данните“, „Процеси и процедури за защита на информацията“, „Поддръжка“, „Защитни технологии“.

- **Откриване** – Разработване и изпълнение на подходящи дейности за идентифициране на появата на събитие, засягащо киберсигурността.

  Функцията „Откриване“ позволява навременното откриване на събития, свързани с киберсигурността. Ето примери за Категории на резултати в тази Функция: „Аномалии и събития“, „Непрекъснато наблюдение на сигурността“, „Процеси на откриване“.

- **Отговор** – Разработване и изпълнение на подходящи дейности за предприемане на действия по отношение на инцидент, засягащ киберсигурността.

  Функцията „Отговор“ поддържа способността за ограничаване на влиянието на даден потенциален инцидент, засягащ киберсигурността. Ето примери за Категории на резултати в тази Функция: „Планиране на отговора“, „Комуникации“, „Анализ“, „Смекчаване“ и „Подобрения“.

- **Възстановяване** – Разработване и изпълнение на подходящи дейности за поддръжане на планове за устойчивост и за възстановяване на способности или услуги, влошени поради инцидент, засягащ киберсигурността.

  Функцията „Възстановяване“ поддържа навременното възстановяване на нормалните операции, за да се намали въздействието на даден инцидент, засягащ киберсигурността. Ето примери за Категории на резултати в тази Функция: „Планиране на възстановяването“, „Подобрения“ и „Комуникации“.

2.2 Нива на изпълнение на Рамката

Нивата на изпълнение на Рамката („Нива“) осигуряват контекст на това как организацията вижда риска за киберсигурността и наличните процеси за управление на този риск. В интервала от Частично (Ниво 1) до Адаптивно (Ниво 4), Нивата описват нарастващата степен на точността и сложността на практиките за управление на риска за киберсигурността. Те помагат да се определи степента, до която управлението на риска за киберсигурността е информирано от нуждите на бизнеса и е интегрирано в цялостните практики за управление на риска на организацията. Съображенията при управлението на риска включват много аспекти на киберсигурността, включително и степента, до която съображенията за поверителност и граждански свободи се интегрират в управлението на риска за киберсигурността и в отговорите на потенциалния риск на дадена организация.

При процеса на избиране на Ниво трябва да се вземат предвид текущите практики за управление на риска, средата на заплахи, правните и регулаторните изисквания, практиките за обмен на информация, целите на бизнеса/мисията, изискванията за киберсигурност във веригите на доставки и ограниченията на организацията. Организациите трябва да определят желаното Ниво, като гарантират, че избраното ниво ще изпълни целите на организацията, че е възможно да се постигне и че намалява риска за киберсигурността за критичните активи и ресурси до нива, приемливи за организацията. Организациите трябва да се съобразят с външните насоки, получени от федерални правителствени департаменти и агенции, центрове за споделяне и

анализ на информация (Information Sharing and Analysis Centers - ISACs), организации за споделяне и анализ на информация (Information Sharing and Analysis Organizations - ISAOs), съществуващи модели на зрялост или други източници , които могат да ги подпомогнат при определяне на желаното от тях Ниво.

Макар и организациите, идентифицирани на Ниво 1 (Частично), да се насърчават да обмислят преминаване към Ниво 2 или по-високо, Нивата на Рамката не представляват нива на зрялост. Предназначението на Нивата е да подкрепя вземането на организационни решения за това как да се управлява рискът за киберсигурността, както и за това кои измерения на организацията са с по-висок приоритет и биха могли да получат допълнителни ресурси. Преминаването към по-високи Нива се насърчава, когато анализът „разходи-ползи“ показва осъществимо и рентабилно намаляване на риска за киберсигурността.

Успешната реализация на Рамката се основава на постигането на резултатите, описани в Целевия(те) профил(и) на организацията, а не на определянето на Ниво. Но изборът и посочването на Ниво, естествено, влияят върху Профилите на Рамката. Препоръчването на Ниво от мениджъри на ниво бизнес/процеси, утвърдено от ръководното ниво, ще помогне да се зададе общият тон за начина на управление на риска за киберсигурността в организацията и трябва да повлияе върху приоритизирането в рамките на Целевия профил и оценките на напредъка при адресиране на пропуските.

Следва дефинирането на Нивата:

Ниво 1: Частично

- *Процес на управление на риска* – Организационните практики за управление на риска за киберсигурността не са формализирани и рискът се управлява *в движение (ad hoc)* и понякога реактивно. Приоритизирането на дейностите по киберсигурността може да не е пряко информирано от целите на организацията по отношение на риска, средата на заплахи или изискванията на бизнеса/мисията.

- *Интегрирана програма за управление на риска* – Съществува ограничена осведоменост за риска за киберсигурността на организационно ниво. Организацията осъществява управлението на риска за киберсигурността нередовно, въз основа на всеки отделен случай, поради разнообразния си опит или информация, получавана от външни източници. Организацията може да не притежава процеси, позволяващи обмен на информацията за киберсигурността в самата нея.

- *Външно участие* – Организацията не разбира своята роля в по-голямата екосистема както по отношение на своите зависимости, така и по отношение на зависимите от нея. Организацията не си сътрудничи или не получава информация (напр. информация за заплахи, най-добри практики, технологии) от други субекти (напр. купувачи, доставчици, зависимости, зависими, организации за споделяне и анализ на информация (ISAO), изследователи, правителства), нито пък споделя информация. Организацията като цяло е неосведомена за рисковете във веригата на доставки в киберната инфраструктура за продуктите и услугите, които доставя и потребява.

Ниво 2: Информирано от риска

- *Процес на управление на риска* – Практиките за управление на риска са утвърдени от ръководството, но може да не са установени като политика в цялата организация. Приоритизирането на дейностите по киберсигурността и нуждите от защита е пряко информирано от целите на организацията по отношение на риска, средата на заплахи или изискванията на бизнеса/мисията.

- *Интегрирана програма за управление на риска* – Съществува осведоменост за риска за киберсигурността на организационно ниво, но не е установен подход за управление на риска за киберсигурността в рамките на цялата организация. Информацията за киберсигурността се споделя в организацията в неформален вид. Съображения за киберсигурността в целите и програмите на организацията могат да се вземат под внимание на някои нива в организацията, но не на всички. Понякога се прави оценка на риска за киберсигурността на организационни и външни активи, но това не е повторяем или повтарящ се процес.

- *Външно участие* – Като цяло организацията разбира своята роля в по-голямата екосистема по отношение или на своите собствени зависимости, или на зависимите, но не и на двете. Организацията си сътрудничи с други субекти и получава известна информация от тях, както и генерира известна част от собствената си информация, но може да не споделя информация с други. Също така организацията е осведомена за рисковете във веригата на доставки в киберната инфраструктура, асоциирани с продуктите и услугите, които доставя и потребява, но не предприема последователни или формални действия по отношение на тези рискове.

Ниво 3: Повторяемо

- *Процес на управление на риска* – Практиките за управление на риска на организацията са одобрени и изразени формално като политика. Организационните практики за киберсигурност се актуализират редовно на базата на прилагане на процесите за управление на риска спрямо измененията при изискванията на бизнеса/мисията и променящата среда на заплахите и технологиите.

- *Интегрирана програма за управление на риска* – Съществува установен подход за управление на риска за киберсигурността в цялата организация. Дефинират се, изпълняват се по предназначение и се ревизират информирани от риска политики, процеси и процедури. Съществуват последователни методи за ефективен отговор на промените в риска. Персоналът притежава необходимите знания и умения, за да изпълнява определените си роли и отговорности. Организацията наблюдава риска за киберсигурността на организационните активи последователно и точно. Ръководните служители по киберсигурността и ръководините служители в звената извън киберсигурността осъществяват редовна комуникация по въпросите на риска за киберсигурността. Ръководните служители гарантират съобразяване с киберсигурността във всички направления на работа в организацията.

- *Външно участие* – Организацията разбира своята роля, зависимости и зависими в по-голямата екосистема и може да допринася за по-широкото разбиране на рисковете на общността. Тя си сътрудничи с други субекти и редовно получава от тях информация, която допълва вътрешно генерираната информация, и споделя информация с други субекти. Организацията е осведомена за рисковете във веригата на доставки в киберната инфраструктура, асоциирани с продуктите и услугите, които предоставя и потребява. Също така тя обикновено предприема формални действия по отношение на тези рискове, включително използване на механизми като писмени споразумения за комуникиране на базови изисквания, структури на ръководство (напр. съвети по риска) и изпълнение и мониторинг на политики.

Ниво 4: Адаптивно

- *Процес на управление на риска* – Организацията адаптира своите практики по киберсигурността на базата на предишни и текущи дейности по киберсигурността, включително научени уроци и прогнозни индикатори. Чрез процес на непрекъснато усъвършенстване, включващ напреднали технологии и практики по киберсигурност, организацията се адаптира активно към изменящата се

среда на заплахи и технологии и отговаря своевременно и ефективно на еволюиращите усъвършенствани заплахи.

- *Интегрирана програма за управление на риска* – В цялата организация има установен подход към управлението на риска за киберсигурността, който използва информирани от риска политики, процеси и процедури за адресиране на потенциалните събития, свързани с киберсигурността. Връзката между риска за киберсигурността и целите на организацията се разбира ясно и се взема под внимание при вземането на решения. Ръководните служители наблюдават риска за киберсигурността в същия контекст като този на финансовия риск и на другите организационни рискове. Бюджетът на организацията се базира на разбиране на настоящата и предвижданата среда на риска и толерантност към риска. Стопанските единици изпълняват визията на ръководството и анализират риска на ниво системи в контекста на толерантността на организацията към риска. Управлението на риска за киберсигурността е част от организационната културата и еволюира от осведоменост за предишни дейности и непрекъсната осведоменост за дейности, свързани с техните системи и мрежи. Организацията може бързо и ефективно да отговаря за промени в целите на бизнеса/мисията по отношение на начина, по който се подхожда към риска и се комуникира за него.

- *Външно участие* – Организацията разбира своята роля, зависимости и зависими в по-голямата екосистема и допринася за по-широкото разбиране на рисковете на общността. Тя получава, генерира и ревизира приоритизирана информация, която информира непрекъснат анализ на нейните рискове, докато средите на заплахи и технологии еволюират. Организацията споделя тази информация вътрешно и външно с други сътрудници. Организацията използва информация в реално време или в почти реално време, за да разбира и последователно да действа при рискове във веригата на доставки в киберната инфраструктура, асоциирани с продуктите и услугите, които предоставя и потребява. Освен това, тя комуникира проактивно, като използва формални (например споразумения) и неформални механизми за разработване и поддържане на стабилни връзки във веригите на доставки.

2.3 Профил на Рамката

Профилът на Рамката („Профил“) представлява съгласуване на Функциите, Категориите и Подкатегориите с изискванията на бизнеса, толерантността към риска и ресурсите на организацията. Профилът позволява на организациите да създадат пътна карта за намаляване на риска за киберсигурността, която да бъде добре съгласувана с целите на организацията и сектора, да е съобразена с правните/регулаторните изисквания и с най-добрите практики в индустрията и да отразява приоритетите при управлението на риска. Имайки предвид сложността на много организации, те могат да решат да имат няколко Профила, съгласувани с определени компоненти и отчитащи индивидуалните им потребности.

Профилите на Рамката могат да бъдат използвани за описване на текущото или желаното целево състояние на конкретни дейности по киберсигурността. Текущият профил показва резултатите за киберсигурността, които в момента се постигат. Целевият профил показва резултатите, които са необходими за постигането на желаните цели при управлението на риска за киберсигурността. Профилите подкрепят изискванията на бизнеса/мисията и подпомагат комуникирането на риска в рамките на организацията и между организациите. Тази Рамка не предписва шаблони на Профили, което дава възможности за гъвкавост на изпълнението.

Сравнението на Профилите (например на Текущия и Целевия Профил) може да покаже пропуски, които трябва да се отстранят, за да се постигнат целите на управлението на риска за киберсигурността. Един план за действие за отстраняването на тези пропуски, за да се изпълни дадена Категория или Подкатегория, може да допринесе към съдържанието на описаната по-горе пътна карта. Приоритизирането на смекчаването на

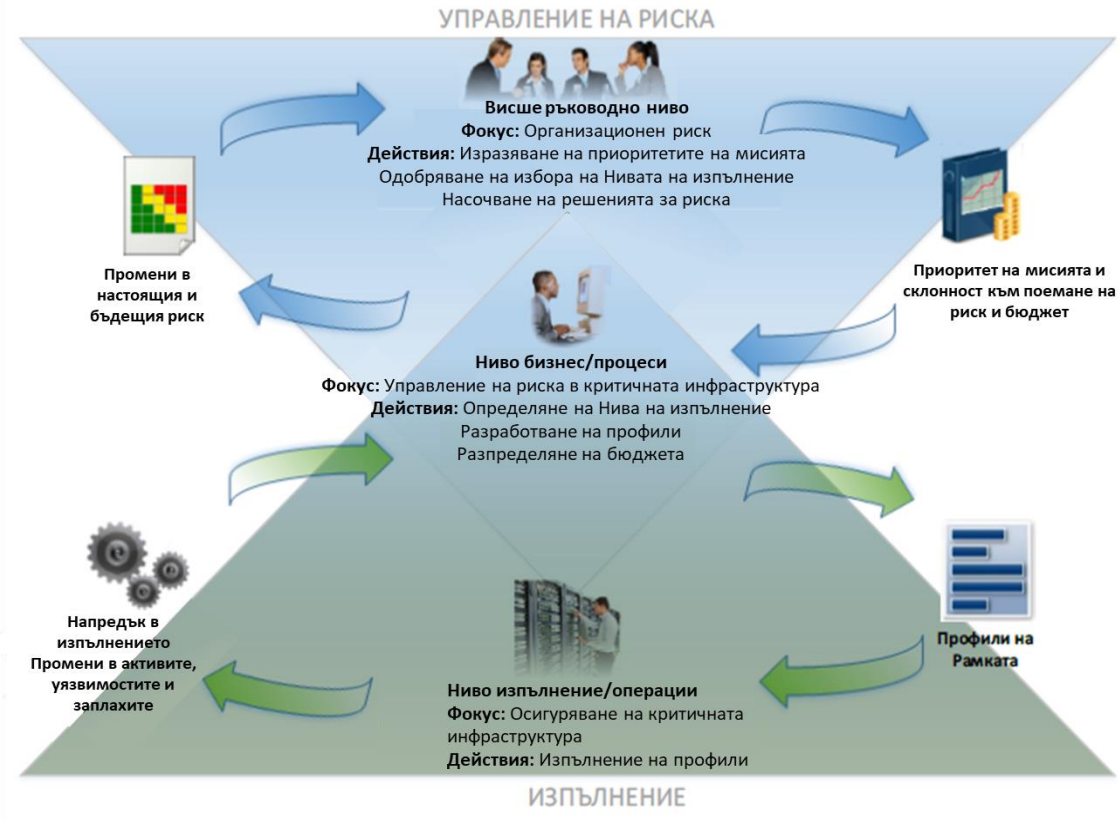
пропуските се обуславя от бизнес нуждите и процесите за управление на риска на организацията. Този подход, базиран на риска, позволява на организацията да определи необходимите ресурси (например персонал, финансиране) с цел постигане на целите на киберсигурността по рентабилен и приоритизиран начин. Освен това, Рамката представлява подход, базиран на риска, където приложимостта и изпълнението на дадена Подкатегория се подчиняват на обхвата на Профила.

2.4 Координиране на изпълнението на Рамката

Фигура 2 описва общия поток на информацията и решенията на следните нива на организацията:

- Ръководно
- Бизнес/процес
- Изпълнение/операции

Ръководното ниво комуникира приоритетите на мисията, наличните ресурси и цялостната толерантност към риска към ниво „бизнес/процес“. Ниво „бизнес/процес“ използва информацията като принос към съдържанието на процеса за управление на риска и впоследствие си сътрудничи с ниво „изпълнение/операции“, за да комуникира нуждите на бизнеса и да създаде Профил. Ниво „изпълнение/операции“ комуникира напредъка в изпълнението на Профила на ниво „бизнес/процес“. Ниво „бизнес/процес“ използва тази информация, за да извърши оценка на въздействието. Ръководството на ниво „бизнес/процес“ докладва резултатите от оценката на въздействието на ръководното ниво, за да информира цялостния процес на управление на риска на организацията, и на ниво „изпълнение/операции“, за да има осведоменост по отношение на въздействието върху бизнеса.



Фигура 2: Условни информационни потоци и потоци на вземане на решения в дадена организация

3.0 Как да се използва Рамката

Дадена организация може да използва Рамката като ключов елемент от своя систематичен процес за идентифициране, оценяване и управление на риска за киберсигурността. Рамката не е предназначена да замени съществуващите процеси; организацията може да използва текущия си процес и да го наложи върху Рамката, за да определи пропуски в настоящия си подход към риска за киберсигурността и да разработи пътна карта за подобрение. Използвайки Рамката като инструмент за управление на риска за киберсигурността, организацията може да определи дейности, които са най-важни за доставката на услуги от критично значение, и да приоритизира разходите, за да максимизира въздействието на инвестициите.

Рамката е проектирана така, че да допълни съществуващите операции на бизнеса и по киберсигурността. Тя може да послужи като основа за нова програма за киберсигурността или като механизъм за подобряване на съществуващата такава. Рамката предоставя средство за изразяване на изискванията към киберсигурността към бизнес партньорите и клиентите и може да помогне в идентифицирането на пропуски в практиките по киберсигурността на организацията. Тя предоставя също и общ набор от съображения и процеси за разглеждане на последиците за поверителността и гражданските свободи в контекста на програмата за киберсигурност.

Рамката може да се прилага през всички етапи на жизнения цикъл от планиране, проектиране, изграждане/закупуване, внедряване, експлоатация и извеждане от експлоатация. Етапът на планиране стартира цикъла на всяка система и полага основата на всичко, което следва. Най-общите съображения за киберсигурност трябва да бъдат обявени и описани възможно най-ясно. При съставянето на плана трябва да се вземе под внимание, че тези съображения и изисквания вероятно ще се развият през останалата част от жизнения цикъл. Етапът на проектиране трябва да отчита изискванията за киберсигурността като част от по-големия мултидисциплинарен процес на системното инженерство[10]. Ключов момент от етапа на проектиране е доказването, че спецификациите на системата за киберсигурността съответстват на нуждите и отношението към риска на организацията, така както са отразени в Профила на Рамката. Желаните резултати за киберсигурността, приоритизирани в Целеви профил, трябва да бъдат включени при: (а) разработване на системата на етапа на изграждане и (б) закупуване или възлагане на системата на друг изпълнител на етапа на закупуване. Същият Целеви профил служи като списък на характеристиките на киберсигурността на системата, които трябва да бъдат оценени при внедряването на системата, за да се провери дали всички характеристики са изпълнени. Резултатите за киберсигурността, определени чрез използване на Рамката, след това трябва да послужат като основа за непрекъсната работа на системата. Това включва периодично повторно оценяване и включване на резултатите в Текущ профил, за да се определи дали изискванията за киберсигурността все още се изпълняват. Обикновено наличието на сложна мрежа от зависимости (например компенсиране и общи контроли) между системите означава, че резултатите, документирани в Целевите профили на свързани системи, трябва да бъдат взети под сериозно внимание, когато системите се извеждат от експлоатация.

В следващите раздели са разгледани различни начини, по които организациите могат да използват Рамката.

[10] Специална публикация 800-160 на NIST, том 1,, *Инженерство на сигурността на системите, Съображения за мултидисциплинарен подход в инженерството на надеждни сигурни системи (System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems),* Рос и сътр., ноември 2016 г. (актуализирана на 21 март 2018 г.), https://doi.org/10.6028/NIST.SP.800-160v1

3.1 Основен преглед на практиките по киберсигурността

Рамката може да се използва за сравняване на текущите дейности по киберсигурността на дадена организацията с тези, които са описани в Ядрото на Рамката. Чрез създаването на Текущ профил, организациите могат да проверят степента, до която постигат резултатите, описани в Категориите и Подкатегориите на Ядрото, приведени в съответствие с петте Функции от високо ниво: Идентифициране, Защита, Откриване, Отговор и Възстановяване. Дадена организация може да установи, че вече постига желаните резултати, като по този начин управлява киберсигурността, съизмерима с известния риск. Като алтернатива, организацията може да констатира, че има възможности (или че е необходимо) да се усъвършенства. Организацията може да използва тази информация за разработване на план за действие за укрепване на съществуващите практики по киберсигурността и намаляване на риска за киберсигурността. Организацията също така може да установи, че инвестира повече от необходимото за постигането на определени резултати. Тя може да използва тази информация, за да приоритизира повторно своите ресурси.

Макар да не заместват процеса на управление на риска, тези пет Функции от високо ниво предоставят на ръководните служители и други стегнат начин, по който да могат да дефинират основните концепции за риска за киберсигурността, така че да могат да направят оценка на начина, по който се управляват идентифицираните рискове и какво е положението на тяхната организация на високо ниво по отношение на съществуващите стандарти, насоки и практики в областта на киберсигурността. Рамката може да помогне на дадена организация да си отговори на основни въпроси, включително и на въпроса: „Как се справяме?“ След това тя може да действа по един по-информиран начин по отношение на укрепването на своите практики по киберсигурността, където и когато прецени това за необходимо.

3.2 Установяване или подобряване на програма за киберсигурност

Следващите стъпки илюстрират по какъв начин дадена организация може да използва Рамката, за да създаде нова програма за киберсигурност или за да подобри съществуващата такава. Тези стъпки трябва да се повторят, когато това е необходимо, за непрекъснато подобряване на киберсигурността.

Стъпка 1: Приоритизиране и определяне на обхвата. Организацията идентифицира целите на своя бизнес/мисия и организационните приоритети на високо ниво. С помощта на тази информация организацията взима стратегически решения по отношение на начините на внедряване на киберсигурността и определя обхвата на системите и активите, които поддържат избраната област или процес на дейност на бизнеса. Рамката може да бъде адаптирана така, че да поддържа различните области или процеси на дейността на бизнеса в една организация, която може да има различни бизнес нужди и свързана с тях толерантност към риска. Толерантността към риска може да бъде отразена в Целево ниво на изпълнението.

Стъпка 2: Ориентиране. След като обхватът на програмата за киберсигурност за областта или процеса на дейността на бизнеса бъде определен, организацията идентифицира свързани системи и активи, регулаторни изисквания и цялостен подход към риска. Организацията прави справка с източници, за да идентифицира заплахи и уязвимости, приложими за тези системи и активи.

Стъпка 3: Създаване на Текущ профил. Организацията разработва Текущ профил, като посочва кои резултати от Категориите и Подкатегориите от Ядрото на Рамката се постигат в момента. Ако даден резултат е постигнат само частично, отбелязването на този факт ще съдейства за подпомагането на следващите стъпки чрез предоставяне на базова информация.

Стъпка 4: Провеждане на оценка на риска. Тази оценка може да се ръководи от цялостния процес на управление на риска на организацията или предишни дейности за оценка на риска. Организацията анализира

оперативната среда, за да определи вероятността от възникване на събитие, свързано с киберсигурността и въздействието, което това събитие може да окаже върху организацията. Важно е организациите да идентифицират възникващите рискове и да използват информация за кибер заплахи от вътрешни и външни източници с цел постигане на по-добро разбиране на вероятността и въздействието на събитията, свързани с с киберсигурността.

Стъпка 5: Създаване на Целеви профил. Организацията създава Целеви профил, който се фокусира върху оценката на Категориите и Подкатегориите от Рамката, описващ желаните резултати за киберсигурността на организацията. Организациите могат да разработят и свои собствени допълнителни Категории и Подкатегории, които да отчитат уникални организационни рискове. При създаването на Целеви профил организацията може също така да вземе под внимание и влиянията и изискванията на външни заинтересовани страни, като субекти, клиенти и бизнес партньори от съответния сектор. Целевият профил трябва да отразява по подходящ начин критериите в целевото Ниво на изпълнение.

Стъпка 6: Определяне, анализиране и приоритизиране на пропуските. За да определи пропуските, организацията прави сравнение между Текущия и Целевия профил. След това тя създава приоритизиран план за действие за справяне с пропуските, отразяващ двигателите, разходите и ползите, и рисковете за мисията, за да постигне резултатите в Целевия профил. По-нататък, организацията определя ресурсите, включително финансиране и работна сила, необходими за отстраняване на пропуските. Използването на Профилите по този начин насърчава организацията да взема информирани решения за дейностите по киберсигурността, подпомага управлението на риска и дава възможност на организацията да извършва рентабилни и целенасочени подобрения.

Стъпка 7: Изпълнение на плана за действие. Организацията определя какви действия да предприеме , за да преодолее пропуските (ако има такива), които са били идентифицирани при предишната стъпка, след което коригира настоящите си практики по киберсигурността, за да постигне Целевия профил. Като допълнително ръководство Рамката идентифицира примерни Информативни референтни източници по отношение на Категориите и Подкатегориите, но организациите трябва сами да определят кои стандарти, насоки и практики, включително и тези, които са специфични за дадения сектор, са най-ефективни за техните нужди.

Организацията повтаря стъпките толкова пъти, колкото е необходимо, за да може непрекъснато да оценява и подобрява своята киберсигурност. Така например организациите могат да установят, че по-честото повтаряне на стъпката „Ориентиране“ подобрява качеството на оценките на риска. Също така организациите могат да наблюдават напредъка чрез итеративни актуализации на Текущия профил, като впоследствие сравняват Текущия профил с Целевия профил. Организациите могат също да използват този процес, за да хармонизират програмата си за киберсигурност с желаното от тях Ниво на изпълнение на Рамката.

3.3 Комуникиране на изискванията за киберсигурност заинтересованите страни

Рамката предлага общ език за комуникиране на изискванията между взаимозависимите заинтересовани страни, отговорни за предоставянето на основни продукти и услуги на критичната инфраструктура. Някои от примерите са следните:

- Дадена организация може да използва Целеви профил, за да изрази изискванията за управление на риска за киберсигурността към външен доставчик на услуги (например облачен доставчик, към който експортира данни).
- Дадена организация може да изрази състоянието си на киберсигурност чрез Текущ профил, за да отчете резултатите или да направи сравнение с изискванията за придобиване.

- Собственик/оператор на критична инфраструктура, след като е идентифицирал външен партньор, от когото зависи тази инфраструктура, може да използва Целеви профил, за да предаде необходимите Категории и Подкатегории.
- Сектор от критичната инфраструктура може да зададе Целеви профил за членовете си, който може да бъде използван сред съставните му елементи като първоначален базов Профил за изграждане на техни персонализирани Целеви профили.
- Дадена организация може по-добре да управлява риска за киберсигурността сред заинтересованите страни, оценявайки тяхната позиция в критичната инфраструктура и по-широката цифрова икономика, като използва Нива на изпълнение.

Комуникацията е особено важна сред заинтересованите нагоре и надолу по веригата на доставки. Веригите на доставки са сложни, глобално разпределени и взаимосвързани съвкупности от ресурси и процеси между множество нива на организации. Веригите на доставки започват с намирането на източници на продукти и услуги и продължават с проектирането, разработването, произвеждането, обработването, боравенето и доставянето на продукти и услуги на крайния потребител. Като се имат предвид тези сложни и взаимосвързани отношения, управлението на риска във веригите на доставки (SCRM) представлява критична организационна функция[11].

Управлението на риска за киберсигурността във веригите на доставки (CSCRM) е съвкупност от дейности, необходими за управление на риска с киберсигурността, свързан с външни страни. По-конкретно, CSCRM се занимава както с ефекта на киберсигурността, който организацията упражнява върху външните страни, така и с ефекта на киберсигурността, който външните страни упражняват върху организацията.

Основна цел на CSCRM е идентифицирането, оценяването и смекчаването на „продукти и услуги, които могат да съдържат потенциално зловредна функционалност, които са фалшифицирани или са уязвими поради лоши практики в производството и разработването във веригата на доставки в киберната инфраструктура“[12]. Дейностите по CSCRM могат да включват:

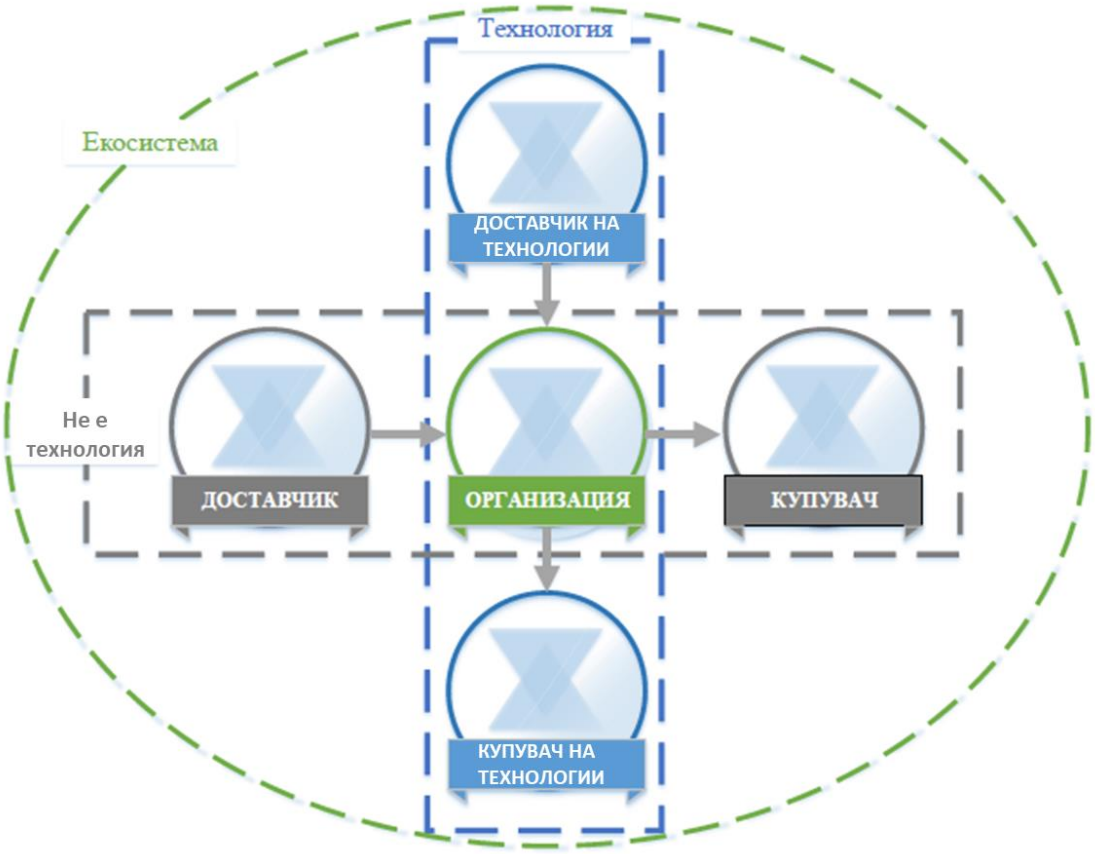
- Определяне на изискванията за киберсигурност към доставчици,
- Законодателно уреждане на изискванията за киберсигурност сключване на официални споразумения (например договори),
- Комуникиране на доставчиците начина, по който тези изисквания за киберсигурност ще бъдат верифицирани и валидирани,
- Проверяване дали изискванията за киберсигурност са изпълнени чрез различни методологии за оценка и
- Ръководене и управляване на горепосочените дейности.

Както е показано на Фигура 3, CSCRM обхваща доставчици и купувачи на технологии, както и доставчици и купувачи на неща с нетехнологичен характер, където технологията е съставена минимално от информационни технологии (IT), системи за промишлен контрол (ICS), кибер-физични системи (CPS) и свързани устройства в по-общ смисъл, включително Интернет на нещата (IoT). Фигура 3 представя организация в определена времева точка. Но при нормалния ход на бизнес операциите, повечето организации

[11] Комуникирането на Изискванията за киберсигурност (Раздел 3.3) и Решенията за покупка (Раздел 3.4) адресират само две употреби на Рамката за управлението на риска за киберсигурността във веригите на доставки (CSCRM) и не са предназначени да адресират CSCRM изчерпателно.

[12] Специална публикация 800-161 на NIST, *Практики за управление на риска във веригите на доставки за федерални информационни системи и организации,* Бойенс и сътр. (NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al), април 2015 г, https://doi.org/10.6028/NIST.SP.800-161

ще бъдат както доставчик нагоре по веригата, така и купувач надолу по веригата по отношение на други организации или крайни потребители.



Фигура 3: Взаимоотношения във веригата на доставки в киберната инфраструктура

Страните, описани на Фигура 3, представляват екосистема на киберсигурността на организацията. Тези отношения изтъкват съществената роля на CSCRM при справянето с риска за киберсигурността в критичната инфраструктура и в по-широката цифрова икономика. Тези взаимоотношения, продуктите и услугите, които предоставят, и рисковете, които представляват, трябва да бъдат идентифицирани и отчетени като фактори за способностите за защита и откриване на организациите, както и за техните протоколи за отговор и възстановяване.

На фигурата по-горе „Купувач" се отнася до хората или организациите надолу по веригата, които консумират даден продукт или услуга на организация, включително организации със стопанска и с нестопанска цел. „Доставчик“ обхваща доставчици нагоре на продукти и услуги по веригата, които се използват за вътрешни цели от организацията (инфраструктурата на информационните технологии (IT)) или се интегрират в продуктите или услугите, предоставяни на купувача. Тези термини са приложими както за базирани на технологии продукти и услуги, така и за небазирани на технологии продукти и услуги.

Независимо дали се вземат предвид отделните Подкатегории на ядрото или всеобхватните съображения на даден Профил, Рамката предлага на организациите и на техните партньори метод, с чиято помощ се

гарантира, че новият продукт или услуга отговарят на критични резултати за сигурността. Избирайки първо резултати, които са от значение за контекста (например предаване на информация, позволяваща лично идентифициране (PII), доставка на услуги от критично значение за мисията, услуги за верифициране на данни, интегритет на продукти и услуги), организацията може след това да оцени партньорите си на базата на тези критерии. Например, ако се закупува система за наблюдение на оперативните технологии (OT) за аномална мрежова комуникация, тогава наличието може да бъде особено важна цел за киберсигурността, която трябва да се постигне, и трябва да накара Доставчика на технологии да вземе решение против някои приложими Подкатегории (например ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Решения за покупка

Тъй като конкретният Целеви профил на Рамката е приоритизиран списък на организационните изисквания за киберсигурност, Целевите профили могат да се използват за информиране на решения за закупуване на продукти и услуги. Тази транзакция се различава от комуникирането на изисквания за киберсигурност със заинтересованите страни (разгледано в Раздел 3.3) в това, че може да не е възможно да се наложи съвкупност от изисквания за киберсигурност върху доставчика. Целта е да се вземе най-доброто решение за покупка при много на брой доставчици на базата на внимателно определен списък от изисквания за киберсигурност. Често това означава допускане на известен компромис, като се сравняват множество продукти или услуги с известни пропуски с Целевия профил.

След закупуване на продукт или услуга, Профилът може да се използва и за проследяване и адресиране на остатъчен риск с киберсигурността. Така например ако закупената услуга или продукт не отговарят на всички цели, описани в Целевия профил, организацията може да разреши остатъчния риск чрез други управленски действия. Профилът също така предоставя на организацията метод за оценка на това дали продуктът отговаря на резултатите за киберсигурността чрез механизми за периодични проверки и тестове.

3.5 Идентифициране на възможности за нови или ревизирани Информативни референтни източници

Рамката може да се използва за идентифициране на възможности за нови или ревизирани стандарти, насоки или практики, при които допълнителни Информативни референтни източници биха помогнали на организациите да се справят с възникващи нужди. Организация, прилагаща дадена Подкатегория или разработваща нова Подкатегория, може да установи, че съществуват много малко Информативни референтни източници по отношение на съответната дейност, ако изобщо съществуват такива. За да удовлетвори тази потребност, организацията може да си сътрудничи с технологични лидери и/или органи по стандартизация, за да изготви, разработи и координира необходимите стандарти, насоки или практики.

3.6 Методология за защита на поверителността и гражданските свободи

Този Раздел съдържа методология за справяне с последиците за личната неприкосновеност и гражданските свободи, които могат да се получат като резултат от киберсигурността. Предназначението на тази методологията е да послужи като общ сбор от съображения и процеси, тъй като последиците за поверителността и гражданските свободи могат да се различават за отделните сектори или във времето и организациите могат да адресират тези съображения и процеси с редица технически нововъведения. Независимо от това, не всички дейности в една програма за киберсигурност водят до съображения, свързани с поверителността и гражданските свободи. Може да се наложи да се разработят технически стандарти, насоки и допълнителни най-добри практики за поверителност, които да поддържат подобрените технически нововъведения.

Между поверителността и киберсигурността съществува здрава връзка. Дейностите по киберсигурността на дадена организация могат също да създадат рискове за поверителността и гражданските свободи, когато се използва, събира, обработва, поддържа или разкрива лична информация. Ето някои примери: Дейности по киберсигурността, които водят до прекомерно събиране или прекомерно запазване на лична информация; разкриване или използване на лична информация, която не е свързана с дейности по киберсигурността; и дейности за смекчаване на неблагоприятните въздействия върху киберсигурността, които водят до отказ от услуга или други подобни потенциално неблагоприятни въздействия, включително някои видове откриване или наблюдение на инциденти, които могат да възпрепятстват свободата на изразяване или сдружаване.

Правителството и неговите представители са отговорни за защитата на гражданските свободи, произтичащи от дейностите по киберсигурността. Както е посочено в методологията по-долу, правителството или неговите представители, които притежават или оперират с критична инфраструктура, трябва да разполагат с установен процес, който да поддъжа съответствието на дейностите по киберсигурността с приложимите закони, разпоредби и конституционни изисквания за поверителност.

За да се справят с последиците за поверителността, организациите могат да помислят за това как тяхната програма за киберсигурност може да включи принципи за поверителност като: минимизиране на данни при събирането, разкриването и запазването на материали, съдържащи лична информация, свързани с инцидента, засягащ киберсигурността; използване на ограничения извън дейностите по киберсигурността за всяка информация, събрана специално за дейности по киберсигурността; прозрачност по отношение на дадени дейности по киберсигурността; индивидуално съгласие и обезщетения за неблагоприятни въздействия, произтичащи от използването на лична информация в дейности по киберсигурността; качество, интегритет и сигурност на данните; отчетност и одитиране.

Когато организациите правят оценка на Ядрото на Рамката в Приложение А, като средство за справяне с посочените по-горе последици за поверителността и гражданските свободи могат да се посочат следните процеси и дейности:

Ръководене на риска за киберсигурността

- Оценката на риска за киберсигурността и отговорите на потенциалния риск на организацията взима под внимание последиците за поверителността на нейната програма за киберсигурност.
- Хората с отговорности, засягащи поверителността, свързана с киберсигурността, докладват на съответното ръководство и са подходящо обучени.
- Съществува процес, който поддържа съответствието на дейностите по киберсигурността с приложимите закони, разпоредби и конституционни изисквания за поверителност.
- Съществува процес за оценка на изпълнението на посочените по-горе организационни мерки и контроли.

Подходи за идентифициране, удостоверяване и упълномощаване на лица за достъп до организационни активи и системи

- Предприемат се стъпки за идентифициране и справяне с последиците за поверителността на мерките за управление на идентичността и контрола на достъпа до степента, до която те включват събиране, разкриване или използване на лична информация.

Мерки за повишаване на осведомеността и обучение

- Приложимата информация от организационните политики за поверителността се включва в дейности за обучаване на работната сила в областта на киберсигурност и осведомеността.

- Доставчиците на услуги, които предоставят за организацията услуги, свързани с киберсигурността, се информират за приложимите политики за поверителност на организацията.

Откриване на аномални дейности и наблюдение на системи и активи

- Съществува процес за извършване на преглед на поверителността при откриване на аномална дейност и наблюдение на киберсигурността на организацията.

Дейности за за отговор, включително обмен на информация или други усилия за смекчаване

- Съществува процес за оценка и справяне с това дали, кога, как и доколко личната информация се споделя извън организацията като част от дейностите за обмен на информация за киберсигурността.
- Съществува процес за извършване на преглед на поверителността на усилията на организацията за смекчаване на ефектите върху кибесигурността.

4.0 Самооценка на риска за киберсигурността с помощта на Рамката

Предназначението на Рамката за киберсигурност е да намали риска чрез подобряване на управлението на риска за киберсигурността предвид организационните цели. В идеалния случай използващите Рамката организации ще могат да измерват и задават стойности на техния риск, *заедно с* разходите и ползите от предприетите стъпки за намаляване на риска до приемливи нива. Колкото по-добре една организация може да измери своя риск, разходите и ползите от стратегиите и стъпките за киберсигурност, толкова по-рационален, ефективен и ценен ще бъде нейният подход и инвестиции в киберсигурността.

С течение на времето, самооценката и провеждането на измервания трябва да подобрят вземането на решения относно инвестиционните приоритети. Така например измерването – или поне надеждното характеризиране – на аспекти на състоянието на киберсигурността на организацията и тенденциите във времето могат да позволят на организацията да разбере и предаде значима информация за риска на зависими страни, доставчици, купувачи и други страни. Организацията може да направи това вътрешно или като потърси извършване на оценка от трета страна. Ако се извършат правилно и със зачитане на ограниченията, тези измервания могат да осигурят основа за стабилни отношения на доверие както в самата организация, така и извън нея.

За да проучи ефективността на инвестициите, организацията първо трябва да има ясно разбиране за организационните си цели, връзката между тези цели и подкрепящите ги резултати за киберсигурността и начина на прилагане и управление на тези отделни резултати за киберсигурността. Въпреки че измерванията на всички тези елементи са извън обхвата на Рамката, резултатите за киберсигурността на Ядрото на Рамката подкрепят самооценката на ефективността на инвестициите и дейностите по киберсигурността по следните начини:

- Избор на това как различните частите на операцията по киберсигурност трябва да повлияят на избора на Целеви нива на изпълнение,
- Оценяване на подхода на организацията към управлението на риска за киберсигурността чрез определяне на Текущи нива на изпълнение,
- Приоритизиране на резултатите за киберсигурността чрез разработване на Целеви профили,
- Определяне на степента, до която конкретните стъпки за киберсигурност са постигнали желаните резултати за киберсигурността чрез оценяване на Текущи профили, и
- Измерване на степента на изпълнение по отношение на каталозите за контрол или технически насоки, посочени като Информативни референтни източници.

Разработването на показатели за ефективност на киберсигурността еволюира. Организациите трябва да бъдат съобразителни, креативни и внимателни към начините, по които използват измервания, за да оптимизират употребата, като същевременно избягват да разчитат на изкуствени показатели за текущото състояние и напредъка в подобряването на управлението на риска за киберсигурността. Преценяването на риска за киберсигурността изисква дисциплина и трябва да се преразглежда периодично. Всеки път, когато се използват измервания като част от процеса, определен от Рамката, организациите се насърчават ясно да определят и да знаят защо са важни тези измервания и как те ще допринесат за цялостното управление на риска за киберсигурността. Те също така трябва да са наясно и с ограниченията на измерванията, които използват.

Така например проследяването на мерките за сигурност и резултатите за бизнеса могат да дадат значима информация за това как промените в грануларните контроли за сигурност засягат изпълнението на организационните цели. Верифицирането на постигането на някои организационни цели изисква анализиране на данните, едва *след* като тази цел е трябвало да бъде постигната. Този вид изоставаща мярка е по-абсолютна. Често пъти, обаче, е по-ценно да се предвиди дали *може* да възникне риск за киберсигурността и въздействието, което той *би могъл* да има, като се използва водеща мярка.

Организациите се насърчават да иновират и да персонализират начина, по който включват измервания при прилагането на Рамката с пълно разбиране на тяхната полезност и ограничения.

Приложение А: Ядро на Рамката

Това приложение представя Ядрото на Рамката: Изброяване на Функции, Категории, Подкатегории и Информативни референтни източници, които описват специфични дейности по киберсигурността, общи за всички сектори на критичната инфраструктура. Избраният формат на представяне за Ядрото на Рамката не предполага конкретен ред на изпълнение или степен на важност на Категориите, Подкатегориите и Информативните референтни източници. Ядрото на Рамката, представено в това Приложение, представлява обща съвкупност от дейности за управление на риска за киберсигурността. И макар че Рамката не е изчерпателна, тя е разширяема, което позволява на организациите, секторите и другите субекти да използват Подкатегории и Информативни референтни източници, които са рентабилни и ефективни и които им позволяват да управляват своя риск за киберсигурността. Дейностите могат да бъдат избрани от Ядрото на Рамката по време на процеса за създаване на Профил, като към този Профил могат да се добавят допълнителни Категории, Подкатегории и Информативни референтни източници. Процесите на управление на риска на организацията, правните/регулаторните изисквания, целите на бизнеса/мисията и организационните ограничения ръководят избора на тези дейности при създаването на Профил. Личната информация се счита за компонент от данни или активи, реферирани в Категориите при оценяването на рисковете за сигурността и защитите.

Макар и предвидените резултати, идентифицирани във Функциите, Категориите и Подкатегориите, да са еднакви за информационните технологии (IT) и системите за промишлен контрол (ICS), оперативните среди и съображенията за IT и ICS се различават. ICS оказват пряк ефект върху физическия свят, включително с потенциални рискове за здравето и безопасността на хората, и въздействат върху околната среда. Освен това, ICS имат уникални изисквания за начина на функциониране и надеждност в сравнение с IT и целите за безопасност и ефективност трябва да се взимат под внимание при прилагането на мерки за киберсигурност.

За улесняване на използването всеки компонент от Ядрото на Рамката получава уникален идентификатор. Всяка от Функциите и Категориите има уникален буквен идентификатор, както е показано в Таблица 1. Подкатегориите във всяка Категория се реферират с числа; уникалният идентификатор за всяка Подкатегория е посочен в Таблица 2.

Допълнителни подкрепящи материали, включително Информативни референтни източници, свързани с Рамката, могат да бъдат намерени на уеб сайта на NIST на: http://www.nist.gov/cyberframework/.

Таблица 1: Уникални идентификатори на Функциите и Категориите

Уникален идентификатор на Функция	Функция	Уникален идентификатор на Категория	Категория
ID	Идентифициране	ID.AM	Управление на активите
		ID.BE	Бизнес среда
		ID.GV	Ръководство
		ID.RA	Оценка на риска
		ID.RM	Стратегия за управление на риска
		ID.SC	Управление на риска във веригите на доставки
PR	Защита	PR.AC	Управление на идентичността и контрол на достъпа
		PR.AT	Осведоменост и обучение
		PR.DS	Сигурност на данните
		PR.IP	Процеси и процедури за защита на информацията
		PR.MA	Поддръжка
		PR.PT	Защитни технологии
DE	Откриване	DE.AE	Аномалии и събития
		DE.CM	Непрекъснато наблюдение на сигурността
		DE.DP	Процеси на откриване
RS	Отговор	RS.RP	Планиране на отговора
		RS.CO	Комуникации
		RS.AN	Анализ
		RS.MI	Смекчаване
		RS.IM	Подобрения
RC	Възстановяване	RC.RP	Планиране на възстановяването
		RC.IM	Подобрения
		RC.CO	Комуникации

Таблица 2: Ядро на Рамката

Функция	Категория	Подкатегория	Информативни референтни източници
ИДЕНТИФИЦИРАНЕ (ID)	**Управление на активите (ID.AM):** Данните, персонала, устройствата, системите и съоръженията, които позволяват на организацията да постигне идентифициране и управление на бизнес целите в съответствие с относителното им значение за организационните цели и стратегията за управление на риска на организацията.	**ID.AM-1:** Инвентаризиране на физическите устройства и системи в организацията	**CIS CSC 1** **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53, Рев. 4,** CM-8, PM-5
		ID.AM-2: Инвентаризиране на софтуерните платформи и приложения в организацията	**CIS CSC 2** **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53, Рев. 4,** CM-8, PM-5
		ID.AM-3: Картографиране на организационната комуникация и потоците от данни	**CIS CSC 12** **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53, Рев. 4,** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Каталогизиране на външните информационни системи	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53, Рев. 4,** AC-20, SA-9
		ID.AM-5: Приоритизиране на ресурсите (напр. хардуер, устройства, данни, време, персонал и софтуер) въз основа на тяхната класификация, важност и бизнес стойност	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53, Рев. 4,** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Установяване на ролите и отговорностите по отношение на киберсигурността на цялата работна сила и заинтересованите страни на трети страни (напр. доставчици, клиенти, партньори)	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Функция	Категория	Подкатегория	Информативни референтни източници
	Бизнес среда (ID.BE): Разбиране и приоритизиране на мисията, целите, заинтересованите страни и дейностите на организацията; използване на тази информация за информиране на ролите, отговорностите и решенията за управление на риска за киберсигурността.	**ID.BE-1:** Идентифициране и комуникиране на ролята на организацията във веригите на доставки	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53, Рев. 4,** CP-2, SA-12
		ID.BE-2: Идентифициране и комуникиране на мястото на организацията в критичната инфраструктура и нейния отраслов сектор	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Клауза 4.1, **NIST SP 800-53, Рев. 4,** PM-8
		ID.BE-3: Установяване и комуникиране на приоритетите за организационната мисия, цели и дейности	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53, Рев. 4,** PM-11, SA-14
		ID.BE-4: Установяване на зависимости и критични функции за предоставяне на услуги от критично значение	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53, Рев. 4,** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Установяване на изисквания за устойчивост в подкрепа на доставката на услуги от критично значение за всички експлоатационни състояния (например при принуда/атака, по време на възстановяване, нормални операции)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53, Рев. 4,** CP-2, CP-11, SA-13, SA-14
	Ръководство (ID.GV): Разбиране на политиките, процедурите и процесите за управление и наблюдение на регулаторните, правните, оперативните изисквания и изискванията към риска и околната среда на организацията и използването им за информиране на управлението на риска за киберсигурността.	**ID.GV-1:** Установяване и комуникиране на организационната политика за киберсигурността	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53, Рев. 4,** -1 контролите от всички фамилии контроли за сигурност
		ID.GV-2: Координиране и хармонизиране на ролите и отговорностите по отношение на киберсигурността с вътрешните роли и външните партньори	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04

Функция	Категория	Подкатегория	Информативни референтни източници
			ISA 62443-2-1:2009 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53, Рев. 4,** PS-7, PM-1, PM-2
		ID.GV-3: Разбиране и управляване на правните и регулаторните изисквания по отношение на киберсигурността, включително задълженията по отношение на поверителността и гражданските свободи	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53, Рев. 4,** -1 контролите от всички фамилии контроли за сигурност
		ID.GV-4: Адресиране на рисковете за киберсигурността чрез ръководене и процеси на управление на риска	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Клауза 6 **NIST SP 800-53, Рев. 4,** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Оценка на риска (ID.RA): Разбиране на риска за киберсигурността за организационните операции (включително мисия, функции, имидж или репутация), за организационните активи и за отделни лица от страна на организацията.	**ID.RA-1:** Идентифициране и документиране на уязвимостите на активите	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53, Рев. 4,** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Получаване на информация за кибер заплахи от форуми и източници за обмен на информация	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53, Рев. 4,** SI-5, PM-15, PM-16
		ID.RA-3: Идентифициране и документиране на заплахи – както вътрешни, така и външни	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12

Функция	Категория	Подкатегория	Информативни референтни източници
			ISO/IEC 27001:2013 Клауза 6.1.2 **NIST SP 800-53, Рев. 4,** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Идентифициране на потенциални въздействия и вероятности за бизнеса	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Клауза 6.1.2 **NIST SP 800-53, Рев. 4,** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Използване на заплахи, уязвимости, вероятности и въздействия за определяне на риска	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53, Рев. 4,** RA-2, RA-3, PM-1
		ID.RA-6: Идентифициране и приоритизиране на отговори на риска	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Клауза 6.1.3 **NIST SP 800-53, Рев. 4,** PM-4, PM-9
	Стратегия за управление на риска (ID.RM): Установяване на приоритети, ограничения, толерантност към риска и допускания на организацията и използването им в подкрепа на решения по отношение на операционния риск.	**ID.RM-1:** Установяване, управляване и съгласуване на процесите на управление на риска от страна на заинтересованите страни на организацията	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Клауза 6.1.3, Клауза 8.3, Клауза 9.3 **NIST SP 800-53, Рев. 4,** PM-9
		ID.RM-2: Определяне и ясно изразяване на толерантността към риска на организацията	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Клауза 6.1.3, Клауза 8.3 **NIST SP 800-53, Рев. 4,** PM-9
		ID.RM-3: Информиране на определянето на толерантността към риска на организацията от нейната роля в критичната инфраструктура и в специфичния за сектора анализ на риска	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Клауза 6.1.3, Клауза 8.3 **NIST SP 800-53, Рев. 4,** SA-14, PM-8, PM-9, PM-11

Функция	Категория	Подкатегория	Информативни референтни източници
	Управление на риска във веригите на доставки (ID.SC): Установяване на приоритетите, ограниченията, толерантността към риска и допусканията на организацията и използването им в подкрепа на решенията, свързани управлението на риска във веригите на доставки. Установяване и внедряване на процесите за идентифициране, оценка и управление на рисковете във веригите на доставки от организацията.	**ID.SC-1:** Идентифициране, установяване, оценяване, управляване и съгласуване на процесите на управление риска във веригите на доставки в киберната инфраструктура със заинтересованите страни на организацията	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53, Рев. 4,** SA-9, SA-12, PM-9
		ID.SC-2: Идентифициране, приоритизиране и оценяване на доставчици и партньори, които се явяват трети страни по отношение на информационни системи, компоненти и услуги, с помощта на процес на оценката на риска във веригата на доставки в киберната инфраструктура	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53, Рев. 4,** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Използване на договорите с доставчици и партньори, които се явяват трети страни, за внедряване на подходящи мерки, предназначени за постигането на целите на програмата за киберсигурност на организацията и плана за управление на риска във веригите на доставки в киберната инфраструктура	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53, Рев. 4,** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Рутинно оценяване на доставчици и партньори, които се явяват трети страни, с помощта на одити, резултати от тестове или други форми на оценка, за да се потвърди, че те изпълняват договорните си задължения	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53, Рев. 4,** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

Функция	Категория	Подкатегория	Информативни референтни източници
		ID.SC-5: Провеждане на планиране и изпитване на начините за отговор и възстановяване със снабдители и доставчици, които се явяват трети страни	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53, Рев. 4,** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
ЗАЩИТА (PR)	**Управление на идентичността, автентифициране и контрол на достъпа (PR.AC):** Ограничаване на достъпа до физически и логически активи и свързани съоръжения до оторизирани потребители, процеси и устройства и управляване на достъпа в съответствие с оценения риск от неразрешен достъп до разрешени дейности и транзакции.	**PR.AC-1:** Издаване, управляване, верифициране, отнемане и одитиране на идентичности и документи за удостоверяване на идентичности за оторизирани устройства, потребители и процеси	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53, Рев. 4,** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA- 9, IA-10, IA-11
		PR.AC-2: Управляване и защита на физическия достъп до активите	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53, Рев. 4,** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Управляване на дистанционния достъп	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53, Рев. 4,** AC-1, AC-17, AC- 19, AC-20, SC-15

Функция	Категория	Подкатегория	Информативни референтни източници
		PR.AC-4: Управляване на разрешенията за достъп и оторизациите, включвайки принципите на най-малко привилегии и разделение на задълженията	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53, Рев. 4,** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Защитеност на интегритета на мрежата (например мрежова сегрегация, мрежова сегментация)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53, Рев. 4,** AC-4, AC-10, SC-7
		PR.AC-6: Доказване и свързване на идентичностите с документите за удостоверяване на идентичностите и потвърждаването им във взаимодействия	**CIS CSC** 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013** A.7.1.1, A.9.2.1 **NIST SP 800-53, Рев. 4,** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Автенифициране на потребители, устройства и други активи (например еднофакторни или многофакторни) съизмеримо с риска при транзакцията (например рискове за сигурността и неприкосновеността на лицата и други организационни рискове)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4

Функция	Категория	Подкатегория	Информативни референтни източници
			NIST SP 800-53, Рев. 4, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Осведоменост и обучение (PR.AT): Предоставяне на обучение по осведоменост в областта на киберсигурността на персонала и партньорите на организацията и обучение във връзка с изпълнението на техните задължения и отговорности, свързани с киберсигурността, в съответствие със свързаните политики, процедури и споразумения.	**PR.AT-1:** Информиране и обучаване на всички потребители	**CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53, Рев. 4,** AT-2, PM-13 PR.
		PR.AT-2: Разбиране на ролите и отговорностите от привилегированите потребители	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53, Рев. 4,** AT-3, PM-13 PR.
		PR.AT-3: Разбиране на ролите и отговорностите от заинтересованите страни, които се явяват трети страни (например доставчици, клиенти, партньори)	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53, Рев. 4,** PS-7, SA-9, SA-16 PR.
		PR.AT-4: Разбиране на ролите и отговорностите от ръководните служители	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53, Рев. 4,** AT-3, PM-13 PR.
		PR.AT-5: Разбиране на ролите и отговорностите от персонала за физическа и киберсигурност	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53, Рев. 4,** AT-3, IR-2, PM-13

Функция	Категория	Подкатегория	Информативни референтни източници
	Сигурност на данните (PR.DS): Управляване на информацията и записите(данните) в съответствие със стратегията за управление на риска на организацията с цел защита на поверителността, интегритета и наличността на информацията.	**PR.DS-1:** Защита на данните в покой	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53, Рев. 4,** MP-8, SC-12, SC-28
		PR.DS-2: Защита на данните в движение	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53, Рев. 4,** SC-8, SC-11, SC-12
		PR.DS-3: Формално управление на активите по време на отстраняване, прехвърляне и разпореждане	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53, Рев. 4,** CM-8, MP-6, PE-16
		PR.DS-4: Поддържане на адекватен капацитет за осигуряване наличността	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53, Рев. 4,** AU-4, CP-2, SC-5
		PR.DS-5: Внедряване на защити срещу изтичането на данни	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3

Функция	Категория	Подкатегория	Информативни референтни източници
			NIST SP 800-53, Рев. 4, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Използване на механизми за проверка на интегритета за верифициране на софтуера, фърмуера и интегритета на информацията	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53, Рев. 4,** SC-16, SI-7
		PR.DS-7: Разделяне на средата(ите) за разработване и изпитвване от продукционната среда	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53, Рев. 4,** CM-2
		PR.DS-8: Използване на механизми за проверка на интегритета за верифициране на интегритета на хардуера	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53, Рев. 4,** SA-10, SI-7
	Процеси и процедури за защита на информацията (PR.IP): Поддържане на политики за сигурност (касаещи целта, обхвата, ролите, отговорностите, ангажираността на управлението и координацията между организационните структури), процеси и процедури и използването им за управление на защитата на информационните системи и активи.	**PR.IP-1:** Създаване и поддържане на базова конфигурация на информационните технологии / системите за промишлен контрол, включвайки принципи за сигурност (например понятието за най-малката функционалност)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53, Рев. 4,** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Внедряване на жизнен цикъл за разработване на системи за управление на системи	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

Функция	Категория	Подкатегория	Информативни референтни източници
			NIST SP 800-53, Рев. 4, PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Съществуване на процеси за контрол на промени на конфигурацията	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53, Рев. 4,** CM-3, CM-4, SA-10
		PR.IP-4: Правене, поддържане и тестване на резервни копия (backups)	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53, Рев. 4,** CP-4, CP-6, CP-9
		PR.IP-5: Спазване на политиката и разпоредбите, касаещи физическата работна среда по отношение на организационните активи	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53, Рев. 4,** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Унищожаване на данните съгласно политиката	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53, Рев. 4,** MP-6
		PR.IP-7: Подобряване на процесите за защита	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Клауза 9, Клауза 10

Функция	Категория	Подкатегория	Информативни референтни източници
			NIST SP 800-53, Рев. 4, CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Споделяне на ефективността на технологиите за защита	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53, Рев. 4,** AC-21, CA-7, SI-4
		PR.IP-9: Съществуване и управляване на планове за отговор (отговор при инциденти и непрекъснатост на бизнеса) и планове за възстановяване (възстановяване при инциденти и възстановяване при бедствия)	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53, Рев. 4,** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Тестване на плановете за отговор и възстановяване	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53, Рев. 4,** CP-4, IR-3, PM-14
		PR.IP-11: Включване на киберсигурността в практиките на човешките ресурси (например премахване на правомощия, проверка на персонала)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53, Рев. 4,** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: Разработване и внедряване на план за управление на уязвимостите	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53, Рев. 4,** RA-3, RA-5, SI-2
	Поддръжка (PR.MA): Извършване на поддръжка и ремонт на компонентите на системите за промишлен контрол и информационните системи в съответствие с политиките и процедурите.	**PR.MA-1:** Извършване и записване на поддръжката и ремонта на организационните активи с одобрени и контролирани инструменти	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7

Функция	Категория	Подкатегория	Информативни референтни източници
			ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53, Рев. 4,** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Одобряване, записване и извършване на дистанционна поддръжка на организационните активи по начин, който предотвратява неразрешен достъп	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53, Рев. 4,** MA-4
	Защитни технологии (PR.PT): Управляване на решенията за техническа сигурност така, че да се гарантира сигурността и устойчивостта на системите и активите в съответствие със свързаните политики, процедури и споразумения.	**PR.PT-1:** Определяне, документиране, изпълнение и ревизиране на одитните/регистрационните записи съгласно политиката	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53, Рев. 4,** AU Family
		PR.PT-2: Защита на преносимите носители и ограничаване на тяхната употреба съгласно политиката	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53, Рев. 4,** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Включване на принципа на най-малката функционалност чрез конфигуриране на системите така, че да предоставят само основни способности	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6,

Функция	Категория	Подкатегория	Информативни референтни източници
			4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53, Рев. 4,** AC-3, CM-7
		PR.PT-4: Защита на комуникационните и контролните мрежи	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53, Рев. 4,** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Внедряване на механизми (например устойчивост на откази, разпределение на натоварването, „гореща“ смяна) за постигане на изискванията за устойчивост в нормални и неблагоприятни ситуации	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53, Рев. 4,** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
ОТКРИВАНЕ (DE)	**Аномалии и събития (DE.AE):** Откриване на аномалните дейности и разбиране на потенциалното въздействие на събитията	**DE.AE-1:** Установяване и управляване на базова линия на мрежовите операции и очакваните потоци от данни за потребителите и системите	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53, Рев. 4,** AC-4, CA-3, CM-2, SI-4

Функция	Категория	Подкатегория	Информативни референтни източници
		DE.AE-2: Анализиране на регистрираните събития с цел разбиране на целите и методите на атаките	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53, Рев. 4,** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Събиране и корелиране на данните за събитията от множество източници и датчици	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53, Рев. 4,** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Определяне на въздействието от събитията	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Установяване на прагове за предупреждение при инциденти	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53, Рев. 4,** IR-4, IR-5, IR-8
	Непрекъснато наблюдение на сигурността (DE.CM): Наблюдаване на информационните системи и активите за идентифициране на събития, свързани с киберсигурността, и проверяване на ефективността на защитните мерки.	**DE.CM-1:** Наблюдаване на мрежата с цел откриване на потенциални събития, свързани с киберсигурността	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53, Рев. 4,** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Наблюдаване на физическата среда с цел откриване на потенциални събития, свързани с киберсигурността	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2

Функция	Категория	Подкатегория	Информативни референтни източници
			NIST SP 800-53, Рев. 4, CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Наблюдаване на дейността на персонала с цел откриване на потенциални събития, свързани с киберсигурността	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53, Рев. 4,** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Откриване на зловреден код	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53, Рев. 4,** SI-3, SI-8
		DE.CM-5: Откриване на неразрешен мобилен код	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53, Рев. 4,** SC-18, SI-4, SC-44
		DE.CM-6: Наблюдаване на дейността на външните доставчици на услуги с цел откриване на потенциални събития, свързани с киберсигурността	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53, Рев. 4,** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Осъществяване на наблюдение за неоторизиран персонал, връзки, устройства и софтуер	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53, Рев. 4,** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Извършване на сканиране за уязвимости	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53, Рев. 4,** RA-5

Функция	Категория	Подкатегория	Информативни референтни източници
	Процеси на откриване (DE.DP): Поддържане и тестване на процеси и процедури за откриване, за да се гарантира осведомеността за аномални събития.	**DE.DP-1:** Ясно дефиниране на ролите и отговорностите, свързани с откриване, с цел осигуряване на отчетност	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53, Рев. 4, CA-2, CA-7, PM-14
		DE.DP-2: Съответствие на дейностите по откриване с всички приложими изисквания	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53, Рев. 4,** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Тестване на процесите на откриване	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53, Рев. 4,** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Комуникиране на информацията за откриване на събития	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53, Рев. 4,** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Непрекъснато подобряване на процесите на откриване	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53, Рев. 4,,** CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
ОТГОВОР (RS)	**Планиране на отговора (RS.RP):** Изпълнение и поддържане на процеси и процедури за отговор с цел гарантиране на отговор на регистрирани инциденти, засягащи киберсигурността.	**RS.RP-1:** Изпълнение на план за отговор по време на инцидент или след него	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53, Рев. 4,** CP-2, CP-10, IR-4, IR-8

Функция	Категория	Подкатегория	Информативни референтни източници
	Комуникации (RS.CO): Координиране на дейностите за отговор с вътрешни и външни заинтересовани страни (например външна подкрепа от правоприлагащи органи).	**RS.CO-1:** Персоналът знае своите роли и реда на операциите, когато е необходим отговор	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53, Рев. 4,** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Докладване на инцидентите в съответствие с установените критерии	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53, Рев. 4,** AU-6, IR-6, IR-8
		RS.CO-3: Обменяне на информацията в съответствие с плановете за отговор	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Клауза 7.4, Клауза 16.1.2 **NIST SP 800-53, Рев. 4,** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Осъществяване на координацията със заинтересованите страни в съответствие с плановете за отговор	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Клауза 7.4 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-8
		RS.CO-5: Осъществяване на доброволен обмен на информация с външни заинтересовани страни за постигане на по-широка ситуационна осведоменост относно киберсигурността	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53, Рев. 4,** SI-5, PM-15

Функция	Категория	Подкатегория	Информативни референтни източници
	Анализ (RS.AN): Осъществяване на анализ, за да се гарантира ефективен отговор и подпомагане на дейностите по възстановяване	**RS.AN-1:** Изследване на уведомленията от системите за откриване	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53, Рев. 4,** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Съществува разбиране за въздействието на инцидента	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53, Рев. 4,** CP-2, IR-4
		RS.AN-3: Извършване на криминологични анализи	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53, Рев. 4,** AU-7, IR-4
		RS.AN-4: Категоризиране на инцидентите в съответствие с плановете за отговор	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Установени са процеси за получаване, анализиране и реагиране на уязвимости, оповестени на организацията от вътрешни и външни източници (например вътрешни тестове, бюлетини за сигурност или изследователи по сигурността)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53, Рев. 4,** SI-5, PM-15
	Смекчаване (RS.MI): Извършване на дейности за предотвратяване разширяването на дадено събитие, смекчаване на ефектите от него и разрешаване на инцидента.	**RS.MI-1:** Ограничаване на инцидентите	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53, Рев. 4,** IR-4

Функция	Категория	Подкатегория	Информативни референтни източници
		RS.MI-2: Смекчаване на инцидентите	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53, Рев. 4,** IR-4
		RS.MI-3: Смекчаване или документиране на новоидентифицираните уязвимости като приети рискове	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53, Рев. 4,** CA-7, RA-3, RA-5
	Подобрения (RS.IM): Подобряване на дейностите за отговор на организацията чрез използване на научените уроци от предишни дейности за откриване/отговор.	**RS.IM-1:** Включване на научените уроци в плановете за отговор	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Клауза 10 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-8
		RS.IM-2: Актуализиране на стратегиите за отговор	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Клауза 10 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-8
ВЪЗСТАНОВЯВАНЕ (RC)	**Планиране на възстановяването (RC.RP):** Изпълнение и поддържане на процеси и процедури за възстановяване с цел гарантиране възстановяването на системите или активите, засегнати от инциденти, засягащи киберсигурността.	**RC.RP-1:** Изпълнение на план за възстановяване по време на инцидент, свързан с киберсигурността, или след него	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53, Рев. 4,** CP-10, IR-4, IR-8
	Подобрения (RC.IM): Подобряване на планирането и процесите на възстановяване чрез включване на научените уроци в бъдещи дейности.	**RC.IM-1:** Включване на научените уроци в плановете за възстановяване	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Клауза 10 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-8
		RC.IM-2: Актуализиране на стратегиите за възстановяване	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Клауза 10 **NIST SP 800-53, Рев. 4,** CP-2, IR-4, IR-8

Функция	Категория	Подкатегория	Информативни референтни източници
	Комуникации (RC.CO): Координиране на дейностите по възстановяване с вътрешни и външни страни (например координационни центрове, доставчици на Интернет услуги, собственици на атакуващи системи, жертви, други екипи за реагиране при инциденти с компютърната сигурност (CSIRT) и оператори).	**RC.CO-1:** Управляване на връзките с обществеността	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Клауза 7.4
		RC.CO-2: Възстановяване на репутацията след инцидент	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Клауза 7.4
		RC.CO-3: Комуникиране на дейностите за възстановяване на вътрешни и външни заинтересовани страни, както и на ръководни и управленски екипи	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Клауза 7.4 **NIST SP 800-53, Рев. 4,** CP-2, IR-4

Информация относно Информативни референтни източници, описани в Приложение А, може да бъде намерена на следните места:

- Цели за контрол на информационните и свързаните с тях технологии (Control Objectives for Information and Related Technology (COBIT)): http://www.isaca.org/COBIT/Pages/default.aspx
- Критични контроли за сигурност на Центъра за интернет сигурност за ефективна киберзащита (CIS Critical Security Controls for Effective Cyber Defense (CIS Controls)): https://www.cisecurity.org
- Американски национален институт по стандартизация/Международно общество по автоматизация (American National Standards Institute/International Society of Automation (ANSI/ISA))-62443-2-1 (99.02.01)-2009, *Сигурност за системи за промишлена автоматизация и управление:Създаване на програма за сигурност на системи за промишлена автоматизация и управление (Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program):* https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Сигурност за системи за промишлена автоматизация и управление: Изисквания за сигурност на системата и нива на сигурност (Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels):* https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Информационни технологии – Методи за сигурност – Системи за управление на информационната сигурност – Изисквания (Information technology -- Security techniques -- Information security management systems -- Requirements):* https://www.iso.org/standard/54534.html
- Специалната публикация 800-53 на Националния институт по стандарти и технологии, Ревизия 4 (NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4), *Контроли на сигурността и поверителността за федералните информационни системи и организации (Security and Privacy Controls for Federal Information Systems and Organizations),* април 2013 г. (включително актуализации към 22 януари 2015 г.). https://doi.org/10.6028/NIST.SP.800-53r4. Информативните референтни източници са картографирани само до нивота на контрола, въпреки че всяко подобрение на контрола може да се окаже полезно за постигане на резултат от Подкатегорията.

Каптографирания между Подкатегориите на Ядрото на Рамката и посочените раздели в Информативните референтни източници нямат за цел да определят окончателно дали посочените раздели в Информативните референтни източници осигуряват желания резултати от Подкатегорията.

Информативните референтни източници не са изчерпателни в това, че не всеки елемент (напр. контрол или изискване) на даден Информативен референтен източник е съотнесен към Подкатегории на Ядрото на Рамката.

Приложение Б: Кратък речник

В това Приложение са дефинирани избрани термини, използвани в публикацията.

Таблица 3: Речник на термините, използвани в Рамката

Възстановяване (Функция)	Разработване и внедряване на подходящите дейности за поддържане на планове за устойчивост и за възстановяване на всички способности или услуги, които са били влошени вследствие на събитие, засягащо киберсигурността.
Доставчик	Доставчици на продукти и услуги, които се използват за вътрешни цели на организацията (например инфраструктурата на информационните технологии (IT))) или се интегрират в продуктите на услугите, предоставяни на Купувачите на тази организация.
Защита (Функция)	Разработване и внедряване на подходящите предпазни мерки за гарантиране на доставката на услуги на критичната инфраструктура.
Идентифициране	Развиване на организационното разбиране за управлението на риска за киберсигурността за системите, активите, данните и способностите.
Информативен референтен източник	Специфичен раздел от стандарти, насоки и практики, общи за секторите на критичната инфраструктура, който илюстрира метод за постигане на резултатите, свързани с всяка Подкатегория. Пример за Информативен референтен източник е Контрол A.10.8.3 на ISO/IEC 27001, който поддържа „Защита на данните в движение“, Подкатегория от Категорията „Сигурност на данните“ във Функцията „Защита“.
Инцидент, засягащ киберсигурността	Събитие, свързано с киберсигурността, за което е определено, че има въздействие върху организацията, предизвикващо необходимостта от отговор и възстановяване.
Категория	Подразделянето на дадена Функция на групи от резултати за киберсигурността, тясно свързани с програмни нужди и конкретни дейности. Като примери на Категории могат да се почота: „Управление на активите“, „Управление на идентичността и контрол на достъпа“, „Процеси на откриване“.
Купувач	Хората или организациите, които консумират даден продукт или услуга.
Киберсигурност	Процесът на защита на информацията чрез предотвратяване, откриване и отговаряне на атаки.
Критична инфраструктура	Системи и активи, физически или виртуални, толкова жизненоважни за Съединените щати, че непригодността или разрушаването на тези системи и активи биха оказали омаломощаващо въздействие върху киберсигурността, сигурността на националната икономика, националното обществено здраве и безопасност, или всяка комбинация от тях.
Мобилен код	Програма (например скрипт, макрос или друга преносима инструкция), която може да бъде изпратена непроменена на хетерогенен сбор от платформи и изпълнена с идентична семантика.
Ниво на изпълнение на Рамката	Обектив, през който да се видят характеристиките на подхода към риска на дадена организация: по какъв начин организацията вижда риска за киберсигурността и какви процеси има за управлението на този риск.
Отговор (Функция)	Разработване и изпълнение на подходящите дейности за предприемане на действия по отношение на събитие, свързано с киберсигурността.
Откриване (Функция)	Разработване и изпълнение на подходящите дейности за идентифициране на появата на събитие, засягащо киберсигурността.

Рамка	Подход, базиран на риска, за намаляване на риска за киберсигурността, състоящ се от три части: Ядрото на Рамката, Профилът на Рамката и Нивата на изпълнение на Рамката. Известна също като „Рамка за киберсигурност“.
Подкатегория	Подразделянето на дадена Категория на специфични резултати от техническите и/или управленските дейности. Като примери на Подкатегории могат да се посочат: „Каталогизиране на външните информационни системи“, „Защита на данните в покой“, „Изследване на уведомленията от системите за откриване“.
Привилегирован потребител	Потребител, който е упълномощен (и следователно надежден) да изпълнява функции, свързани със сигурността, които обикновените потребители не са упълномощени да изпълняват.
Профил на Рамката	Представяне на резултатите, които дадена система или организация е избрала от Категориите и Подкатегориите на Рамката.
Риск	Мярка за степента, до която даден субект е застрашен от потенциално обстоятелство или събитие, и обикновено е функция на: (i) неблагоприятните въздействия, които биха възникнали, ако настъпи това обстоятелство или събитие; и (ii) вероятността от възникване.
Събитие, свързано с киберсигурността	Промяна в киберсигурността, което може да окаже въздействие върху организационните операции (включително върху мисията, способностите или репутацията).
Таксономия	Схема на класификация.
Управление на риска	Процесът на идентифициране, оценяване и реагиране на рискове.
Функция	Един от главните компоненти на Рамката. Функциите осигуряват най-високото ниво на структура за организиране на основните дейности по киберсигурността в Категории и Подкатегории. Петте Функции са: Идентифициране, Защита, Откриване, Отговор и Възстановяване.
Ядро на Рамката	Съвкупност от дейности и референтни източници, които са общи за секторите на критичната инфраструктура и са организирани с оглед на конкретни резултати. Ядрото на Рамката се състои от четири вида елементи: Функции, Категории, Подкатегории и Информативни референтни източници.

Приложение B: Акроними

В това Приложение се дефинират избрани акроними, използвани в публикацията.

ANSI	American National Standards Institute	Американски национален институт по стандартизация
CEA	Cybersecurity Enhancement Act of 2014	Закон за подобряване на киберсигурността от 2014 г.
CIS	Center for Internet Security	Център за Интернет сигурност
COBIT	Control Objectives for Information and Related Technology	Цели за контрол на информационните и свързаните с тях технологии
CPS	Cyber-Physical Systems	Кибер-физични системи
CSC	Critical Security Control	Критичен контрол за сигурност
DHS	Department of Homeland Security	Департамент за вътрешна сигурност
EO	Executive Order	Изпълнителна заповед
ICS	Industrial Control Systems	Системи за промишлен контрол
IEC	International Electrotechnical Commission	Международна електротехническа комисия
IoT	Internet of Things	Интернет на нещата
IR	Interagency Report	Междуведомствен доклад
ISA	International Society of Automation	Международно общество по автоматизация
ISAC	Information Sharing and Analysis Center	Център за обмен и анализ на информация
ISAO	Information Sharing and Analysis Organization	Организация за обмен и анализ на информация
ISO	International Organization for Standardization	Международна организация по стандартизация
IT	Information Technology	Информационни технологии
NIST	National Institute of Standards and Technology	Национален институт по стандарти и технологии
OT	Operational Technology	Оперативни технологии
PII	Personally Identifiable Information	Информация, позволяваща лично идентифициране
RFI	Request for Information	Искане за предоставяне на информация
RMP	Risk Management Process	Процес на управление на риска
SCRM	Supply Chain Risk Management	Управление на риска във веригите на доставки
SP	Special Publication	Специална публикация