РЕПУБЛИКА БЪЛГАРИЯ

Актуализирана
Национална стратегия за киберсигурност

„КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023 ”

Министерски съвет

София, 2021

СЪДЪРЖАНИЕ

В Република България се провежда единна национална политика за киберсигурност, която разглежда системата за киберсигурност, като част от системата за защита на националната сигурност. Киберсигурността се определя като състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им. Страната ни участва активно във формирането и осъществяването на политиките за киберсигурност в рамките на ЕС и НАТО и се стреми към постигане на киберустойчивост на цялото общество и държава.

Приета бе и се изпълнява Национална стратегия за киберсигурност "Киберустойчива България 2020"[1], основополагащ документ за единно формиране, планиране, осъществяване, координиране и контрол на политиката в областта на киберсигурността, провеждана от държавните институции в сътрудничество с бизнеса, гражданите и техните организации. Националната стратегия е синхронизирана със Стратегията на ЕС за киберсигурност от 2013 г., и е съобразена с изискванията на Директивата на ЕС[2] за мрежова и информационна сигурност. Постигната е висока степен на съгласуваност и приемственост между двата документа, отнасящи се до националното и европейското равнище на сигурност. В изпълнение на Директивата, Националната стратегия бе изпратена на Европейската комисия и на страните-членки, като Комисията е дала положителна оценка за съответствие. Документът е предоставен и на всички партньорски държави от НАТО.

Националната стратегия за киберсигурност изразява колективния ангажимент и отговорност на всички заинтересовани страни и волята на Правителството на Република България да гарантира **отворено, безопасно и сигурно киберпространство.**

В Програмата за управление на правителството за периода 2017 – 2021 г. са включени мерки за изпълнение на ключови приоритетите в областта на обществения ред, сигурността и отбраната. Разписани са дейности за реализиране на Националната стратегия за киберсигурност; дейности за минимизиране на рисковете и неутрализиране на опасностите за националната сигурност; за развитие на способностите в сферата на отбраната за противодействие на кибератаки и хибридно въздействие.

През периода 2017-2019 г. са разработени и приети основните нормативни актове[3], с които е създадена правната и регулаторната рамка за киберсигурност. Със закон са определени организацията и управлението на системата за киберсигурност, установен е механизмът за координирани действия на политическо и стратегическо ниво, посочени са компетентните органи по мрежова и информационна сигурност и техните отговорности, регламентиран е общият ред за оперативно взаимодействие между съответните институции и специализираните структури. Регламентирани са и задълженията на административните органи; лицата, осъществяващи публични функции; организациите, предоставящи обществени услуги; операторите на съществени услуги; доставчиците на цифрови услуги по отношение на изискванията за киберсигурност и уведомяване при киберинциденти. С Наредбата за минималните изисквания за мрежова и информационна сигурност са регламентирани минималните мерки за управление на мрежовата и

1 Приета с Решение на Министерски съвет №583/18.07.2016

2 Директива (ес) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

3 Закон за киберсигурност, Обн. ДВ. бр.94 от 13 Ноември 2018г.; Наредба за минималните изисквания за мрежова и информационна сигурност, Обн. ДВ. бр.59 от 26 Юли 2019г.

информационна сигурност, мерките за защита и устойчивост. Въведени са правила за извършване на проверки за съответствие с изискванията за мрежова и информационна сигурност; определен е реда за водене, съхраняване и достъп до регистъра на съществените услуги и са стандартизирани формите за уведомленията за инциденти, формата за обобщена статистическа информация за инциденти, и е уеднаквена таксономията и приоритизацията в тази област.

С приемането на Закона за киберсигурност и свързаните с него нормативни актове и осъщественото институционално изграждане бе постигнат сериозен напредък, който даде тласък за изпълнение на мерките, заложени в Стратегията. Хоризонталната политиката за киберсигурност е нова област на управление и реализирането й изисква не само значителни средства за създаване на капацитети и способности на държавата, бизнеса и обществото, но и формиране на изцяло нова култура на киберхигиена. В този контекст се отчита известно забавяне при изпълнение на част от мерките, предвидени в Националната стратегия за киберсигурност.

В периода на изпълнение на Стратегията се отчита четирикратно увеличаване на броя постъпили сигнали за извършени компютърни престъпления. Констатира се усложняване на киберкартината в страната, което се потвърждава и от увеличението с 45 % на броя на получените сигнали за киберинциденти за тригодишен период, като тези с висок приоритет нарастват с 29 %.[4] Значителен обществен резонанс предизвикаха киберинциденти с прекъсване на услугите на Търговския регистър през м. август 2018 г., както и кибератаката срещу информационната система на НАП през м. юли 2019 г. В последната година два фактора оказват съществено влияние върху картината на застрашеност в киберпространството - въздействието на пандемията COVID - 19 и нарастващите възможности на извършителите на киберзаплахи. Наблюдаваните съществени промени през 2019 и 2020 г. в киберкартината на заплахите и рисковете за киберсигурността в национален и общоевропейски план (вкл. масирани кибератаки и връзка между кибератаки, хибридни заплахи и тероризъм, опити за намеса в демократични процеси и пряко в избори) налагат съответни промени в Националната стратегия за киберсигурност "Киберустойчива България 2020".

Актуализацията на Стратегията се налага и с оглед ускореното развитие на процеса на цифрова трансформация, както и от съображения, свързани с изтичането на срока на Програмата за управление на правителството. Внасянето на промени в Стратегията е съобразено с приетата Стратегия на ЕС за Съюза на сигурност[5] с обхват 2020—2025 г., в която на базата на анализ на заплахите се посочват четири взаимосвързани стратегически приоритета. На първо място е изведено изграждането на способности и капацитет за осигуряване на среда на сигурност, подготвена за бъдещето, като в сферата на киберсигурността е подчертана необходимостта от подход, който обхваща цялото общество и при който институциите, агенциите и органите на ЕС, държавите-членки, промишлеността, академичните среди и физическите лица отдават на киберсигурността дължимия приоритет. Констатирано е, че правната рамка за защита и устойчивост на

4 Статистически данна за периода 2018-2020 г.на НЕРИКС – ДАЕУ

5 СЪОБЩЕНИЕ на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегията на ЕС за Съюза на сигурност - **COM(2020) 605 final 24.07.2020**

критичните инфраструктури[6] не е в синхрон с променящите се рискове и са необходими адекватни мерки за тяхната защита и устойчивост, които адресират както физическата сигурност, така сигурността на киберпространството. Следващият стратегически приоритет на Стратегията на ЕС за съюз на сигурност е ефективното справяне с киберпрестъпността, което е възможно само ако правоприлагащите органи работят в сферата на цифровите разследвания с ясни правила за разследване и наказателно преследване на престъпленията и предоставяне на необходимата защита на жертвите. Най-широката осведоменост на обществото следва да се превърне в ключов приоритет, за да могат гражданите да са в течение за рисковете и превантивните мерки, които сами биха могли да предприемат. Това е част от един проактивен подход, допълващ действията за пълното прилагане на действащата законова рамка. Следващият стратегически приоритет е изграждане на силна европейска екосистема на сигурност и в частност, сътрудничеството и обмена на информация.

За успешно реализиране на хоризонталната политика за цифровизация и киберсигурност са необходими нови и значими по обем инвестиции. Поради това в проекта на План за възстановяване и устойчивост[7] правителството предвижда в средносрочна перспектива осигуряване на финансови средства за преодоляване забавянето на цифровизацията в България. Подобрената среда за пренос на данни, както и цифровата свързаност и високата защита на публичните институции, администрациите и потребителите, ще позволят адекватно осъществяване на предвидените по Кохезионната политика мерки за осигуряване на високо ниво на киберсигурност. В тази връзка при актуализирането на Националната стратегията за киберсигурност са взети под внимание възможностите за оптимално използване на достъпа до финансиране по Механизма за възстановяване и устойчивост на ЕС, както и средствата от европейските фондове и оперативни програми през следващия програмен период 2021-2027 г. Това ще позволи иницииране и осъществяване на пакети от проекти.

Актуализацията на Националната стратегия за киберсигурност „Киберустойчива България 2020“ е съобразена с приетата наскоро **Националната програма за развитие България 2030**[8]**.** В рамките на приоритета „Институционална рамка“ програмата посочва, че мрежовата и информационна сигурност е пряко свързана с доверието на потребителите в електронните услуги, а безопасното и широко използване на продукти и услуги, базирани на данни зависи от потигането на най-високи стандарти за киберсигурност. Визията и целите на политиката за цифрова трансформация на Република България за периода 2020-2030 г.[9] потвърждават ключовата взаимнозависимост межу цифровите технологии и киберсигурността. В тази връзка при актуализацията на националната стратегия за киберсигурност следва да се постигне съгласуваност както с целите така и с времевия хоризонт на приетите нови стратегически документи. Наложително е да се определят и реалистични етапи за нейното изпълнение.

За изпълнение на целите и набелязаните мерки на Актуализираната стратегия ще се разработи Пътна карта към нея, която ще се приеме от Министерски съвет, в изпълнение

6 Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г.); Директива 2008/114/ЕО на Съвета относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

7 В процедура по съгласуване с Европейската комисия, преди приемане от Министерски съвет.

8 Приета с Протокол № 67 на Министерския съвет от 02.12.2020 г.

9 Национален стратегически документ “Цифрова трансформация на България за периода 2020-2013”, приет с Решение на Министески съвет №493/21.07.2020

на Закона за киберсигурност. Мониторинг и оценка на изпълнението и периодична актуализация на Стратегията и Пътната карта се осъществява от Съвета по киберсигурност.

1. България – киберсигурност за цифрова трансформация в сложна и наситена със заплахи среда

1.1 Цифрова зависимост, заплахи и киберсигурност

Информационните и комуникационните технологии (ИКТ) са основен елемент на цифровата промяна в Европа – от „умните“ крайни устройства до високоскоростния интернет, мобилните приложения и научните изследвания в областта на бъдещите и нововъзникващи технологии. ИКТ, заедно с ефективно организирани научни изследвания и образование, са и основополагащ фактор за изграждането на конкурентноспособна икономика, основана на знанието.

Информационните и комуникационните технологии са в основата на системи, които поддържат ежедневната дейност на държавните институции, бизнеса и гражданите, правят възможно функционирането на икономиката в ключови сектори като здравеопазване, енергетика, финанси и транспорт, екология и цифрова инфраструктура и не на последно място отбрана, сигурност, управление при кризи. Държавата, бизнесът и гражданите, разчитат на лесен достъп и надеждно функциониране на комуникационните и информационните системи и технологии и интернет средата. През следващото десетилетие се очаква на територията на ЕС да има изключително голям брой свързани цифрови устройства, тъй като цифровизацията и свързаността се превръщат в основни характеристики на все по-голям брой продукти и услуги, както и с новите технологии като „интернет на предметите“, големите информационни масиви и др.

В края на 2020 г. в България близо 79 % от домакинствата и над 95 % от нефинансовите предприятия[10] използват интернет, като съществено нараства броя на предприятията осъществяващи автоматизиран обмен на данни с външни ИКТ системи. Почти цялата комуникация на публичната администрация с бизнеса е само електронна. Нарастват и услугите към гражданите, които се извършват по интернет. Интернет свързаността и скоростта на информационните канали непрекъснато расте – през 2020 г. България е на 39-то място в света от 221 държави по скорост на интернет, показва класацията Worldwide Broadband Speed League на Cable.co.uk , а със средна скорост от 82.42 Mbps за ноември 2020 г. се подрежда на дванадесето място сред страните с най-висока скорост на мобилните данни (виж: www.speedtest.net/global-index). Интензифицирането на усилията по подобряване и ускоряване разгръщането на широколентовия достъп до интернет и широкомащабното разгръщане на цифровата инфраструктура[11], ще предоставят нови възможности за отдалечени и облачни услуги, но и нови възможности за мащабно и злонамерено използване.

10 НСИ – изследване: https://www.nsi.bg/sites/default/files/files/pressreleases/ICT_hh2020_PSRP7D5.pdf
https://www.nsi.bg/sites/default/files/files/pressreleases/ICT_ent2020_PSRP7D5.pdf

11 Национален стратегически документ “Цифрова трансформация на България за периода 2020-2013”, приет с Решение на Министески съвет №493/21.07.2020

Цифровите инфраструктури са критичен фактор за управлението и предвидимото функциониране на ресурсите и системите с национално значение, на модерната и иновативна икономика, на прозрачното управление, на свободното и демократично гражданско общество.

Киберпространството предоставя големи възможности за развитие, но води и до нарастваща и необратима цифрова зависимост на основните функции и дейности в обществото. Злонамерени или неумишлени действия могат да доведат до нарушаване работата на системите за управление и устройствата, свързани с критичната инфраструктура и възпрепятстване на нормалното им функциониране. Заплахите и рисковете в киберпространството са трудни за дефиниране поради сложността на определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата, трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите. Идентифицирането, защитата и минимизирането на тези заплахи и рискове не са традиционни и изискват нова култура на взаимодействие между участниците в киберпространството.

В края на второто десетилетие мащабните кибератаки се нареждат на трето място, по отношение вероятността от осъществяване, след климатичните промени и природните бедствия, а киберзависимостта е вторият фактор, който ще определя глобалната картина на рисковете за държави, икономика и общество през следващите десет години[12].

През 2020 г. пандемията COVID – 19 ускори внедряването на ИКТ за управление и координиране на здравните власти, преминаването към дистанционен режим на работа, широкото използване на телеконференциите като ефективен работен формат, дистанционното обучение в електронна среда. Бурно развитие се наблюдава в електронната търговия, банковите разплащания, застрахователното дело. Нарастването на цифровизацията и свързаността увеличават рисковете за обществото. Пандемията направи социалните и икономическите норми на поведение още по – зависими от сигурното и надеждно киберпространство.

Еднакво засегнати от случайни киберинциденти или целенасочени кибератаки са публичният и частният сектор, както и цялото общество. По своята природа кибератаките са „асиметрични“ – с малки усилия и инвестиции могат да бъдат нанесени огромни поражения. Атаките, осъществявани през интернет са комплексни, организирани и използват широк спектър от така наречените „**съвременни упорити заплахи“**[13]**,** с продължителен скрит период и потенциал да прераснат в **национална криза, предизвикана от намеса в киберпространството**.

Кибератаките срещу **критични инфраструктури (КИ)** и уязвимости на техните системи за управление и комуникация са с най-голям потенциал за нанасяне на значително увреждащо въздействие. Нарушение в работата на общата и споделена **критична комуникационно - информационна инфраструктура (ККИИ)** оказва изключително въздействие върху обществото с непредвидими и потенциално катастрофални последици. Свързаността и зависимостта в киберпространството позволяват пробивът в сигурността или дефектът на една комуникационна и информационна система от даден сектор да доведат до каскаден ефект в други сектори със

12 http:/reports.weforum.org/global-risk-2018/global-risks-2018-fractures-fears-and-failures/

13 Advanced Persistent Threats (APT)

сериозни възможни последици, включително и до невъзможност за предоставяне на жизненоважни услуги. Реакцията при мащабни инциденти налага координирани действия и превантивни мерки за минимизиране възможностите за прерастване в кризи, както и за адекватни последващи действия за своевременното възстановяване на нормалното функциониране на системите.

Значителна част от кибератаките са злонамерени действия, извършени за получаване на финансови облаги. Киберпрестъпления се извършват и с цел тормоз, измама, разпространение на детска порнография, нарушаване правата на интелектуалната собственост. Изнудването остава широко разпространено, като нанася значителни щети или причинява големи вредни последици на потърпевшите. Противодействието срещу **киберпрестъпността** се усложнява от нарастващия брой и разнообразието на атаките, от пораженията и мотивация на хората, извършващи тези атаки.

Източници на организирани кибератаки може да са държавни, военни и терористични организации, лица и структури, извършващи индустриален шпионаж, трансгранични мрежи и организирани престъпни групи. Източник на растяща заплаха от особено голям мащаб са държавно–спонсорирани актьори - държави с тоталитарни режими и такива с неукрепнала демократична система, с доктрина за водене на информационни, кибер и хибридни войни. Тези държави, както и различни не-държавни или терористични групировки, развиват специализирани способности за **кибертероризъм** и водене на **кибервойни** чрез прилагане на целия набор от методи, въздействащи върху комуникационните и информационните системи за нарушаване на физическата, персоналната, информационната и комуникационната сигурност. Сред най-сериозните деструктивни въздействия са тези от хибриден характер. Пулсиращи, краткотрайни, но много интензивни атаки към много цели едновременно, както и сложността и обхвата на въздействието могат да засегнат всички сфери на обществото и да се превърнат в **хибридна война** срещу държава или група от държави. С деструктивен характер са и заплахите, свързани с тенденцията на разпространение и засилване на **радикализацията и на тероризма** в глобален план, като **киберпространството се превърна във важна арена** и източник на рискове за сигурността на гражданите, бизнеса и държавата. Интернет се използва като основен канал за манипулирана информация и пропаганда, създаване на психоза, привличане на последователи, терористи и подпомагане на терористични организации.

Координираното развитие на капацитета и способностите на обществото чрез ангажиране на **всички заинтересовани страни** гарантира достигане на **ново ниво на зрялост в киберпространството – киберустойчивост.** То се характеризира със способности за посрещане на неочаквани, преднамерени или непреднамерени заплахи, за адресиране на динамично променящи се рискове, за адекватна реакция, овладяване и възстановяване.

Киберустойчивостта изисква обществото да притежава капацитет и готовност за справяне с „неизвестните неизвестни“, ограничаване на вредните последствия, максимално запазване и функциониране на жизненоважните дейности и услуги, и своевременно възстановяване. Постигането ѝ изисква сигурност и надеждност на цялата **цифрова екосистема** - информация, организация и процеси, технологии, хора и съоръжения, както и специфични изисквания към дизайна и реализацията на комуникационните канали, системите и услугите, надеждната им свързаност и оперативна съвместимост.

1.2 Предизвикателства, заплахи и рискове, възможности на национално ниво

България е част от глобалния процес на цифровизация и повишаващата се цифрова зависимост. **Осъществява се процес на реформа на държавното управление,** икономическото и обществено развитие **чрез внедряване на електронните услуги.** Изискванията за киберсигурност са от съществено значение за успешното реализиране на **електронното управление**. Предизвикателствата, освен свързаните с техническата защита и надеждност, са и в изграждането на доверие и култура на ползване, както и в своевременното докладване на инциденти и проблеми.

Широкото използване на социалните мрежи и интернет в обществените отношения, добавя и съответните по значимост, мащаб и бързодействие киберзаплахи. Разпространението на фалшиви новини създава смут и паника сред населението, модифицирането на лица, говор и жестове на значими политически фигури, манипулирането на пазарното поведение на потребителите са възможен елемент от хибридна война и предизвикателство, на което се търси отговор.

Новите технологии и **тенденциите за развитие** дават големи възможности на бизнеса, но също така водят и до нови, все още недостатъчно предвидими заплахи и предизвикателства. С развитието на облачните услуги, на Уеб 4.0 технологиите, 5G комуникациите с акцент върху защитата и контрола на личното пространство и данните, все по-богатите мултимедийни форми за комуникация в социалните мрежи, „интернет на сигурните предмети“[14], системите с изкуствен интелект, преминаването към виртуални валути, квантовите технологии, ролята на Космоса в киберпространството и др. се очаква да нарастват рисковете от типа „съвременни упорити заплахи“, които могат да въздействат върху критични за обществото ресурси, системи и услуги в Република България.

Специфичен елемент в страната е съществуването на голямо многообразие от информационни системи с различно предназначение и функционалности, въвеждани в различни периоди и в различна степен на зрялост спрямо оперативната съвместимост и мрежовата и информационна сигурност(МИС), включително комуникационни и информационни системи, действащи в критични сектори.

Киберсигурността е ключов елемент на **националната сигурност**. Киберпространството се определя като **пета област/домейн**[15] за провеждане на военни операции, операции срещу националните интереси, териториалната цялост, националната сигурност на суверенни държави, срещу правата и свободите на гражданите[16]. Увеличаването на рисковете и заплахите в **геополитическата и стратегическата среда за сигурност** и в частност в киберпространството създават условия за увеличаване на уязвимостите на стратегическите граждански и военни комуникационно-информационни системи и на системите за командване и управление на силите, участващи в мисии и

14 IoT - Internet of Things - умни устройства, свързани в интернет /Интернет на сигурните предмети/

15 В допълнение към земя, море, въздух и космическо пространство. НАТО определи киберпространството като област за провеждане на военни операции

16 NATO - http://www.nato.int/cps/en/natohq/topics_78170.htm

** NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23.05.2019, https://www.nato.int/cps/en/natohq/opinions_166039.htm

операции на и извън територията на страната. Това налага адекватно и своевременно развитие и придобиване на способности за **киберотбрана**, като неразделна част от способностите за защита на системата за управление на националната сигурност, свързани с отбраната и гарантирането на териториалната цялост на Република България, с подкрепата на международния мир и сигурност в съюзен и коалиционен формат и принос на Въоръжените сили към националната сигурност в мирно време при овладяване на кризи от невоенен характер.

„Кибератаките могат да доведат до щети, не по-малки от тези, причинени по конвенционалните методи. Една единствена атака е в състояние да причини на нашите икономики загуби в размер на милиарди долари, да доведе до стагнация на световните компании, да парализира нашата критична инфраструктура, да подкопае демокрацията и да постави пред сериозно изпитание нашите военни способности.

Кибератаките добиват все по-интензивен, комплексен и разрушителен характер. Варират от отделни опити до високотехнологични сложни атаки. Те могат да бъдат извършени от държавни и недържавни участници. От непосредствена близост или от голяма дистанция. Могат да засегнат всеки един от нас.

... Лидерите на НАТО се съгласиха, че кибератака може да задейства член 5 от учредителния договор. Атаката срещу един съюзник се възприема като атака срещу всички. НАТО определя киберпространството като военна област.“

*Йенс Столтенберг, генерален секретар на НАТО***

Възможностите за справяне с предизвикателствата от необратимото пренасяне на основните дейности на обществото, бизнеса и държавното управление в киберпространството са:

- Повишаване ефективността на технологиите при намаляващи цени; възможности за постигане на решения, основани на оптимално съотношение направени разходи – реализирани ползи;
- Практически неограничен достъп до динамичен и глобален пазар на продукти и услуги в областта на киберсигурността – достъп до технологии, свързани с криптографията, криптоанализа и откриването на неправомерен достъп;
- Широк достъп до знание, ноу хау, добри практики и решения в областта на киберсигурността;
- Възможности, произтичащи от членството в ЕС и НАТО с пряко въздействие върху разработване на съгласувани политики, подходящо законодателство, ефективно функциониращо сътрудничество в сферата на МИС, получаване на съдействие при необходимост, реализиране на съвместни проекти, учения, обучителни и тренировъчни дейности;
- Правителствена политика, гарантираща подкрепа и осигуряваща мащабно финансиране на приоритетите и дейностите в областта на киберсигурността. Използване на проектното управление за постигане на киберустойчиво общество, ефективността на което значително би се повишила с разработване и изпълнение на

единна национална програма за киберустойчивост в подкрепа на всички електронни услуги. Реализиране на проекти в рамките на годишните национални индикативни планове по Фонд "Вътрешна сигурност"; планирани инвестиции за реформи по Плана за възстановяване и устойчивост, по новите оперативните програми за следващия програмен период 2021-2027 г. Приоритет ще се дава на проекти, които са част от приоритетните вериги на стойността на ЕС. От особена важност са възможностите за съвместен отговор в ЕС чрез програмите „Цифрова Европа" и „Хоризонт Европа", както и програмите в Организацията за комуникация и информация на НАТО.

2. Визия „Киберустойчива България"

Цифровата свързаност е ядрото на цифровата трансформация, а сигурното киберпространство и доверието са основни фактори за нейното успешно осъществяване. До 2030 г. България трябва да постигне киберустойчивост и да изгради функционираща, надеждна и сигурна цифрова инфраструктура за отключване на пълния потенциал на цифровите технологии за цифрова трансформация на всички ключови сектори. С хоризонт до 2030 Република България ще разполага **с** напълно завършена национална екосистема за киберустойчивост, интегрирана в системите за киберсигурност на ЕС и НАТО.

2.1. Стратегическа цел

Цифровите технологии преобразяват ежедневието на гражданите и в този процес особено внимание и грижи трябва да отделят на киберсигурността. Те имат огромно значение за прехода към цифровата икономика и общество, като паралелно оказват огромно въздействие върху развитието на трудовия пазар, постигане на напредък в образованието и новите цифрови умения, за подобряване на конкурентоспособността и иновациите, за насърчаване на общото благо и за стимулиране на по-успешното приобщаване на гражданите. Ускоряването на цифровата трансформация е съществен елемент от отговора на ЕС и държавите-членки на икономическата криза, породена от пандемията COVID-19. В тази условия стратегически приоритет в политиката на правителството на Република България е изграждането на модерна и сигурна цифрова инфраструктура, като основа за цифровата трансформация на държавата, бизнеса и обществото.

В съответствие със стратегиите и политиките на Европейския съюз и НАТО. **стратегическата цел** на правителствената политиката за киберсигурност е постигане **на киберустойчивост на цялото общество и държава**, изразяващо се в ефективна защита срещу и адекватна реакция на кибератаки и киберинциденти, ограничаване на вредните последствия от тях, гарантиране на максимално устойчиво функциониране на жизненоважни дейности и услуги, и своевременно възстановяване до нормалното състояние[17].

За постигането на киберустойчивост на национално ниво е необходимо да се премине през три последователни фази, всяка от които се характеризира с достигане на качествено ново състояние и **ниво на зрялост** на организации, държава и общество. Трите

17 CERT(US) – Resilience Management Model, ISO 27000, NIST стандарти и др.

нива на зрялост - **информационна сигурност, киберсигурност и киберустойчивост**[18] могат да се определят съобразно два основни аспекта:

- осигуряване на общоприетата „триада“ в областта на информационната сигурност - **Конфиденциалност-Интегритет-Наличност (КИН)**[19]**;**
- ниво на познаване на заплахите и съответните рискове – класификация на **„известните неизвестни“**, използвана също и в областта на националната сигурност[20].

На Фигура 1. са показани трите нива на познаване на заплахите и рисковете и съответните нива на състоянието на киберсигурност:

Фигура 1. Нива на познаване на заплахите и рискове и нива на киберсигурността

- **ниво „известни известни“** – защита и предпазване на информационните активи и комуникационна инфраструктура от известни слабости, заплахи и пробиви, свързани с основната „триада“ на **информационната сигурност;**
- **ниво „известни неизвестни“** - предполагаеми комплексни и комбинирани заплахи, свързани с информационната сигурност, ИКТ, мрежите и системите, разнообразие от **съвременни упорити заплахи**[21], атаки срещу репутацията на организации и личности, кампании за дезинформация, и други непредсказуеми последствия от масовото пренасяне на дейностите в киберпространството, пробиви в триадата КИН в особено големи мащаби (национални, регионални и световни), изискващи разширено и системно прилагане на КИН за всички активи в цифровата екосистема - информация, технологии и съоръжения, организация и процеси и хора, за постигане на киберсигурност;
- **ниво „неизвестни неизвестни“** или подготовка за неизвестното - неочаквани по характер заплахи в киберпространството, динамично променящи се рискове и комплексни въздействия с непредсказуеми последствия, които изискват гъвкавост

18 Eurocontrol: Manual for National ATM Security Oversight (2012)

19 Confidentiality, Integrity, Availability (CIA)

20 Насим Талеб, Черният лебед - https://en.wikipedia.org/wiki/Black_swan_theory;

21 Advanced persistent threats (APT)

и устойчивост на системите, организацията и процесите, и съответни стандарти при разработването и внедряването им**, състояние на киберустойчивост**.

За достигане на киберустойчивост, като най-високо ниво на зрялост, са необходими систематични, планирани и координирани действия на всички заинтересовани страни и ясно дефинирани и поетапно реализирани мерки във всяка една от **трите фази, при ясно лидерство и ресурсна осигуреност.**

Фаза 1 (инициираща): Инициране и постигане на базов капацитет за киберсигурност - **киберсигурни институции.**

Фокусът е върху постигането на минимално общо ниво на МИС на ниво отделни организации/нормативно задължени субекти, изграждане на **Национална координационно-организационна мрежа за киберсигурност** със съответните механизми, процеси и техническа платформа, чрез която се осигурява предаване на информация и се осъществява оперативно сътрудничество. Доразвитие на Националната система за управление при кризи, провеждане на общи и специфични секторни учения с участието на държавни, бизнес и академични структури. Реализиране на кампании за формиране на базово ниво на киберхигиена за уязвими обществени групи. Изграждане на система за изследвания и образование и сертификация на хора и технологии в сферата на киберсигурността.

Фаза 2 (развитие - от капацитет към способности): киберустойчиви институции и "киберсигурно" общество.

Организиране на идентифицирания и създаден през Фаза 1 капацитет за реализиране на **устойчивост на ниво отделни организации** и способности за координиран отговор при киберинциденти и кризи, систематични дейности по превенция. Институционализиране на устойчив механизъм за взаимодействие при мащабни киберинциденти и кампании, заплахи от кибер и хибридни кризи. Мониторинг на цялостната киберкартина, изграждане на базови способности за оперативен и стратегически анализ и оценка, оперативно и техническо взаимодействие със структурите на НАТО, ЕС и други международни мрежи.

Фаза 3 (зрялост): **киберустойчиво общество.**

Ефективно взаимодействие на оперативно и на стратегическо ниво в национален и международен аспект (ЕС и НАТО). На базата на модела за ангажираност на всички заинтересовани страни и общите интереси, Република България приоритетно развива способности както в държавния, така и в частния и изследователския сектор в идентифицирани ниши за постигане на **водещи позиции** в региона и **специализация** в партньорските мрежи в областта на киберустойчивостта.

Основните дейности по трите фази, очакваните резултати и индикаторите за изпълнение се определят с Пътната карта към Стратегията.

2.2. Принципи

Основните ценности на Европейския съюз важат в еднаква степен в цифровия и във физическия свят. Същото законодателство и норми, които се прилагат в другите области на нашия живот, важат и в киберпространството.[22]

Принципите, върху които се разработва и осъществява политиката на Република България за киберсигурност са в съответствие с принципите, от които се ръководи политиката на ЕС в тази област:

- **Защита на основните права, свободата на изразяване на мнение, личните данни и неприкосновеността на личния живот** - Киберсигурността може да е надеждна и ефективна само ако се основава на основните права и свободи, регламентирани от Конституцията на Република България и залегналите в Хартата на основните права на Европейския съюз и по-специално: правото на зачитане на личния живот и тайната на съобщенията; защитата на личните данни; свободата на стопанската инициатива; правото на собственост; правото на ефективни правни средства за защита и правото на изслушване. От друга страна правата на индивида не могат да бъдат осигурени без да се гарантира сигурността на мрежите и информационните системи;
- **Осигуряване на свободен и равен достъп до интернет** - Ограниченият или липсващият достъп до интернет и цифровата неграмотност поставят гражданите в неблагоприятно положение, като се има предвид голямата степен на навлизане на цифровите технологии във всички дейности на обществото;
- **Демократично и ефикасно управление с участието на множество заинтересовани страни в настоящия модел на управление на интернет, като фактор за киберсигурност** - Цифровият свят не се контролира от една единствена организация. Редица заинтересовани страни, много от които са търговски и неправителствени организации, участват в оперативното управление на интернет ресурсите, протоколите и стандартите, както и в бъдещото развитие на интернет. Съществуващият модел на управление следва да се запази и развива;
- **Споделена отговорност за гарантиране на киберсигурността** - Интегриран и кохерентен подход за разпределяне на ролите и отговорностите, свързани с киберсигурността по всички нива и органи на държавното управление, гражданите, бизнеса и институциите. Всички участници, независимо дали са публични органи, представители на частния сектор или отделни граждани, трябва да имат съзнание за тази споделена отговорност, да предприемат действия, за да защитят себе си и, ако е необходимо да осигурят координиран отговор с цел укрепване на киберсигурността.

Актуализацията на Националната стратегията за киберсигурност се разработва при съобразяване и със следните **допълнителни принципи**:

- законност и пропорционалност, съразмерност и забрана за прекомерност, като елементи от съдържанието на правовата държава - мерките за повишаване на киберзащитата и разходите да са съизмерими със съответните рискове и заплахи;
- неделимост на киберсигурността от националната сигурност;
- съгласуваност с ангажиментите и принципите на сътрудничество и взаимодействие, произтичащи от членството на Република България в ЕС и НАТО,

22 JOIN(2013) 1 final/07.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

активно участие в създаването на общ капацитет и способности за защита на киберпространството;
- прилагане на комплексен подход при изграждане на системата за киберсигурност;
- координираност в дейността на държавните институции и организации в съответствие с тяхната компетентност;
- диалог и широкообхватно сътрудничество между държавните институции, бизнеса, в лицето на операторите на съществени услуги и доставчиците на цифрови услуги, изследователските и академичните организации, промишлеността, националните, секторните и клъстерните бизнес асоциации, работодателските и неправителствените организации;
- откритост, прозрачност и отговорност при формирането и провеждането на политиката за киберсигурност;
- ефективност и ефикасност на управленските и изпълнителските дейности – периодична оценка на изпълнението на Стратегията, на нивото на киберсигурност и на съответните капацитети и способности. Своевременна актуализация на Стратегията и Пътната карта към нея за адресиране на идентифицирани нови заплахи и рискове;
- демократичен и граждански контрол над системата за киберсигурност.

2.3. Приоритети

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

- постигане на устойчиво киберпространство;
- намаляване на киберпрестъпността;
- повишаване устойчивостта на комуникационните и информационните системи, подкрепящи отбраната и националните интереси в областта на сигурността;
- стимулиране на изследванията и иновациите за разработване на промишлени и технологични ресурси, необходими за киберсигурността;
- разгръщане на международното сътрудничество и взаимодействие.

2.4. Подход - общо усилие, ориентирано към резултати

Постигането на киберустойчивост на национално ниво изисква координирани действия по сигурност и надеждност на всички компоненти и активи на киберпространството: **информация, технологии, хора, организации и съоръжения**, дизайн и реализация на комуникационните канали, услугите и системите за управлението им, тяхната свързаност и оперативна съвместимост, както и цялостно ръководство и управление.

Постигането на целите и дейностите в рамките на отделните фази се основава на идентифицирането, включването и активното ангажиране на **всички заинтересовани страни**. От съществена важност е ясното определяне на ролите на заинтересованите страни по отношение на активите и комуникационните и информационни системи –

собственик, стопанин, оператор, потребител/клиент, доставчик и др., като за всяка роля и съответните бизнес процеси е нужно да бъде оценена степента на цифровата зависимост, включително и в перспектива.

Основните фактори за успешното и ускорено постигане на целите на Актуализираната стратегия са:

- Обвързаност на целите на Стратегията с приоритетите и целите на националните стратегически и програмни документи, определящи визията и общите цели на политиките за развитие на страната в средносрочен и дългосрочен план;
- Ефективно и ефикасно ръководство и управление на системата за киберсигурност в страната в изпълнение на Стратегията, гарантиране на необходимите ресурси и на първо място човешкия капитал в областта;
- Съгласуваност с хоризонталните и секторните стратегии и прилагане на всеобхватен, комплексен подход за постигането на сигурност на киберпространството и цифровата среда като задължително условие за успешна цифрова трансформация на българското общество, за модернизиране и повсеместно въвеждане на интелигентни ИТ решения във всички сфери на икономиката и социалния живот;
- Идентифициране и ангажиране на **всички основни заинтересовани страни („стейкхолдъри“)**[23] – ясно определяне на ролите, отговорностите и постигане на общо съгласие за приоритетите и дейностите по трите фази, последователно прилагане на този принцип във всички нормативни и регулаторни рамки, както и при моделите на публично-частните партньорства с участие на академичните и неправителствените организации;
- Въвеждане на ефективно **проектно и програмно управление** за реализиране на набелязаните мерки и оценка на постигнатите резултати и способности – формулиране на дейностите по мерките като отделни проекти, ориентирани към конкретни и измерими резултати, синхронизацията им в портфолио за пълно изграждане на функционални способности, и хармонизиране и съгласуваност с Пътната карта, независимо от източниците на финансиране;
- **Ефективно използване на опита и добрите практики** на водещи партньори в ЕС и НАТО, активно включване в партньорски програми и инициативи, и активизиране на партньорствата в региона за изграждане на общ капацитет и способности, обвързване на националните и международните проекти и програми, интегриране в международните мрежи за киберсигурност и координирани действия при киберкризи.

3. Области и приоритетни насоки за действие

Постигането на **стратегическата цел - киберустойчиво общество и държава**, изисква системна и последователна политика и действия в следните ключови области: установяване и развитие на национална система за киберсигурност; постигане на устойчивост на киберпространството чрез мрежова и информационна сигурност; защита и устойчивост на стратегическите обекти и първични администратори; ефективно противодействие на престъпността; киберотбрана и защита на националната сигурност.

23 Подход „мултистейкхолдер“ (multi stakeholder)

3.1. Установяване и развитие на националната система за киберсигурност, като част от системата за защита на националната сигурност

Цели

Цел 1: *Изграждане на механизъм за стратегическо и оперативно планиране и ръководство, координирани действия на* ***политическо и стратегическо ниво*** *за развитие на необходимия капацитет и способности за киберсигурност.*
Цел 2: *Осигуряване на актуална* ***киберкартина*** *и разбиране на ситуацията в киберпространството и вземане на навременни и адекватни решения.*
Цел 3: *Взаимодействие за* ***ефективна и координирана превенция, реакция и възстановяване.***

Сигурността на киберпространството е неотделима част от националната сигурност. Актуализираната стратегия за национална сигурност на Република България[24] посочва жизненоважните и други важни национални интереси, необходимите условия и предпоставки за тяхното реализиране. За развитие и гарантиране на сигурно киберпространство, като един от важните национални интереси се изгражда **Националната система за киберсигурност**, която е интегрален елемент на **системата за управление и защита на националната сигурност**.

Системата за киберсигурност гарантира демократично и ефикасно управление на държавните и административните органи, публичните институции, предоставящи обществени услуги, и споделяне на усилията от лицата, осъществяващи публични функции, ръководителите на стратегически обекти от значение за националната сигурност, операторите, предоставящи съществени и/или цифрови услуги, гражданите и техните организации. Всички участници носят споделена отговорност за предприемане на действия, за да защитят себе си и ако е необходимо да осигурят координиран отговор с цел укрепване на общото ниво на киберсигурност.

Нарастващ брой организации, включително неправителствени и от частния сектор, декларират жизнена необходимост и готовност да участват активно за повишаване на общата киберсигурност за развитие на единен цифров пазар и общество. Капацитет развиват софтуерни и ИКТ фирми, изследователски звена, професионални организации, както и отделни специалисти. Това създава национална общност на компетентност по киберсигурност, част от общността на ЕС, която с регулация се развива около Европейския център за компетентност по киберсигурност и националните координационни центрове.

Актуализираната национална стратегия за киберсигурност е платформа за обединяване и развитие на дейности и ресурси в **обща структура и процеси за координирани действия на всички нива** – политическо/стратегическо, оперативно, тактическо и техническо, като се обхванат и ангажират всички основни заинтересовани страни. Предвидените мерки целят да бъде **изградена и институционализирана единна система** на отговорности, процеси и процедури за мониторинг на общото състояние на киберпространството, взаимодействие и ефективно използване на техническия капацитет за превенция, координиран отговор и възстановяване, анализ на тенденциите и създаване на способности за активно и ефикасно противодействие.

Приоритетни насоки за действие

24 Актуализирана стратегия за национална сигурност на Република България, ДВ, бр. 26 от 23.03.2018 г.

3.1.1. Политики, стратегии и планове - стратегическо ниво

Основната нормативна уредба за изграждане и функциониране на Националната система за киберсигурност е **Законът за управление и функциониране на системата за защита на националната сигурност(**ЗУФСЗНС), **Законът за киберсигурност(**ЗКС**)**, правните актовете на ЕС, задължителни или правнообвързващи за държавите-членки[25], както и международните ангажименти на Република България, поети с влезли в сила международни договори, по които Република България е страна в НАТО, ООН и др. организации. Определени аспекти са регламентирани и в други закони - Закон за електронните съобщения, Закон за електронното управление, Закон за електронната идентификация, Закон за Държавна агенция „Национална сигурност“ (ДАНС), Закон за защита на класифицираната информация, Закон за електронния документ и електронните удостоверителни услуги, и др., както и в подзаконови актове, приети за тяхното изпълнение.

Формирането на единна политика за киберсигурност е отговорност на Народното събрание, Министерския съвет и Президента на републиката. Функциите и отговорностите по киберсигурността са разпределени между висшите държавни органи както следва:

Народното събрание на Република България осигурява приемането на закони и други актове, свързани с киберсигурността и упражнява парламентарен контрол.

Президентът, в качеството му на Върховен главнокомандващ на въоръжените сили на Република България, получава цялостна информация за състоянието и развитието на Националната система за киберсигурност, а при въвеждане на „извънредно положение“, „военно положение“ или „положение на война“ ръководи дейностите по осигуряване на киберустойчивост на държавното и военното управление.

Управлението на Националната система за киберсигурност се осъществява от **Министерския съвет** в съответствие с Конституцията, законите и подзаконовите нормативни актове и при съобразяване с целите и приоритетите, посочени в приети стратегически документи. Министерският съвет приема и периодично актуализира Националната стратегия за киберсигурност. В Програмата за управление на Правителството на Република България за периода 2017-2021 г.[26], в секторните програми и плановете на компетентните административни органи и техните администрации са отразени съответните цели, насоките и очакваните резултати от създаването и развитието на Националната система за киберсигурност. За реализацията на Стратегията, Министерският съвет приема Пътна карта и План за изпълнение[27] и следи за постигане на приоритетите и целите, както и за осигуряване на необходимите ресурси за изпълнение на заложените дейности. Министерският съвет в своите дългосрочни програмни документи[28] определя краен срок за изграждане на напълно завършена интегрирана национална екосистема за киберсигурност.

---

25 Съгласно Договора за функциониране на Европейския съюз - чл. 288 и следващи

26 Приета с Решение № 447 на Министерския съвет от 09.08.2017 г.

27 Мярка 162 от Програмата за управление на Правителството на Република България за периода 2017-2021 г.

28 Визия, цели и приоритети на националната програма за развитие България 2030 и определяне на водещи ведомства за детайлизиране на стратегията по отделните приоритети, одобрени с Решение № 33 на Министерския съвет от 20 януари 2020 г.

Съветът по сигурността[29] към Министерския съвет анализира състоянието на системата за защита на националната сигурност, изготвя оценки и предлага решения и действия, по отношение осигуряване и защита на мрежовата и информационната сигурност от посегателства, включително и по отношение на способностите за противодействие на заплахи и управление при кризи/киберкризи, като съществен елемент от дейностите по защита на националната сигурност.

Координирането на действията на **политическо и стратегическо ниво** за гарантиране постигането на необходимите капацитет и способности за киберсигурност, се осъществява от постоянно действащ консултативен орган **Съвет по киберсигурност** към Министерски съвет. Съветът осигурява сътрудничеството между компетентните държавни органи, бизнеса, академичния сектор, неправителствените организации при определянето и провеждането на държавната политика в областта на киберсигурността. Съставът и функциите на Съвета се определят със закон[30]. Председател на Съвета е зам.-министър председател, определен от министър-председателя. Организацията на дейността на Съвета се урежда с акт на Министерски съвет[31].

Функциите на **секретар на Съвета** се изпълняват от **националния координатор по киберсигурност**32, определен от министър-председателя. Националният координатор, под ръководството на Председателя на Съвета по киберсигурност организира, ръководи изготвянето/актуализирането на **Националната стратегия за киберсигурност** и **Пътната карта** към нея, които са основа за реализиране на политиката на стратегическо ниво. Към Съвета могат да се създават работни групи за изготвяне на проекти на стратегически документи и нормативни актове или на други експертни предложения по конкретни въпроси, свързани с компетентността им.

Отговорността за разработване на адекватни секторни политики и/или стратегии за постигане на киберсигурност, планиране и изпълнение на мерки за развитие на съответни способности имат административните органи, принадлежащи към системата на изпълнителната власт, както и всеки друг орган, носител на административни правомощия, овластен въз основа на закон, включително лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, както и публичните и частните субекти и операторите на критични инфраструктури, доставчиците на информационни и обществени електронни съобщителни мрежи и/или услуги. Всички посочени участници имат пряка отговорност в своя сектор и споделена отговорност и ангажимент за ефективното участие в националните мерки и планове, осигуряването на съответните ресурси за развитие на капацитет и способности за последователно постигане на мрежова и информационна сигурност, киберсигурност на цялото общество, бизнеса и държавата.

Критерии за функционираща система за киберсигурност на стратегическо ниво:

- Пълнота и непротиворечивост на приети и влезли в сила законови и подзаконови нормативни актове, регламентиращи въпросите на институционалното изграждане на съответните органи и взаимодействието между тях;

29 ЗУФСЗНС, обн. ДВ бр. 61/2015 г., в сила от 01.11.2015 г., изм. с ПЗР на Закона за киберсигурност ДВ, бр. 94 от 2018 г.

30 Закон за киберсигурност обн. ДВ бр. 94/2018 г.

31 Правилник за организацията и дейността на съвета по киберсигурността, приет с ПМС № 375 от 27.12.2019 г. обн. ДВ бр.102/2019г., в сила от 31.12.2019 г.

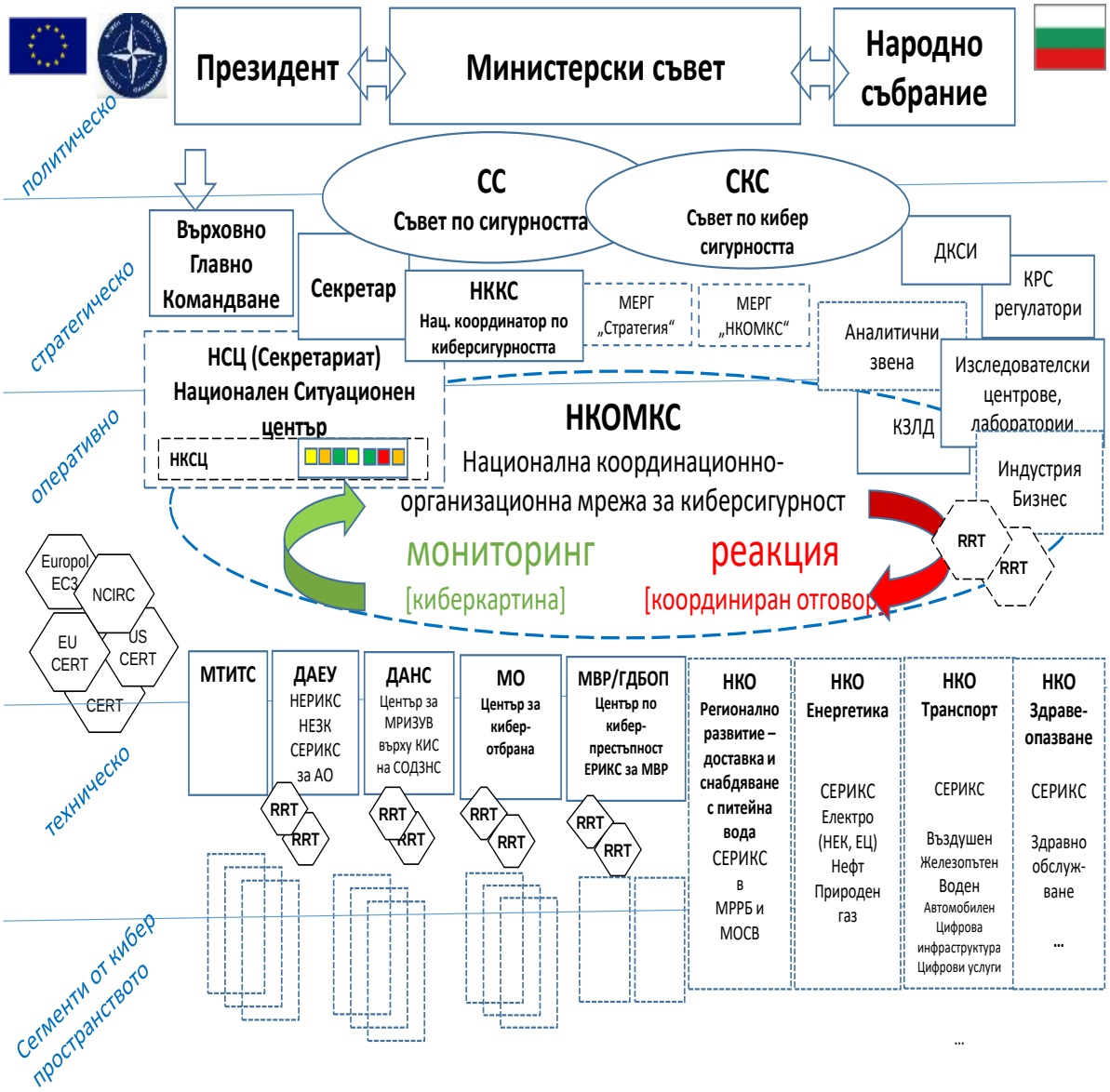
32 Виж. 6

- Зрялост на органите и структурите, осигурени с достатъчно ресурси за ефективно и ефикасно изпълнение на възложените им дейности и задачи;
- Изведени приоритети за развитието на човешките, технологичните, инфраструктурните и организационните компоненти;
- Разработена Пътна карта към Актуализираната стратегия за киберсигурност, подкрепена от портфолио от проекти и програми с ефективно управление;
- Разработен Национален план за управление на киберкризи;

Подходът за поетапно достигане на **базово ниво на национална киберсигурност** и функционираща оперативна система се основава на оптимално използване на съществуващите ресурси чрез изграждане на национална мрежа за координация и взаимодействие (през Фаза 1). Гъвкавата и отворена архитектура на модела осигурява поетапно развитие и добавяне на способности и структури за постигане на **национална киберустойчивост** (Фаза 2 и 3).

Общият модел на Националната система за киберсигурност е представен на фиг. 2.

Фигура 2. Модел на националната система за киберсигурност



3.1.2. Оперативна координация

По силата на ЗУФСЗНС, **Секретариатът** на Съвета по сигурността е **Национален ситуационен център** от Националната система за управление при кризи. Националният ситуационен център подпомага Министерския съвет при ръководството и координацията на действията по превенция, реакция, управление и овладяване на кризи; взаимодействието и координацията с органите на Европейския съюз, НАТО и други държави, както и осигурява **защитена система за обмен на информация и непрекъснат обмен на информация за анализ и оценка на риска**.

За постигане на Цел 2 и Цел 3 и за координация на **оперативно ниво** се създава организационна мрежа - **Национална координационно-организационна мрежа за киберсигурност** (НКОМКС) със съответна техническа платформа**,** както и **Национален киберситуационен център** (НКСЦ) в рамките на Националния ситуационен център със следните основни функции:

- Мониторинг на националната **киберкартина** - състояние на киберпространството в държавата, обобщена информация и индикация за статуса и безпроблемното функциониране на комуникационните и информационни системи (включително електронните съобщителни системи, преносните мрежи, националната и международната информационна свързаност). За целта се определя стандартизиран протокол и многостепенен код на състоянията (съгласуван с установените кодове за кризи, както и с тези на ЕС, НАТО и партньорски мрежи), връзка към споделяната техническа информация (на ЕРИКС/CERT[33] също CSIRT/CIRC и др.), анализ на възможните причини и източници, оценка на въздействието, както и ефективност на предприетите мерки и действия. Способност за оценка в реално време и вземане на решения по киберсигурността.
- **Координирана реакция (отговор)** и оперативно взаимодействие при мащабни инциденти, комплексни атаки и кризи – осъществява се с организационно-технически средства и се базира на актуалната киберкартина, анализа на състоянието и чрез технически протокол и организационни мерки се предоставя информация за състоянието на национално ниво, за възможни комбинирани заплахи и хибридни въздействия, за потенциален кинетичен и каскаден(„домино“) ефект и се дават препоръки за превантивни действия на оперативно и тактическо/техническо ниво, за активиране на планове и действия от киберотбраната, привличане на експерти (от работните групи към СКС, международни и др.)

НКОМКС представлява „**нервната система**“ на Националната система за киберсигурност, и се изгражда и развива по модела на **публично-частните партньорства** (ПЧП) с ангажиране на всички заинтересовани страни от публичния и частния сектор. НКОМКС се базира на държавните организации и органи, пряко ангажирани в Националната система за киберсигурност (и общо в защита на националната сигурност). НКОМКС е отворена за постепенно включване на всички заинтересовани организации и институции (държавни, бизнес, академични и неправителствени), които стопанисват, управляват, функционират и отговарят за различни активи, компоненти и сегменти на киберпространството. За целта се дефинират и прилагат изисквания за оперативна

33 **ЕРИКС** - Екипи за реагиране при инциденти с компютърната сигурност; CERT - Computer Emergency Response Team/Computer Emergency Readiness Team; CSIRT - Computer Security Incident Response Team; CIRC – Computer Incident Response Capability/Center (NATO).

съвместимост, роли, отговорности и оперативни способности на базата на общ механизъм, стандартизирани процеси и протоколи за мониторинг, превенция, реакция и възстановяване.

Всяка заинтересована организация осигурява капацитет и способности за непрекъснато следене на състоянието на поверените ѝ обекти и сегменти от киберпространството по отношение на аспектите на киберсигурността и функционирането на комуникационните и информационните системи (КИС) (**вътрешен мониторинг**), и екипи за **незабавна реакция** при киберинциденти или нарушение във функционирането на КИС. Тези функции, организационно и технически се изпълняват от центрове и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС/CERT и др.), в които функционират постоянно или се създават ad-hoc екипи и групи за бързо реагиране (RRT – Rapid Reaction Team).

Включените в НКОМКС организации интерактивно взаимодействат, като непрекъснато изпращат към НКОМКС информация за киберсъстоянието си за целите на националния мониторинг и съответно **получават актуалната киберкартина за страната, оперативна оценка** на общата ситуация, указания и препоръки за координация и взаимодействие с други организации. Функциите на НКОМКС са на **координираща мрежа**, а не на централизиран команден център. Задължение на всеки участник в НКОМКС е да **действа незабавно и автономно** в рамките на своите компетентности, планове и способности. На базата на получаваната обща оценка на ситуацията и на цялостната киберкартина, тези действия се адаптират, разширяват и координират с други центрове и организации. Всички участници предприемат **превантивни действия** и повишат динамично състоянието си на готовност на базата на собствен анализ и оценка, с отчитане на националната киберкартина и препоръките по НКОМКС. Наблюдението на динамиката и развитието на киберкартината в мрежата на НКОМКС ще се извършва от **екипи за оперативен анализ** (ситуирани в ЕРИКС/CERT, или специализирани звена), които осигуряват оперативна оценка на тенденциите за развитие на киберзаплахите и негативните последствия, препоръки за превенция и пълно възстановяване.

Моделът на НКОМКС позволява поетапно включване и на организации с непълно изграден капацитет, като някои дейности могат да бъдат **делегирани с технически и организационни мерки** на други участници в мрежата.

Към НКОМКС се развиват способности за ad-hoc сформиране на: а) **специализирани комбинирани екипи за реакция** при мащабни инциденти от интердисциплинарен характер и/или хибридни атаки, с ангажиране на изследователски лаборатории; б) специализирани екипи за разследване и разкриване на киберпрестъпления, на екипи за киберотбрана, активно противодействие на кибертероризъм и терористични заплахи.

Архитектурата и моделът за работа на НКОМКС е на принципа на виртуална мрежа на взаимодействие и следва принципите на доказано работещия и гъвкав модел „**ориентиран към услуги**“[34]. **Гръбнакът** на НКОМКС се изгражда на базата на структури, центрове и организации, отговорни за киберсигурността в различни сегменти на киберпространството:

- Национален ЕРИКС в рамките на ДАЕУ;
- Национално единно звено за контакт в рамките на ДАЕУ;

34 Service Oriented Model/Architecture, Collaboration Networks

- Секторни ЕРИКС в ДАЕУ и към Националните компетентни органи, определени с решение на МС;
- Център за киберотбрана (Mil CIRC – Computer Incident Response Capability) в МО
- Център по киберпрестъпност в ГДБОП-МВР;
- ЕРИКС в ГДБОП-МВР;
- Център по киберсигурност – Дирекция КИС-МВР;
- Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху КИС на стратегически обекти и дейности от значени за националната сигурност в ДАНС;
- ЕРИКС за класифицирани мрежи в ДАНС;
- Национален център за контратероризъм в ДАНС;
- Аналитични звена;
- Регулаторни и акредитиращи структури;
- Изследователски и други специализирани звена.

За първоначалното изграждането на НКОМКС се използват основно съществуващите ресурси и центрове, разширени със съответните организационни и технически средства. Поетапно се развива допълнителен капацитет и способности в секторните и ведомствени ЕРИКС, както и разширяване на базата на ПЧП и мобилизиране на национални и международни ресурси. Приоритетно към НКОМКС се включват системите за наблюдение на **критични инфраструктури, центрове за ранно оповестяване и борба с киберпрестъпления, секторни и бизнес** ЕРИКС.

В Националния ситуационен център (НСЦ) се разполага национален център за непрекъснат мониторинг на киберкартината в държавата и осигуряване на координирана реакция - **Национален киберситуационен център** (НКСЦ). НКСЦ има функции по събиране, анализиране и незабавното докладване на постъпила информация във връзка с предотвратяване, ограничаване и овладяване на кризи[35], както и за координиране на действията и комплексната реакция при заплахи за националната сигурност в резултат на кибератака. Той осигурява оперативна оценка на обобщената степен на заплахата на национално ниво, разпространява препоръки за превантивни действия и организиране на координирани действия при киберкриза или при непосредствена заплаха от такава. Оперативно-техническите действия се поемат от съответните ЕРИКС и екипите за бързо реагиране(RRT).

Моделът на НКОМКС е в съответствие с препоръките на ENISA, ITU и НАТО за разпределен механизъм на отговорности и взаимодействие на федеративен принцип, с фокус върху координирането на действията. Той следва да осигури „отвореност“ и лесно интегриране на нови участници, включително на регионално и международно ниво. За развитието на НКОМКС активно се ангажират бизнес, академични и неправителствени организации чрез установяване и развитие на ефективен модел на ПЧП.

Принципите за проектиране и развитие на НКОМКС и изискванията към организациите и центровете за мониторинг се определят от Съвета по киберсигурност в съответствие с развитието на модела и архитектурата на Националната система за киберсигурност и изискванията за оперативна съвместимост.

Изискванията за обмен на информация, за техническа и киберзащита на НКОМКС се осъществяват по разработени правила, протоколи и нива на поверителност, които

35 Криза - по смисъла на §1,т.3 на ДР на Закона за управление и функциониране на системата за защита на НС

отчитат и изискванията за класифицирана информация със съдействието на държавните регулаторни органи[36]. Съответните изисквания и нива за достъп се регламентират и прилагат за организациите и лицата от страна на всички участници и при спазване на принципа **„необходимо е да се знае“**[37]. Този принцип се развива съобразно новите принципи за споделяне - **„нужно е да се сподели“**[38] и **„отговорност да се сподели“**[39] за постигане на отворен характер на мрежата НКОМКС и ефективно включване на всички участници(публични и частни организации) за постигане на киберустойчивост на национално ниво.

3.1.3. Национален координатор по киберсигурност

Функциите на Националния координатор по киберсигурността (НККС) се определят със закон[40]. Той осигурява връзката между двете нива на Системата за киберсигурност - стратегическото ръководство и системата за координация на оперативно ниво, както и връзката с Националната система за управление при кризи. Националният координатор участва при изграждането и развитието на НКОМКС и осигуряването на нейната надеждност, сигурност и устойчивост и в създаването и развитието на НКСЦ, като обособена структура в Националния ситуационен център[41]. За окомплектоване на Националния киберситуационен център с необходимите човешки ресурси се командироват компетентни служители от министерства и ведомства по реда на Закона за държавния служител или по реда на специалните закони.

3.1.4. Национална система за управление при киберкризи

Управлението при кризи е съществен елемент от дейностите по защита на националната сигурност. Положение на криза се обявява, съответно отменя, с решение на Министерския съвет. Управлението при кризи се осъществява от Министерския съвет чрез Националната система за управление при кризи, която включва национален, ведомствени и областни ситуационни центрове. Това са структури, осъществяващи събиране, анализиране и незабавно докладване на постъпила информация във връзка с предотвратяване и/или ограничаване на кризи, както и за **координиране на мерките и действията** за реакция, овладяване и преодоляване на кризата.

Националната система за управление при киберкризи е част от Националната система за управление при кризи[42] и включва: ангажиране на мрежата НКОМКС, с участващите в нея организации, центрове и екипи за реакция; Националния координатор по киберсигурността и експертния капацитет на НКСЦ в Секретариата на Съвета по

36 ДКСИ (Държавна Комисия за Класифицирана Информация), ДАНС (Държавна Агенция за Национална Сигурност), и други специализирани органи

37 Need-to-know – нужно е да се знае, обоснована необходимост за достъп до конкретна информация, независимо от общото разрешение за достъп

38 Need-to-share – източникът на информация определя нуждата и адресатите на споделяне на информация (например: за да получиш помощ, трябва да споделиш нужната информация)

39 Responsibility to share (provide)

40 Закон за киберсигурност ДВ бр. 94/2018, в сила от 17.11.2018 г.

41 Функциите на НСЦ са определени в глава трета на Закона за управление и функциониране на системата за защита на НС ДВ бр. 61/2015, в сила от 01.11.2015 г.

42 Закон за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС), 2015 г.

сигурността при МС. Те осигуряват дейността на **Националния ситуационен център** за справянето с кризи и бедствия, на национално ниво, в два аспекта:

1) За предотвратяване и справяне с киберкризи – непрекъснат мониторинг на националната киберкартина за ранно идентифициране и оценка на нивото на заплахите. При състояние на повишена заплаха от кибератака или от такава с хибриден характер, сформиране на екипи за анализ, реакции и възстановяване, с привличане на експерти от различни ведомства и организации, препоръчване на превантивни действия, ескалиране на предупрежденията и координация за овладяване на киберкризи;

2) При **общи кризи** или **мащабни заплахи от хибриден характер** (включително бедствия и аварии) - завишен мониторинг на киберкартината във връзка с безпроблемното функциониране на системите, необходими за справяне с кризите, и предотвратяване на разширяването им в киберпространството (във взаимодействие с Единната спасителна система[43] и други специализирани системи за управление при кризи със съответното ниво на защита и устойчивост).

Киберкризите[44] по своя жизнен цикъл следват етапите на всяка криза: забелязване, осмисляне и оценка, взимане на решения, прекратяване, възстановяване, извличане на поуки. Има аналогия и в основните състояния - нормално, инцидент, криза. Поради виртуалния си характер и многообразието на събитията в киберпространството те имат редица особености, като: съвършено нов тип, непознати и непрекъснато развиващи се по форма и характер кризи; мерките, плановете и процесите за взаимодействие и реакция се различават съществено от тези при „стандартните“ кризи; индикациите за наближаваща криза трудно се наблюдават директно (комбинация от „неизвестни известни“ и „неизвестни неизвестни“), а преходът от ескалиращи инциденти към комплексна криза може да е в рамките на часове и минути; нямат „територия“ и ограничено пространство, трудни са за идентификация и определяне на източника и обхвата; могат да имат „кинетичен ефект“ и да са основен компонент от реализация на хибридна атака.

Заплахите от киберкризи най-често се проявяват индиректно чрез сигнали за нарушения в различна степен на функциите на съответните комуникационни и информационни системи и оттам на съответните услуги, дейности и бизнес. Процедурите на най-високо ниво (**деклариране на киберкриза**, обявяване на ескалиране, поискване и оказване на помощ, международно взаимодействие), следват процедурите, установени в Националната система за управление при кризи и съответните планове, но с отчитане на специфики като бързодействие, интензивност и мащабност на въздействията, както и необходимостта от бързи и координирани действия по ограничаване на последствията. Процедурите за действие при киберкризи следват насоките от **Европейските стандартни оперативни процедури (SOP)**[45] за взаимодействие при киберкризи, концепцията **„Blueprint**“ за Европейски координиран отговор на широкомащабни киберинциденти и

43 Закон за защита при бедствия, Глава Трета. Единна спастелна система в сила от 14.10.2011 г., изм. ДВ. бр.8 от 25 Януари 2011г., изм. ДВ. бр.39 от 20 Май 2011г., изм. ДВ. бр.80 от 14 Октомври 2011г., изм. ДВ. бр.68 от 2 Август 2013г., изм. и доп. ДВ. бр.53 от 27 Юни 2014г., изм. и доп. ДВ. бр.14 от 20 Февруари 2015г., изм. ДВ. бр.79 от 13 Октомври 2015г., изм. и доп. ДВ. бр.81 от 20 Октомври 2015г., изм. и доп. ДВ. бр.51 от 5 Юли 2016г., доп. ДВ. бр.81 от 14 Октомври 2016г., доп. ДВ. бр.97 от 6 Декември 2016г., изм. ДВ. бр.13 от 7 Февруари 2017г., изм. и доп. ДВ. бр.97 от 5 Декември 2017г., изм. и доп. ДВ. бр.77 от 18 Септември 2018г., изм. и доп. ДВ. бр.60 от 7 Юли 2020г.

44 Относно дефиницията на „киберкриза” виж Приложение-речник

45 EU SOP's – European Standard Operational Procedure for cooperation during cyber crisis, част от European Cyber Crisis Cooperation Framework (ECCCF). Препоръка (ЕС) 2017/1584 на Комисията и заключенията на Съвета от 26 юни 2018 г. относно координирана реакция на мащабни киберинциденти и кризи

киберкризи с трансграничен характер[46], моделът на **взаимодействие и управление на кризи на НАТО**. От тях произтичат част от **основните стандартни изисквания** към мрежата НКОМКС, за да се осигури нейната оперативна съвместимост и отвореност и на международно ниво.

Управлението при киберкризи се осъществява въз основа на **Национален план за действие**[47], който се предлага от Съвета по киберсигурност и се приема от Министерския съвет. В плана се разработват дейностите за осигуряване на готовност, превенция, откриване, отговор, смекчаване, възстановяване, международно сътрудничество. Планират се дейностите за координация и взаимодействие със съответните **ведомствени и областни ситуационни центрове,** както и за ангажиране на **националните компетентни органи по МИС и съответните секторни ЕРИКС. Националният, ведомствените и областните планове за действие при киберкризи** следва да се разработват в синхрон със съответните планове за **защита на националната сигурност и киберотбрана**. Хибридният характер на заплахите от киберкризи изисква **комплексен подход** при реакция и защита и задължително добавяне на адекватен **киберфокус във всички планове за управление при кризи**, както и допълнителни способности в съответните организации.

За своевременни превантивни действия при непосредствена заплаха, както и реакция при киберкризи ще бъде установен **механизъм на координиран отговор**. Той се базира на разработени стандартни оперативни процедури и на способностите на ЕРИКС и техните специализирани групи за бързо реагиране(RRT). За посрещане на национални киберкризи и кризи от хибриден характер се разработва механизъм и способности за сформиране и координация на **национални смесени групи за бързо реагиране.**

Когато киберкризата по своя характер изисква преминаване към киберотбрана се задействат системата за управление на отбраната и плановете за отбрана.

3.1.5. Повишаване на ролята и отговорностите на държавните структури и на заинтересованите страни

Изграждането на ефективна Национална система за киберсигурност изисква преглед и предефиниране на ролите и отговорностите на държавните органи, академичния сектор, бизнеса и неправителствените организации, което включва:

- Подобряване на взаимодействието и координацията на най-високо държавно ниво в определянето на **националните политики и приоритети** за сигурност на киберпространството – народно събрание, правителство, президент, съдебна власт;
- Регламентиране на отговорностите съобразно ролите на собственик, управляващ, стопанин и оператор за съответните сегменти на киберпространството на **министерствата и ведомствата**, пряко ангажирани в системата за националната сигурност или отговорни за критични инфраструктури, **операторите на критични инфраструктури** и произтичащите задължения по осигуряване на МИС, надеждност и защита на КИС, създаване на вътрешна организация и технически

46 Blueprint Recommendation C (2017) 6100 final of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.

47 National Cyber Contingency plan

капацитет за мониторинг на състоянието им, регистриране на инциденти, реакция и възстановяване;

- Преглед и разпределение на отговорностите и функциите за всички сегменти на киберпространството на национално ниво и във връзка с международните ангажименти и сътрудничество, развитие на регулаторните и насърчителните механизми;
- Подготовка и **включване в Националната система за киберсигурност** и управление на споделения киберриск за всички организации и заинтересовани лица (държавни, бизнес, академични/научно-изследователски, неправителствени организации) – създаване на капацитет и покриване на изискванията за националната мрежа НКОМКС, развитие на способности за координирана реакция и взаимодействие на национално, секторно и регионално ниво.

3.2. Мрежовата и информационна сигурност – фундамент на киберсигурността

Цели:

Мрежовата и информационна сигурност (МИС) е фундамент на киберсигурността. Тя трябва да бъде в пълна синергия и взаимно допълване с другите два стълба на киберсигурността - правоприлагане и киберотбрана, за да се постигне устойчива Национална екосистема за киберсигурност в страната.

Основната цел по отношение на МИС е изграждането на Национална система за киберсигурност, базирана на инструментариум и решения за постигане на високо ниво на мрежова и информационна сигурност. Тя трябва да осигури ефективна киберзащита и да подпомага укрепване възможностите на мрежите и системите в държавата за противодействие срещу кибератаки от престъпници, кибертерористи, хактивисти и дори държавно-спонсорирани играчи.

Това трябва да се постигне с подходящи мерки на национално, секторно, организационно и индивидуално ниво по отношение на обхвата, и на техническо, оперативно и политическо ниво по отношение на спецификата им.

Специфичните приоритетни насоките действие за следващите години, по които следва да се разработват и реализират мерките по отношение на мрежовата и информационна сигурност са следните:

3.2.1. Изграждане на среда за сътрудничество и партньорство

Тази среда трябва да се изгради между публичните институции, научните, образователните, неправителствените и бизнес организации, както и отделни експерти, които могат да допринесат за повишаване на нивото на МИС в страната. Това е постижимо чрез повишаване нивото на сътрудничество и партньорство с всички заинтересовани страни (интернет доставчици, компании и експерти по киберсигурност) за споделяне на информация и експертиза на основата на НКОМКС и чрез различни други партньорски събития и инициативи.

3.2.2. Налагане на минимално общо ниво на МИС на ниво организация

Това ниво трябва да съответства на съществуващите рискове за сигурността на информационните ресурси на организацията спрямо идентифицираните потенциални

заплахи към тях. Трябва да включва и налагане на принципа за „**киберсигурност по подразбиране“** при разработване и допускане в експлоатация на ключови информационни системи и инфраструктури. Друг съществен аспект за постигането на минимално общо ниво на МИС е и налагането на системен контрол за предприемане на подходящи мерки за киберзащита от организациите и налагането на унифициран системен подход за оценка и намаляване на рисковете по отношение на МИС.

3.2.3 Укрепване капацитета на институциите със съответни роли и отговорности по отношение на МИС, съгласно националната рамка за управление на киберсигурността, дефинирана в Закона за киберсигурност

Укрепването на капацитета на тези институции е от първостепенна важност, защото те трябва да поемат лидерски отговорности в областта на МИС. Вече създадените секторни структури за МИС трябва да бъдат утвърдени чрез налагане на секторния подход по отношение на операторите на съществени услуги (ОСУ) и доставчиците на цифрови услуги (ДЦУ), като заедно с това следва да се предвиди и укрепване на техническия и оперативен капацитет и способности на Националния ЕРИКС и съответните секторни ЕРИКС.

Съгласно Закона за киберсигурност Министерският съвет делегира отговорности в областта на киберсигурността на определени институции. За постигане на кумулативен ефект е важно да се постигне високо ниво на интегрираност на системите за киберсигурност между тези институции, едновременно с укрепване на капацитета им. Трябва да бъдат затвърдени и проиграни в детайли схемите и процесите на ескалация и координация между тях на стратегическо, оперативно и техническо ниво за постигане на високо ниво на увереност при разрешаване на инциденти със значително увреждащо въздействие, включително при киберкризи.

Отчитайки изискванията за защита на личните данни е необходимо също така да се повиши взаимодействието с органите и администраторите за защита на личните данни във връзка със заплахите от компрометиране на лични данни в следствие на киберинциденти.

3.2.4. Интегриране на Националната система за киберсигурност в европейските структури и инициативи в областта на МИС

Националната система за киберсигурност трябва да включва изграждане на съответните структури и организации съгласно ангажиментите на Република България в европейските структури за киберсигурност, като Националното единно звено за контакт по Директивата МИС, Националния орган за сертифициране в киберсигурността, Националния координационен център за киберсигурност по предвидените от Европейската комисия за създаване на мрежа от центрове за компетентност по киберсигурност и Европейския център за компетентност в областта на индустрията, технологиите и научните изследвания в областта на киберсигурността и др.

3.2.5. Въвеждане на европейската рамка за сертифициране на киберсигурността

Трябва да бъде изградена съответната национална организация съгласно изискванията на Акта за киберсигурност[48] на ЕС, което ще даде възможност европейските

48 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и

сертификати за киберсигурност и декларациите за съответствие на ИКТ продукти, услуги и процеси да бъдат признавани и използвани във всички държави-членки, включително и в България.

3.2.6. Ангажиране на частния сектор в повишаване нивото на МИС

Преобладаващата част от мрежовите и информационните системи са частна собственост или се управляват и експлоатират от частния сектор. Преминаването на следващ етап на зрялост изисква съвместна работа и ангажимент на държавата и бизнеса за повишаване на общото ниво на МИС за ефикасното реализиране и разширяване на сигурните и надеждни интернет базирани услуги.

За постигане на тази цел е необходимо ускоряване на трансфера и възприемане на добрите практики, технологии и доказани модели от индустрията, както и внедряване на съвременни инструменти и платформи за идентифициране и реакция на инциденти и пробиви в сигурността, анализ, изследване на доказателствата, тестове и симулации, провеждане на пилотни и тестови проекти по инициатива и с ресурси на индустрията. Трябва да бъдат подпомагани частни инициативи и проекти за повишаване на инвестициите в МИС.

3.2.7. Осигуряване на високо ниво на киберзащита на критичните информационни ресурси и инфраструктура

Необходимо е да се повиши взаимодействието и сътрудничеството между компетентните органи по отношение на киберсигурността на 5G мрежите, ключовите SCADA системи, включително транспортните инфраструктури и др. От особена важност е осигуряването на високо ниво на киберзащита на ключовите държавни информационни ресурси и инфраструктури като ДХЧО, ЕЕСМ, информационните системи на електронното управление и др.

3.2.8. Провеждане на информационни кампании за киберсигурност и киберхигиена

Повишаване информираността на населението по отношение на киберсигурността и киберхигиената ще подобри и повиши цялостното ниво на МИС. За да бъде постигнато това е необходимо разширяване на обхвата на инициативите и кампаниите за киберхигиена по МИС за достигане до максимален брой граждани и бизнеси във всички сфери и при силно взаимодействие между държава, бизнес и общество. Като основна линия по отношение на киберхигиената трябва да бъдат предприети мерки и стимули за интегриране на световно признати добри практики в областта на киберсигурността.

Важно е да се укрепи и взаимодействието между компетентните органи и частния бизнес в областта на киберхигиената чрез организиране на съвместни кампании на публични и частни доставчици на интернет-базирани услуги за въвеждане и публикуване на техните политики и мерки за осигуряване на МИС, киберзащита и непрекъснатост на услугите като съществени елементи от конкурентните предимства, прозрачността, балансирането на регулаторните механизми и пазарните принципи за постигане на сигурно и надеждно пространство за крайните интернет потребители.

комуникационните технологии. Националната система за сертифициране включваща Национален орган за сертифициране на киберсигурността, органи за оценка на съответствието, акредитиращ орган, национлна схема и др.

3.2.9. Повишаване на уменията и професионалните компетентностите на експертите по мрежова и информационна сигурност

Непрестанното възникване на нови и все по-сложни заплахи за киберсигурността налагат непрестанното повишаване на компетентностите и квалификацията на експертите. Това е постижимо единствено с редовното им участие в различни курсове с тематика в областта на МИС. Друга важна част от поддържането на уменията и компетенциите, както и за подобряване на екипността и съвместната работа между всички национални структури в сферата на киберсигурността, е редовното участие в различни учения по линия на Европейския съюз, НАТО, Международния съюз по далекосъобщения и други международни организации, така и в национални такива. Неизменна част от повишаване на квалификацията е и самото организиране на национални учения с различна тематика, която да е съобразена с актуалните тенденции и заплахи в киберпространството.

3.3. Защита и устойчивост на стратегически обекти[49] и първични администратори[50]

***Главна цел*:** Подобряване на защитата и устойчивостта на комуникационните и информационни системи на ведомствата, които са стратегически обекти, критичните информационни инфраструктури (КИИ) и първичните администратори на данни и подържаните от тях първични регистри.

Голямата зависимост на бизнеса, обществото и държавата от КИИ, тяхната трансгранична взаимосвързаност и взаимозависимостите им с други инфраструктури, както и уязвимостта и заплахите, пред които са изправени, повишават необходимостта от **разглеждане на тяхната сигурност и устойчивост от системна гледна точка,** като предна линия за защита срещу неизправности и злонамерени атаки. Комплексът от рискове, насочени към критични комуникационно-информационни инфраструктури е с различен произход, като се формира от човешка дейност, природни бедствия или технически неизправности. Тази тяхна разнородност често ги прави силно специфични, слабо разбрани и напълно и/или неанализирани в достатъчна степен. Формираната комплексност на рисковете и слабо детерминираният контекст, в който се развиват, забавя и силно затруднява адресирането и управлението им.

Друг ключов проблем възниква от нарастващата обвързаност на информационните и комуникационните системи със системите на редица сектори от критичната инфраструктура, като сигурност, енергетика, транспорт, финанси, здравеопазване, телекомуникации, снабдяване с храни и вода, отбрана и редица други[51]. Повечето от информационните системи, услугите, мрежите и инфраструктурите формират жизненоважна част от икономиката и обществените дейности, като или предоставят съществени продукти и услуги, или са основна платформа за други **критични инфраструктури** и позволяват упражняване на правата и свободите на гражданите. Те се определят като **критични комуникационно-информационни инфраструктури**, тъй като тяхното разстройване или разрушаване може да доведе до срив в държавата и обществото и нарушаване на нормалното им функциониране. При неблагоприятни въздействия срещу

49 Съгласно ПМС №181/2009 за определяне на стратегически обекти и дейности от значение за националната сигурност

50 По смисъла на чл.2, ал.2 на Закона за електорнното управление

51 Виж COM(2009) 149, връзка COM(2005) 576 на ЕК

тези системи, непредвидените негативни последствия и възможните каскадни ефекти за другите сектори и обществото могат да бъдат многократно по-големи в количествено и качествено изражение от ползите, за чието създаване те са проектирани и създадени.

***Приоритетни насоки за действие:*:**

- Разработване на модел за своевременна идентификация на критична за националната сигурност информационна инфраструктура;
- Интегриране на способности и процедури за активно ангажиране в управлението на риска за ККИИ;
- Въвеждане на процедури за интегриране на обществото в информационната защита на ККИИ чрез фокусирано повишаване на осведомеността;
- Разширяване на координацията и взаимодействието със страни – членки на ЕС, НАТО за минимизиране на рисковете и заплахите срещу ККИИ;
- Повишаване техническите, административните и организационните способности на органите, ангажирани в защита на информационните системи на стратегическите обекти и дейностите, които са от значение за националната сигурност и на първичните администратори на данни и подържаните от тях първични регистри;
- Изграждане на капацитет и способности за мониторинг на киберинциденти в информационната инфраструктура на стратегическите обекти и дейностите, които са от значение за националната сигурност;
- Разработване и прилагане на специфични **планове и процедури** за защита на информационните системи на стратегическите обекти и дейностите, които са от значение за националната сигурност и на ведомствата, първични администратори на данни и подържаните от тях първични регистри;
- На основата на партньорство и взаимно разбиране на отговорностите, ръководителите на стратегическите обекти и дейностите, които са от значение за националната сигурност **актуализират** общите и специфичните изисквания и мерки за киберсигурност, в посока постигане на киберустойчивост, и покриване на целия жизнен цикъл за управление на киберрисковете и реализиране на целия комплекс от дейности по идентифициране на организационната структура и активите, тяхната защита, откриване на инциденти, реакция, възстановяване и съответни поуки и подобряване[52];
- Актуализиране на стандартните оперативни процедури за управление на рисковете и неутрализиране на заплахите за ККИИ;
- Насърчаване и подкрепа за създаване на секторни или клъстерни организации за споделяне на информация и повишаване на колективната киберсигурност в областта на критичните инфраструктури (ISAC/ISAO [53]).

3.3.1. Подобряване на взаимодействието между държавата и операторите на критични инфраструктури – стратегически обекти и дейности

- Разпределение на ангажиментите и засилване на сътрудничеството на държавата с операторите на ККИИ и КИ, чрез споразумения за взаимодействие;

52 NIST: Framework for Improving Critical Infrastructure Cybersecurity (2014): Identify, Protect, Detect, Respond, Recover, развити също и в стандарти и модели като ISO/ICE 2700x, COBIT, CCS CSC, CERT-RMM

53 ISAC/ISAO Information Sharing and Analysis Center/Organization

- Включване на операторите на критичните инфраструктури в процесите на националното управление при кризи и бедствия, произтичащи от киберсигурността, в изграждането на цялостната архитектура на сигурността. Развитие на капацитета и способностите им за управление на риска при кризи чрез създаване на функционираща система за сигурност, включително определяне на вътрешни органи по сигурността;
- Периодично преразглеждане и своевременното актуализиране на **споразуменията за сътрудничество** между компетентните държавни органи и операторите на стратегическите обекти и дейности, които са от значение за националната сигурност и на първичните администратори на данни и подържаните от тях първични регистри в контекста на развитието на предизвикателствата в киберпространството и на тази основа, изменение и допълнение на плановете за действие при кризи и за киберзащита.

3.3.2. Развитие и модернизация на системите за управление и защита на критични инфраструктури - – стратегически обекти и дейности

- Идентифициране на нови предизвикателства пред киберсигурността, релевантни към 5G комуникационната свързаност, интернет на предметите;
- Приоритетно **модернизиране на процесите, технологиите и системите** и подобряване на защитата и сигурността на системите за управление от типа ICS/SCADA[54], адекватни на съвременните изисквания за киберсигурност, в съответствие с **международно признати стандарти** и модели, съответен одит и сертификация;
- Идентифициране, изолиране на достъпа и поетапна подмяна на софтуер, системи и компоненти с изтекъл срок на поддръжка от производител или доставчик (включително и операционни системи, офис пакети и др.), или излезли от употреба, представляващи особено уязвима и лесна цел за злонамерени действия, дефекти и опасна нестабилност.

3.3.3. Своевременна защита на новите области на киберпространство

Бързото и широкото навлизане на цифровите технологии в ежедневния живот и бизнеса, предопределят и **непрекъснатото разширяване на оценката за „критичност“ на комуникационните и информационни системи в съответствие с нарастващата цифрова зависимост**, което изисква механизъм за динамичното разширяване на обхвата на изискванията и мерките към критичните инфраструктури и върху развиващите се обществено значими електронни среди и платформи, като различни системи за **електронна търговия, портали за плащания в интернет, социални мрежи, машини за търсене, облачни услуги и приложения, онлайн магазини за приложни програми**[55], **онлайн медии**, и др.

Области с висок ръст на цифровизация на бизнес процесите са **финансовите услуги, е-разплащанията и цифровите валути, сферата на електронното**

54 Industrial Control Systems – ICS, Supervisory Control and Data Acquisition – SCADA и други

55 App-store и др.

здравеопазване и осигуряване, и други, което определя техните комуникационни и информационни инфраструктури като критични. Независимо от това, дали тези области са формално включени към списъците за КИ, тяхното бързо развитие и навлизане в живота на граждани и фирми изисква **своевременната интеграция в Националната система за киберсигурност** и обхващането им от изискванията и механизмите за координация за киберсигурност. Прилагането на мерките е на базата на баланс на механизма на регулация и саморегулация и **добавяне на киберсигурността към изискванията и предимствата в конкурентната бизнес среда.**

Утежняването на ситуацията с глобения и отворен интернет в условия на геополитическо напрежение в последните години е съпроводено с целенасочени дейности, които нанасят вреди на международната сигурност и осуетяват ползите от киберпространството за икономическо, социално и политическо развитие. Децентрализираната архитектура на световният интернет показва висока степен на устойчивост по отношение на способността да поддържа рязко увеличен обем на трафика в условията на глобалната пандемия от COVID-19. България като държава член на ЕС и НАТО е необходимо да бъде подготвена за евентуални бъдещи дестабилизиращи геополитически или технически събития, които засягат базисните функции на интернет. Осигуряването на надеждното функциониране на глобалната мрежата е стратегическа цел, за чието постигане се разработва и провежда обща европейска политика, която е фокусирана върху предприемане на убедителни мерки срещу киберинциденти и злонамерени онлайн дейности, както и ограничаването на зависимостта от инфраструктура и услуги, намиращи се извън ЕС. Това ще изисква комбинация от законодателни мерки и преглед на съществуващите правила, за да се гарантира високо общо ниво на сигурност на мрежовите и информационните системи в ЕС; повишаване на инвестициите в научни изследвания и иновации; и търсене на начини за внедряване или укрепване на основни интернет инфраструктури и ресурси, по-специално системата за имена на домейни[56]. Важен елемент за защита на ключовите европейски и национални цифрови активи е да може да се предложи канал за сигурни комуникации за критичната инфраструктура. Европейската комисията вече работи с държавите членки за въвеждането на сертифицирана напълно защитена откай докрай основана на квантовите технологии инфраструктура, наземна и базирана в космоса, в съчетание със сигурната правителствена сателитна система за комуникация, определена в Регламента за космическата програма[57]. Правителствените спътникови далекосъобщения на ЕС, които са част от космическата програма, ще осигурят в близко бъдеще надежсен и икономически ефективен комуникационе капацитет, за да се гарантират мисии и операции от критично значение за сигурността и безопасността, които се управляват от ЕС и неговите държави-членки, включително от субекти в областта на националната сигурност и от институции, органи и агенции на ЕС. България пое ангажимент[58] да работи съвместно с ковисията и други държави-членки за сигурна и квантова комуникационна инфраструктура (QCI) за Европа.

56 Система за имена на домейни (DNS) представлява йерархична и децентрализирана система за именуване на компютри, услуги или други ресурси, свързани към интернет или частни мрежи. Тя преобразува имена на домейни в IP адреси, необходими за локализиране и идентифициране на компютърни услуги и устройства

57 Предложение за регламент за създаване на космическа програма на Съюза и на Агенция на Европейския съюз за космическата програма COM(2018) 447

58 През м. февруари 2020 г. България подписа Декларацията на EuroQCI за развитие и разгръщане на QCI в периода 2021-2027 г.

3.4. Ефективно противодействие на киберпрестъпността

Цели:
Цел 1: Установяване на ефективен и ефикасен процес по **превенция и защита, реакция, разследване и адекватно правоприлагане;**
Цел 2: **Подобрен оперативен капацитет и способности** за противодействие на киберпрестъпленията и сътрудничество на национално, европейско и международно ниво.

Правоприлагането и борбата с киберпрестъпността е **вторият основополагащ стълб** на киберсигурността. Икономическите, материалните и моралните щети, произтичащи от киберпрестъпни и злонамерени действия намаляват силно доверието в цифровите и електронните услуги и в развитието на отворено и демократично общество и динамична и устойчива икономика.

Паралелно с развитието на цифровизацията в Република България нараства броя и разнообразието на престъпленията в киберпространството. Кражбите на данни с личен и финансов характер носят репутационен риск за финансовите институции, което допринася за ниското ниво на докладване пред полицейските органи. Значителна част от киберпрестъпленията днес са свързани с кибератаки и проникване в информационните системи, с цел блокиране или кражби на данни за изнудване на лица и предприятия. Естеството на организираната киберпрестъпност предполага изразена мултинационалност и трансграничност в дейността на престъпните групи.

В много случаи киберинцидентите, като събития или поредица от нежелани или неочаквани събития са предизвикани от престъпни деяния. **Широката осведоменост** на обществото за рисковете е от изключително значение за превенцията на престъпността в киберпространството. Адресирането на проблемите, свързани с постоянно развиващите се форми на киберпрестъпността е важно за всички нива на образованието и общата осведоменост, като внимание трябва да се обърне на подрастващите, които все по-интензивно „живеят“ във виртуалното пространство.

Приоритетни насоки за действие

3.4.1. Превенция на киберпрестъпността

- Повишаване нивото на информираност на обществото за състоянието, структурата и тенденциите в развитието на киберпрестъпността и причините и условията, които я улесняват;
- Своевременно осведомяване на гражданите, бизнеса, обществото за нововъзникващи киберзаплахи и свързаните с тях ескалиращи възможности за престъпни посегателства, така че всички възможно засегнати да бъдат осведомени за рисковете, пред които се изправят в онлайн средата, и да могат предварително да вземат самостоятелно мерки за защита;
- Засилване на сътрудничеството с неправителствени организации, бизнес асоциации и общности и образователни институции за разработване и прилагане на програми, насочени към различни групи от населението с оглед тяхната роля и уязвимости в киберпространството;

- Разширяване подкрепата на мрежите от изследователи, които събират информация за приложения, рискове и последствия от онлайн технологиите върху живота на децата. Фокусиране на превенцията върху закрилата на подрастващите в онлайн среда, във връзка с тяхната пристрастеност към интернет, зависимостта им от социалните мрежи, както и слабата им осведоменост за различните форми на киберпрестъпления и предвидените санкции за извършени наказуеми деяния. Чувствително ограничаване разпространението на материали, съдържащи случаи на сексуална злоупотреба с деца;
- Дефиниране на специфични мерки и действия за превантивната защита срещу съществуващи и нововъзникващи заплахи, и съгласуваност с прилаганите мерки за киберхигиена, за достигане на общо високо ниво на МИС, включително по отношение на непознати въздействия и атаки;
- Прилагане на адекватни мерки за индивидуална превенция и защита с цел предотвратяване на увреждащо въздействие върху потенциално заплашените субекти/обекти;
- Повишаване на правната култура на крайните потребители относно наказуемостта за типичните деяния, извършвани в киберпространството. Ежегодно организиране на **седмица на превенцията на киберпрестъпността;**
- Провеждане на осведомителни кампании за ограничаване използването и разпространението на нелицензирани цифрови продукти (софтуер, медия), което представлява престъпление по отношение на авторските права, и е сериозна заплаха за разпространение на зловреден код и последващи нелегитимни действия (включително и „съучастие“ в киберпрестъпни деяния в голям мащаб, чрез бот-нет мрежи, откраднатa идентичност и др.). Засилване на превенцията чрез широко огласяване на резултатите от проведени операции на правоохранителните органи, както и елиминиране на практиката за използване на нелицензиран софтуер и отсъствие на минимални мерки за киберзащита в публичните институции при персонална отговорност на ръководителите им;
- Широко популяризиране в медиите на Центъра по киберпрестъпност в ГДБОП-МВР и неговата мисия по разкриване, разследване и документиране на компютърни престъпления. Повишаване правната култура на гражданите относно общественото им задължение за уведомяване за киберпрестъпления, които са им станали известни или са потърпевши от тях.

3.4.2. Повишаване на административния, организационен и технически капацитет и способности на компетентните структури

Устойчивата тенденция към нарастване броя на компютърните и компютърно-свързаните престъпления, все по-лесния достъп на правонарушителите до средства за извършване на такива престъпления, включително чрез ползване/предоставяне на киберпрестъпни услуги[59] ограничава възможността за реакция от страна на правоохранителните и правоприлагащите органи. Ефективното изпълнение на възложените им със закон функции за разкриване, разследване и наказателно преследване

59 Предоставяни вече и като услуга - Cybercrime-as-a-service.

на правонарушителите, налага повишаване на техния административен, технически и организационен капацитет и способности **чрез реализиране на комплексни мерки:**

- Институционално укрепване на съществуващи специализирани структури в МВР, пряко ангажирани с противодействието на киберпрестъпността чрез:
  - прецизиране на функционалната им компетентност;
  - осигуряване на необходимите човешки ресурси и съвременни технически средства и технологии;
- Засилване на информационния обмен с Европейския център за борба с киберпрестъпността в Европол, с **партньорските структури и организации** за постигането на ефективно и навременно разследване на киберпрестъпления с трансграничен характер;
- Повишаване на капацитета и способностите за ефективно участие в трансгранични съвместни екипи за разследване на киберпрестъпления със служби и органи на други държави и международни организации, формирани под ръководство на ВКП;
- Активно участие в различните международни и регионални инициативи и проекти за противодействие на киберпрестъпността;
- Ефективно използване на възможностите за обучение в рамките на двустранното правоохранително сътрудничество, в обучителните курсове, организирани от Агенцията на Европейския съюз за обучение в областта на правоприлагането;
- Чрез споразумение за ПЧП в областта на обучението осигуряване на **високи нива на компетентност** на полицейските служители; осъществяване на трансфер на опит и добри практики по отношение използването на нови методи за анализ на заплахите и оценка на риска; прилагане на иновативни инструменти в събирането и изследванията на доказателства за престъпления в киберпространството.

3.5. Киберотбрана и защита на националната сигурност

Цели:

***Цел 1: Защита и противодействие** на различни видове **атаки и организирани действия с деструктивен характер в киберпространството,** които застрашават сигурността и стабилното функциониране и развитие на държавата и обществото, както и партньорски държави по силата на взаимни договорености и ангажименти.*

***Цел 2:** Постигане на устойчивост към организирани мащабни хибридни въздействия на институционално и национално ниво, гарантиране и поддържане на основните функции на държавата (управление, бизнес, граждани) и възстановяване на нормалната дейност.*

Мерките за постигането на тези цели и поетапното им изпълнение ще доведе до повишаване на сигурността и устойчивото и конкурентно развитие на гражданското общество, бизнеса и държавата в киберпространството. Те са органично свързани с развитието на Националната система за киберсигурност, с изграждане на модела за координация и взаимодействие на национално ниво и осигуряват развитието в **два аспекта**:

- Защита и киберустойчивост на комуникационните и информационни системи, мрежите и организацията за управление на **националната отбрана и въоръжените сили** на Република България, и изпълнение на ангажиментите и

активно участие в развитието на способности за колективна отбрана на **споделеното киберпространство** с партньорите и съюзните държави от НАТО и ЕС;

- Осигуряване на **ефективен механизъм за бърза и координирана реакция** при мащабни кибер и хибридни атаки и кризи с възможни катастрофални последствия, както и устойчивост на системите за управление на жизненоважните ресурси за функциониране на държавата и обществото в извънредни ситуации.

Киберотбраната е **третият основополагащ стълб** на киберсигурността съгласно Европейската стратегия за киберсигурност (2013г).

Приоритетни насоки за действие:

3.5.1. Киберотбрана и въоръжени сили

Използването на киберпространството като пети оперативен домейн за провеждане на операции и вменените със Закона за киберсигурност отговорности на министъра на отбраната за защита и активно противодействие на кибератаки и хибридни въздействия върху системите за управление на отбраната и въоръжените сили изискват прилагането на взаимообвързани и допълващи се мерки за осигуряване и развитие на административен, технически и организационен капацитет и способности за киберотбрана, съвместими с тези на съюзниците в НАТО и ЕС, както и общи такива на съюзно ниво:

- Установяване и развитие на устойчив организационен модел за координирано и ефективно ръководство, планиране и управление на киберотбраната на стратегическо, оперативно и тактическо ниво;
- Интегриране на киберотбраната, като елемент от стратегическото планиране в програмите за изграждане на отбранителни способности и в плановете за провеждане на операции от въоръжените сили;
- Развитие на център за киберотбрана (milCCIRC) за осигуряване на непрекъснато наблюдение (24/7) и оценка на сигурността на КИС и формиране на пълна оперативна картина на киберпространството;
- Развитие на екипи за киберотбрана, включително за своевременна реакция на киберинциденти и атаки и възстановяване на критични комуникационни и информационни услуги за изпълнение на мисиите на въоръжените сили;
- Реализиране на инвестиционни проекти за киберотбрана и използване на възможностите на членството на Република България в НАТО и ЕС, както и на програмите за подкрепа и двустранно сътрудничество с други страни за участие в съвместни инициативи и развитие на общ капацитет и способности;
- Изграждане на експертен капацитет по киберотбрана с развитие и използване на възможностите на националната и военно-образователната системи и повишаване на знанията и подготовката на личния състав за провеждане на кибероперации, чрез участие в курсове, тренировки и учения в национален и международен формат;
- Ефективно използване на членството на Република България в Центъра за компетентност на НАТО в областта на киберотбраната (NATO CCD CoE), както и възможностите на Центъра за компетентност на НАТО за управление на кризи и реакция при бедствия в София[60] за развитие и усъвършенстване на специалисти по

60 NATO CMDR COE – NATO Crisis Management and Disaster Response Center of Excellence

планиране и провеждане на операции в киберпространството и за изучаване на съвременните устойчиви заплахи, атаките срещу КИ, методите и системите за защита;

- Координирано споделяне на добри практики, информация за киберинциденти и взаимопомощ с държавни институции, НАТО и ЕС, сътрудничество с бизнеса и академичната общност;
- Развитие на изследователска и научно-приложна дейност за създаване на устойчиви системи и модели в областта на киберсигурността, както и подобряване на взаимодействието с научни и изследователски организации и активно включване в международни програми на НАТО и ЕС по линия на изследователски проекти;
- Прилагане на комплексен и цялостен подход за формиране и развитие на орган/и за оценка на съответствието на продукти/средства, процеси и услуги за киберсигурност с национално значение, съгласно Регламент ЕС 2019/881 на Европейския парламент и на Съвета;
- Адаптиране и прилагане на модела на ЕС и НАТО за обединение и споделяне на ресурси на национално ниво, специалисти, технологии, база и развитие на формите на ангажираност – използване на механизма за резерв на въоръжените сили за създаване на специализиран „киберрезерв“ и други форми на ангажиране на киберспециалисти от индустрията, академичните и професионалните среди.

3.5.2. Противодействие на хибридни заплахи и кибертероризъм

- Прилагане на мерки и средства за **повишаване на осведомеността** за цялостната среда от заплахи и състоянието на киберкартината на национално ниво (на базата на националната мрежа НКОМКС), разработване и въвеждане на унифицирана и надеждна система от индикатори за оперативна оценка, разпознаване и предупреждения на национално ниво (както и в мрежите на НАТО и ЕС);
- Изпълнение на мерки за повишена защита, устойчивост на системите за мониторинг и контрол на националните граници, контролно-пропускателните пунктове, за координирано управление на пристанища (в съответствие с National Single Window)[61], летища, ръководство на въздушно движение, и осигуряване на непрекъснато оперативно взаимодействие със съответните структури на ЕС, Шенгенското пространство, НАТО и други партньорски организации и мрежи;
- Развитие на комбинирани мерки и средства за **идентифициране и асоцииране на източниците и извършителите** на хибридни действия (които в преобладаващата част използват ИКТ и киберпространството като средство за въздействие);
- Развитие на способности за превантивно и активно координирано противодействие за ограничаване на вредните последствия и предотвратяване на извънредни ситуации;
- Установяване на специфични оперативни процедури и средства за **бързо действие при особено интензивни агресивни и деструктивни въздействия** от типа на терористични актове (с кибер или хибриден характер), насочени към КИ и създаване на способности за формиране на екипи за бързо реагиране (RRT) със смесена крос-секторна и международна експертиза;

61 Directive 2010/65/EU National Single Window (NSW) for maritime transport

- Установяване на критерии и процедури за управление, вземане на решения и **готовност за отговор в извънредни ситуации** и съответни организационни и технически средства за: реализиране на **непрекъсната осведоменост и контрол на ситуацията на национално ниво** в целия диапазон - състояние на повишена интензивност и мащаб на инцидента, заплаха от кибер и хибридна криза, извънредни ситуации с характеристики и степен на възможно въздействие от мащаба на кибер или хибридните войни; съгласуваност, координация и тестване на механизмите за **получаване и предоставяне на международна помощ и колективни действия**.

3.5.3. Киберразузнаване

- Установяване на механизми и технически средства за поддържане на актуална картина на възможните заплахи от различен мащаб, източници и характер (кибер, хибридни), тенденции за развитие в геополитически контекст и съответен анализ на националната киберкартина, интегриране с НКОМКС;
- Развитие на способности за подпомагане установяването на източниците на въздействия при атаки (“attribution”) и предприемане на адекватни форми за защита и противодействие.

4. Взаимодействие между държава, бизнес и общество, подобряване на споделянето на информация

Цели:

Развитие ***на ефективен механизъм и среда за споделяне на информация и взаимодействие между всички групи заинтересовани страни*** *за постигане на отворено, сигурно и безопасно киберпространство*

Целта изисква идентифициране на интересите и очакванията в краткосрочен и дългосрочен план, разпределение на отговорностите и ангажиментите. Отговорността за надеждността и сигурността на киберпространството е обща и налага споделяне на информация, изграждане на съвместен капацитет, повишаване на общото разбиране и „култура“ за киберсигурност и стремеж към киберустойчивост, както и съвместното развитие на сигурна, надеждна и атрактивна киберсреда за развитие на конкурентна икономика и общество.

За постигане на тази цел Съветът по киберсигурност към Министерския съвет създава Работна група на **високо равнище** по въпросите на подобряване на взаимодействието и споделянето на информация между държавните институции, бизнеса, академичната общност (БАН и Съвета на ректорите), НПО в сферата на киберсигурността. Работната група следва да осъществява подготовка и наблюдение на изпълнението на програма „Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество“, финансирана от държавата и бизнеса и одобрявана и отчитана ежегодно от Съвета по киберсигурност.

Приоритетни насоки за действие:

4.1. Установяване на ефективни механизми за споделяне на информация и ангажираност на всички заинтересовани лица

- Идентифициране и ангажиране на всички групи заинтересовани лица за определяне на необходимостта, възможностите и интересите за споделяне на информация относно възникването и оценяването на рисковете от въздействието на инциденти на различни нива: **стратегическо, оперативно, техническо**; идентифициране, анализ, и координирано приемане на мерки за управление на заплахите; непрекъснат преглед и подобряване на мерките за справяне с инциденти и възстановяване;
- Определяне на **целевите роли и интереси на различните групи заинтересовани лица** и установяване на адекватна **форма на участие в Националната система за киберсигурност** – от съдействие за набелязване на мерки за изпълнение на поставените цели, през участие в проекти за развитие на капацитет и способности, до пълно включване с поемане на отговорности, участие в ПЧП;
- Стимулиране и подпомагане създаването на адекватни групови и **колективни платформи за споделяне на информация и колективен отговор** - на базата на секторен подход (за отделни сектори и подсектори – напр. енергетика, транспорт, финанси); на клъстерен принцип – бизнес и териториални връзки и зависимости; на основа вериги за доставки и по-общите – за създаване на стойност. Развитие на съответни пакети и стимули за всички заинтересовани страни;
- Адаптиране, развитие и прилагане на форми и методи за институционализация - **създаване на секторни и клъстерни центрове и организации** за споделяне на информацията и анализ (на базата на опита на САЩ и държави от ЕС[62] и различните модели на ISAC/ISAO[63]) и разширяването им от механизъм за споделяне на информация до активно включване в националната мрежа НКОМКС и ефективно участие в колективната защита и противодействие - допълването им със съответни оперативни и специализирани технически способности и екипи/центрове за реакция;
- Развитие на методите и средствата за изграждане на **доверие за обмен на информация.** Използване на протоколи и правила, съгласно утвърдени международни и национални стандарти и модели, за постигане на доброволно, но силно ангажирано и отговорно участие[64].
- Разработване на **национална класификация и общ „език“** за споделяне на чувствителна информация, хармонизирана с международните норми и практики, с националното законодателство и съответстваща на развитието на всички аспекти на киберпространството – заплахи, инциденти, реакция и превантивни мерки, оценка на риска и нива на готовност, еквивалентни нива на чувствителност на информацията (в национален и международен аспект). Съгласуване на изискванията към информационните канали, източниците на информация и отговорностите[65], които да стимулират включването на публични и частни

62 САЩ, Кралство Нидерландия и др.

63 ISAC – Information Sharing and Analysis Centers, ISAO – Information Sharing and Analysis Organizations

64 Стратегия за кибер сигурност на Кралство Нидерландия - “Voluntary, but not without engagement”

65 Напр. нивата за ограничено споделяне на ISAC/ISAO на базата на „светофар“ (TLP); кодовете за нива на заплаха „зелен-жълт-оранжев-червен“ (време, бедствия) – широко използвани в национални и международни мрежи

организации в националната мрежа НКОМКС и тяхната ангажираност на оперативно и техническо ниво за справяне с инциденти и кризи;

- Дефиниране и изпълнение на общ пакет от мерки за гарантиране на сигурността и **надеждността на информационните канали**, в съответствие с мерките за повишаване на МИС – нива на защита и криптиране, сегментиране и регламентиран достъп, мерки за повишена сигурност, като HTTPS-only, удостоверяване на домейни (DNSSEC) и други допълнителни препоръки на международните интернет организации и партньорски мрежи и организации;
- Установяване, институционализиране и ускорено развитие на **ефективно публично-частно партньорство за киберсигурност** като основен механизъм на взаимодействие и ангажираност за изграждане и разширяване на НКОМКС;
- Активно взаимодействие и включване в Европейската инициатива за договорно „Публично-частно партньорство за киберсигурност“[66], развитие на „Единен цифров пазар“[67] и мрежите и програмите на НАТО[68] – ангажиране на ИКТ асоциации и клъстери, изследователски и академични организации, както и на национални, секторни и клъстерни бизнес асоциации, индустриални и работодателски организации, неправителствени организации.

4.2. Фокус върху средния и малък бизнес

През 2019 г. индексът за навлизането на цифровите технологии в икономиката и обществото (DESI) показва, че само 6% от малките и средни предприятия в България осъществяват продажби онлайн, а съгласно Националната програма за развитие – визия, цели и приоритети България 2030[69] делът им към края на периода следва да достигне 12% при средно 17% за ЕС. За да се осигурят условия за ускоряване на цифровата трансформация на малкия и средния бизнес се предвижда предприятията да получат подкрепа в областта на цифровите технологии и информационната сигурност.

***Приоритетни насоки за действия в областта на киберсигурността*:**

- Инициране на фокусирани програми, добавяне на основните мерки към програмите за развитие на **конкурентоспособността на малкия и среден бизнес, включително и микропредприятията,** за повишаване на осведомеността и „киберкултурата“, включващи специфични пакети от препоръки и изисквания, така, че да гарантират **ефективно участие в единния цифров пазар** (на национално и международно ниво), осъзнаване на цифровата зависимост от каналите за информация, управление на доставките, сигурността на комуникационните и информационни системи. Внедряване на базови или адаптирани за малки и средни предприятия(МСП) стандарти за информационна и киберсигурност на ниво предприятие;
- Развитие на механизмите за насърчаване и организирано **включване на малките и средните предприятия в мрежите за споделяне на информация и превенция** на базата на секторен или клъстерен подход, осъзнато споделяне на **киберрисковете**

66 European cPPP – Contractual Public-Private-Partnership for Cybersecurity (2016) industrial research and innovation – ECSO: European Cyber Security Organisation

67 Digital Single Market (DSM) strategy of European Commission (EC) and Rolling Plan 2015 for ICT Standardisation

68 NATO NICP – NATO Industry Cyber Partnership http://www.nicp.nato.int/index.html

69 Одобрени с Решение № 33 на Министерския съвет от 20 януари 2020 г.

по веригите за доставка и целия поток на взаимосвързан цифровизиран бизнес и пазари;

- Дефиниране и прилагане на адаптиран подход за стимулиране на инициативност, саморегулация и следване на културата на „**дигиталните лидери**“ – развитие на киберкомпонента в бизнес отношенията и комуникациите и използване на типичните бизнес екосистеми: „малки за малки“ (малкият бизнес и гражданите се обслужват от малки софтуерни и ИТ фирми, без специфичен фокус и внимание към кибераспектите), „малки за големи“ (малките фирми участват преобладаващо във вериги за доставки и допринасят за общата киберсигурност, или за „несигурността“) – активно ангажиране на бизнеса и ИКТ асоциациите, приоритетно подпомагане от държавните институции, националните и международните програми;
- Организиране на специфични секторни и междусекторни **симулации, упражнения или учения** с цел повишаване знанията и ангажираността на малкия и среден бизнес и създаване на условия за включването му в обхвата на националните и международните упражнения или учения.

4.3. Установяване на обща комуникационна стратегия за информираност относно кибервъздействия и противодействия

- Във взаимодействие с всички заинтересовани страни да се разработи **обща стратегия и препоръки за комуникация и публично споделяне на информация**, свързана с инциденти и последствия, като компетентните органи следва да постигат нужния баланс между интереса на обществеността да бъде информирана за заплахите и възможните търговски щети и накърняването на репутацията на публичните администрации и участниците на пазара, свързани с инцидентите, както и да бъде гарантирано адекватно санитаризиране на информацията и конфиденциалност до отстраняване на пробивите;
- Всички организации и институции с отговорности по управление, стопанисване, експлоатиране и развитие на различни сегменти и ресурси в киберпространството да установят вътрешни комуникационни политики, процедури и механизми, които да осигуряват своевременна управленска информация на ръководството за заплахи за киберсигурността и състоянието на поверените им системи и ресурси, ситуационна оценка в контекста на националната киберкартина (поддържана от НКОМКС), както и своевременно съгласуване на управленско ниво и чрез платформите за споделяне на информация на подходящ формат за навременно информиране на гражданите и обществеността чрез електронните медии, социалните мрежи и други информационни канали.

4.4. За сигурна, свободна и надеждна интернет среда

- Компетентните държавни институции в широко взаимодействие с неправителствените организации[70] и на базата на препоръките на световните интернет организации да продължат да развиват управлението и стопанисването на дейностите, свързани с управление и достъп на граждани и бизнес до интернет

70 Интернет общество, ИКТ и софтуерни асоциации, интернет доставчици и доставчици на електронни услуги, бизнес и работодателски организации

свързаност и информация, като развиват ефективен регулаторен и саморегулаторен механизъм, гарантиращ баланса между достъпност и надеждност, сигурност и поверителност, защита на личните данни и чувствителната информация и дейностите в интерес на националната и колективна сигурност - особено внимание следва да се обърне на запазването на неформалните, ползващи се с доверие и голямо обществено влияние канали за споделяне на информация между участниците на пазара, както и между публичния и частния сектор;

- Адаптиране, изпреварващо развитие и **прилагане на препоръките на международните интернет институции и организации, така че** демократичното развитие и управлението на интернет пространството в страната да постави Република България сред водещите държави в света с напълно изградена инфраструктура за **сигурна криптирана комуникация и валидация на интернет домейните** (като инициативите „https-only" и DNSSEC);
- Въвеждане на мерки за осигуряване на **надеждност, достъпност и сигурност на отворените данни** – прилагане на специфични изисквания и стандарти към доставчиците (публични и частни) и базираните на отворени данни системи и услуги[71].

5. Развитие и подобряване на правната и регулаторната рамка

Спецификата и динамиката на развитието на обществото и пренасянето на основни дейности в киберпространството изискват **адекватна, модерна и адаптивна правна и регулаторна рамка** за определяне на ролите и отговорностите на участниците в киберпространството, така че да се осигури ефективно и ефикасно взаимодействие между всички заинтересовани лица, защита на ценностите и осигуряване на сигурна и надеждна среда за устойчиво развитие на граждани, бизнес и държава. В процеса на цифровата трансформация икономиката и обществото са по - уязвими за киберзаплахи и кибератаки. Киберпрестъпленията обхващат широк спектър от престъпни дейности, които имат изразен мултинационален и трансграничен характер. В тези условия правоприлагащите органи трябва да разполагат с надеждни правни инструменти за координиран и съвместен отговор на заплахите.

Развитието и усъвършенстването на правната и регулаторната рамка се основава на принципа за съответствие и пропорционалност на нормативно въвежданите мерки /изисквания/стандарти на идентифицираните заплахи и рискове, както и на възможностите, мащаба и обхвата на различните категории организации (публични, бизнес, граждански).

Цели:

Цел 1: *Усъвършенстване на нормативната уредба съобразно динамиката на обществените отношения в областта на киберсигурността. Своевременно транспониране на законодателните инструменти на ЕС във вътрешното право на Република България.*

71 В изпълнение на Директива (ЕС) 2019/1024 за свободно достъпните данни

Цел 2: *Адаптиране на политическата и правната рамка към новите технологични тенденции и нововъзникващи технологии.*

Приоритетни насоки на действие

- Въвеждане в националното законодателство на актовете на правото на Европейския съюз в областта на киберсигурността;
- Развитие и подобряване на правната уредба за регулиране на изискванията за киберсигурност и контрол за спазването им, за да се предотвратява и намалява до минимум въздействието на атаки и инциденти, засягащи МИС;
- Усъвършенстване на нормативната уредба в областта на защита на информационните и комуникационните системи **с критично значение за дейността на стратегическите обекти** и дейности, от значение за националната сигурност;
- Приемане на законови промени за **гарантиране на ефикастно разследване и наказателно преследване** на престъпления в киберпространството с оглед на тяхната специфика, включително като проявление на хибридни въздействия, за да се осигури надеждна защита на правата и законните интереси на гражданите, бизнеса и държавата, и да се подобри сътрудничеството и съвместния отговор на ниво ЕС и в по-широк международен план;
- За осигуряване на висококачествени и достъпни услуги от обществен интерес в областта на киберсигурността, установяване на нормативна основа за **дългосрочно договорно сътрудничество** с участие на публични и частни партньори при изграждане на технологични паркове, центрове за върхови постижения, центрове за компетентност и в развитието на НКОМКС и съответните механизми за споделяне на информация и отговорности;
- Изучаване на чуждия опит в развитието на правната рамка в областта на киберсигурността и предприемане на изпреварващи законодателни инициативи във връзка с динамиката в развитието на продукти, услуги и процеси, вследствие на новите технологични тенденции и нововъзникващи технологии;
- Прилагане на комплексен и цялостен подход за развитие на **регулаторните режими/механизми**, както и допълване на действащите такива в посока киберсигурност. Реализиране на балансиран подход между режимите на регулация и саморегулация чрез:
    - **нормативно регламентирани** минимални задължителни изисквания за МИС;
    - **комбиниран подход,** съчетаващ задължителни нормативни изисквания и доброволни секторни регламенти и наложени практики;
    - **доброволни механизми,** приложими за малък и среден бизнес, въведени на базата на осведоменост, киберкултура, неформални правила и препоръки.
- Стимулиране развитието и прилагането на схеми за **оценка (одит), и акредитация** на организации, способности и системи:
    - на ниво организации (публични и частни) и специалисти;
    - на ниво сектори и национална система за сигурност;
    - на международно ниво – в съответствие с изискванията и стандартите, сертификацията и акредитацията за взаимодействие със системите на ЕС, НАТО и други партньорски организации и държави.

- Стимулиране широкото прилагане на Европейската рамка[72] за **сертифициране на** ИКТ продуктите, услугите и процесите, за да се адресира потенциалното отрицателно въздействие на уязвимостите. Установяването и отстраняването им има важна роля за намаляване на цялостния риск, свързан с киберсигурността, с което се предоставят важни предимства за гражданите и бизнеса.

6. Повишаване на компетентностите и капацитета и стимулиране на изследванията и иновациите в областта на киберсигурността; повишаване на осведомеността

Цели:

Цел 1: *Постигане на висока* ***осведоменост на всички*** *заинтересовани страни и* ***споделено разбиране и оценка за заплахите*** *в киберпространството във връзка с нарастващата всеобща зависимост от цифровите технологии и необходимостта от адекватни мерки на всички нива за постигане на информационна и киберсигурност, развитие на обща киберкултура.*

Цел 2: *Включване на аспекти на киберсигурността и придобиване на адекватни компетентности във* ***всички нива и форми на образование и обучение*** *за създаване на специалисти и лидери за сигурно и устойчиво развитие на цифровата икономика, общество и държавно управление.*

Цел 3: Развитие на капацитет и *стимулираща среда за развитие на изследванията и иновативни приложения за превръщането на Република България във* ***водещ център за разработване на киберустойчиви системи на бъдещето в сътрудничество със съюзниците в ЕС и НАТО.***

Усилията в тази област са подчинени на приложението на оптимизиран модел за цифрова трансформация, с изпълнение на програми за промени в 4 квадранта, в две стъпки на спиралата на промяна:

- Академичен сектор
  - Изследвания по киберсигурност;
  - Образование и подготовка.
- Администрация
  - Разработване на политики;
  - Придобиване на способности.
- Оператори на цифрови системи/услуги
  - Определяне на изисквания към киберсигурността;
  - Опериране на придобитите способности - гарантиране на киберсигурност.
- Индустрия
  - Разработка на нови системи и услуги, за киберсигурност;

72 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии. Съгласно чл. 58 на този регламент всяка държава-членка определя на един или повече национални органи за сертифициране на киберсигурността.

- Производство/предоставяне на системи и услуги.

В същото време от определението на цифровата трансформация, като едновременна и хармонизирана промяна на процеси, организации, технологии и хора в новата цифрова среда на опериране, се налага да се определи обхвата на изследванията – процеси, организации, технологии, както и фокуса на обучение на хората около процеси, организации, технологии с единен фокус върху киберустойчивостта.

Мерките са фокусирани върху академичния и неправителствения сектор във взаимодействие с администрацията, операторите и индустрията.

Приоритетни насоки на действие

6.1. Изследвания, иновации и цифрово лидерство

- Стимулиране развитието на изследователската и научно-приложната дейност в съвременните и предизвикателни области на информационната и ИКТ сигурност[73] и създаването на устойчиви системи и модели в съответствие с областите на Стратегическата изследователска програма за киберсигурност (ЕС)[74] – поддържане на високо ниво на международно сътрудничество с водещи световни центрове и специалисти с фокус върху горещи и актуални области във връзка с настоящи и бъдещи предизвикателства, технологии, развитие на инфраструктурата, методи и модели за използване – европейски програми, мрежи (координационни центрове), включително и за свързаните области - квантови изчисления, суперкомпютри, изкуствен интелект (ИИ) и т.н. , както и за новите технологии с НАТО;
- Ангажираност на всички заинтересовани страни за идентифициране на перспективни и критични области и осъществяване на продуктивна връзка и взаимодействие между центровете за научни и приложни изследвания, академичните звена, водещите софтуерни и ИКТ фирми, и академичните звена в различни сектори и обвързване на **магистърски и докторски програми с реални бизнес и индустриални приложения** за формиране на национална (академична) общност за киберсигурност за участие в Програмите „Цифрова Европа“ и „Хоризонт Европа“ чрез Националния координационен център по киберсигурност.
- Създаване на ефективни механизми за ангажиране на научния и изследователския потенциал (както в България, така и от чужбина) за намиране на **иновативни решения за дейността на държавата и публичния сектор** - електронно управление и услуги, сигурност на е-идентичност и електронно гласуване, криптиране, сигурност на облачните и мобилни услуги, и други въпроси на киберсигурността, както и създаване на условия и програми за финансиране на ускореното развитие и внедряване;
- Приоритетно развитие и използване на механизми за подкрепа (национални, европейски, двустранни програми) и стимулиране на международно сътрудничество във връзка с приоритетното развитие на цифровата икономика и

73 ИКТ сигурност- ИКТ продукти, ИКТ услуги и ИКТ процеси в областта на киберсигурността - виж в чл. 2, т.12, т. 13 и т.14 на РЕГЛАМЕНТ (ЕС) 2019/881 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността)

74 ENISA: Strategic Research Agenda - https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view и връзка с cPPP (Contractual PPP on CYBER)

информационното общество в България. Развитие и стимулиране на формите на **ПЧП и клъстери** за създаване на смесени изследователски и приложни лаборатории, технологични паркове и центрове, които да създават възможности и да подпомагат създаването на конкурентни и сигурни ИКТ решения, продукти и услуги, както и да подпомагат бързото и безопасно навлизане на новите цифрови технологии в бизнеса и обществото. Стимулиране на цифровото предприемачество, създаване на бизнес инкубатори за **стартиращи конкурентни бизнеси в областта на киберсигурността**.

6.2. Развитие на капацитет и споделени умения

- Развитие и разширяване обхвата на програми за **технологично развитие на индустрията, модернизация и интелигентна специализация**[75] в областта цифровата икономика и услуги – стимулиране развитието на системи с дизайн за киберсигурност и решения, гарантиращи адекватни нива на киберсигурност и защита, изграждане и развитие на съответния **индустриален, фирмен и професионален капацитет** със **с**ъздаване на **национална система за сертифициране**[76] на киберсигурността на ИКТ_продукти, процеси и услуги и за акредитиране на системите и услугите в администрацията и индустрията.
- Определяне на подходяща образувание/структура/, издигане на кандидатурата му и получаване на решение за акредитацията от Европейската комисия, за изпълнение на функции на **Национален координационен център (НКЦ) за целите** на съответния регламент на ЕС, след влизането му в сила[77]. НКЦ трябва да притежава или има пряк достъп до технологичен опит в сферата на киберсигурността и да е в състояние ефективно да привлича и да се координира с промишления сектор, публичния сектор и научноизследователската общност. Освен това трябва да разполага с капацитет да подпомага европейския Експертния център и да участва в Мрежата на националните координационни центрове, създавани в изпълнение на посочения регламент с мисия: запазване и развитие на необходимия технически и промишлен потенциал, свързан с киберсигурността, за да защити единния цифров пазар; увеличаване на конкурентоспособността и превръщане на киберсигурността в конкурентно предимство на други отрасли.
- Приоритетно развитие на съвместни инициативи, програми и проекти в новите области на цифровата икономика и цифрово зависимото общество (сигурност на облачните платформи и услуги, мобилни и умни устройства, интернет свързани устройства, и съответни приложения) – използване на механизмите за ПЧП,европейските и международните програми за изграждане на **технологични паркове, центрове за върхови постижения** и центрове за компетентност (като изграждащите се лаборатории и иновативна екосистема в София Тех Парк,

75 Иновационна стратегия за интелигентна специализация на Република България 2014-2020 г. и процес на интелигентна специализация, приета с Решение на МС №857 от 03.11.2015 г; актуализиран вариант 15.10.2015 г

76 В изпълнение на Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии

77 Регламента на ЕП и Съвета за Европейски център за промишлени, технологични и изследователски експертни познания в областта на кибесигурността –виж https://www.consilium.europa.eu/bg/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/ и https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:ST_12104_2018_INIT

приложните центрове и лаборатории в БАН, университети, центрове и лаборатории във фирми и бизнес организации, стартъп фирми) – **координация и концентриране** на създадения капацитет, база и компетентности за ефективно подпомагане и повишаване на конкурентоспособността на индустрията чрез тестване за пробиви в киберсигурността, симулационни среди за проверка и повишаване устойчивостта към атаки и пробиви и решаване на задачи и предизвикателства, дефинирани от бизнеса и държавата на базата на единна система:
    - за ранно предупреждение за киберинциденти;
    - от свързани киберполигони;
    - за оценка и управление на киберриска в секторите и междусекторно.
- Създаване на ефективен **механизъм за споделяне на ресурси, капацитет и умения** между частния, публичния и академичния сектор на базата на взаимен интерес и обща визия и стратегия за развитие – отчитане на изпреварващата роля в технологично отношение на бизнеса и необходимостта за създаване на съответна среда за развитие и подпомагане от държавата и от програмите за интелигентен растеж и развитие;
- Ангажиране на големите софтуерни, ИКТ компании и мултинационални технологични компании в Република България, които са ключов фактор и носител на съвременни средства и ресурс на световно ниво, с цел осигуряване на принос в развитието на професионални компетентности и капацитет, ускорено реализиране на механизъм за споделяне, и включването им в процеса на развитие на Националната система за киберсигурност, включително и за повишаване на общата сигурност на интернет пространството в страната, подкрепа за малкия и среден бизнес и интернет обществото, в национални и международни центрове за компетентност.

6.3. Осведоменост, образование и обучение

- **Ангажиране на всички заинтересовани страни** в повишаване на общата осведоменост и разбиране на възможните директни и индиректни последствия от кибервъздействия – включване на **киберхигиената и изискванията за киберсигурност** във всички програми за стимулиране развитието на цифровата икономика, гражданското информационно общество, електронното управление, технологиите и иновациите за повишаване на **киберкултурата** и отговорното използване на цифров обмен на информация, предоставяне и използване на електронни услуги по цялата верига на доставки и общата и споделена отговорност за киберхигиена – ефективно използване на механизмите и **платформите за споделяне на информация;**
- Добавяне на аспектите на киберсигурността и отговорното и безопасно използване на интернет и новите технологични предизвикателства (изкуствен интелект, блок-чейн, квантови изчисления) в програмите за **начално и средно образование** – ефективно обвързване с придобиването на ИКТ умения и компютърна грамотност, използването на електронно съдържание и форми на обучение, комбинация с извънкласни и игрови форми на обучение, засилване на взаимодействието и ангажираността на индустрията, обществото и семейството;

- Допълване и развитие на **педагогическите програми и обучението на учителите и преподавателите** на всички нива, с включване на елементите на киберсигурността за възпитаване на учениците в отговорното използване на ИКТ и интернет;
- Осъвременяване и модернизация на програмите в **професионалното и университетското образование** в две основни направления:
  - → създаване на специалисти за ИКТ, софтуерната и технологичната индустрия, и в различните сфери на МИС и киберсигурността – покриване изискванията за дизайн и разработване на киберсигурни и устойчиви информационни системи (сигурност, методи и принципи за „сигурно кодиране“, оценка на рисковете, стандарти и методи);
  - → изграждане на лидери на цифровизацията и кадри за развиващата се цифрова икономика и интелигентна специализация на България, съобразно новите технологични тенденции и изискванията за киберустойчивост на зависимите бизнес модели, производства и услуги от цифровите технологии;
    - Значително увеличаване (с над 50%) на броя завършващи и започващи работа в Република България специалисти по цифровизация, включително по киберсигурност;
    - Създаване на магистърски програми за подготовка на информационни мениджъри и мениджъри по киберустойчивост, мениджъри по цифровизация за администрацията, сектора за сигурност и индустрията;
- Ефективно използване на формите на **продължаващо обучение, допълнителна квалификация и преквалификация** на всички нива за допълване и актуализиране на компетентностите в сферата на киберсигурността и използването на ИКТ във връзка с бързото развитие на технологии и платформи и произтичащите нови отговорности и заплахи, функционална и тематична квалификация в съответствие с установените стандарти и сертификация чрез създаване на сертификационни програми за служителите в администрацията, сектора за сигурност и академичния сектор;
- Организиране на специфични секторни и междусекторни **симулации, упражнения или учения** с цел повишаване знанията и уменията на служители в администрациите на административните органи за справяне с киберинциденти и кибератаки, му в обхвата на националните и международните упражнения или учения.
- Развитие и използване на съвременни методи и средства за достъпно, атрактивно и ангажиращо обучение на всички нива – иновативно използване на всички медийни канали и развиващи се непрекъснато форми, социални мрежи, игрови елементи и форми на социална и колективна ангажираност, постоянно действащи програми и кампании и включване в световни и европейски инициативи (като месец на киберсигурността[78], конкурси, „хакатони“).
- Подкрепа за провеждане на Национална кампания за цифрова трансформация в рамките на стратегията "Цифрова трансформация на България за периода 2020 -

78 European Cyber Security Awareness Month (October)
US: https://en.wikipedia.org/wiki/National_Cyber_Security_Awareness_Month
ENISA: https://cybersecuritymonth.eu/

2030 г."[79], с обхват на всички слоеве на обществото и в контекста на развитието на цифровото десетилетие в ЕС.

7. Международно взаимодействие, кибердипломация

Цели:

Цел 1: *България ще изпълнява активна роля в международното сътрудничество в областта на киберсигурността на европейско и на глобално ниво. Ще допринася за формирането на международни стратегии, за разработване на правно обвързващи регламенти, за наказателно преследване, обмен на информация, участие в международни учения с фокус върху киберсигурността и разработване на съвместни проекти за сътрудничество по линия на НАТО, ЕС, ООН и ОССЕ.*

Цел 2: *България ще продължи да изпълнява съюзните си ангажименти по линия на НАТО в областта на киберотбраната и активно ще участва в прилагането на Меморандума за разбирателство в областта на киберотбраната, одобрената по време на срещата на върха на Алианса в Уелс Инициатива за сътрудничество с индустрията в областта на киберотбраната, както и Ангажимента в сферата на киберотбраната в рамките на НАТО от срещата на върха през 2016 г. и решенията, взети в рамките на срещата на върха на НАТО в Брюксел през 2018 г.*

Цел 3: *Ангажиментите на България по линия на ЕС са обвързани със заложените приоритети в основополагащи документи като Европейската стратегия по киберсигурност, и Рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството и Европейската политическа рамка за киберотбрана. Основна цел е изграждането на гарантиран максимално защитен достъп до интернет. С оглед подобряване на националните способности и справянето с киберзаплахите, България следва активно да сътрудничи с органите на ЕС, занимаващи се с въпросите на киберсигурността (Агенция на ЕС за киберсигурност, Европол, Европейската агенция по отбрана), и да развива регионалното и двустранно сътрудничество и взаимодействие.*

Приоритетни насоки на действие

7.1. Кибердипломация

Важен елемент от ангажиментите на България за осигуряване на свободно и сигурно киберпространство е работата в областта на кибер дипломацията. Заключенията, приети на Съвета общи въпроси относно кибердипломацията[80] определят като ключово по-нататъшното развитие на **общ и всеобхватен европейски подход към кибердипломацията.** Рамката за съвместен дипломатически отговор (т. нар. инструментариум за кибердипломация) дава възможност на ЕС и неговите държави членки да използват всички мерки на Обща външна политика и политика на сигурност (ОВППС), включително при необходимост ограничителни мерки, за да предотвратяват, разколебават, възпират и реагират на злонамерени действия в киберпространството, насочени срещу неприкосновеността и сигурността на ЕС и неговите държави-членки. ЕС

79 Приета с Решение на Министерски съвет №493/17.07.20 г.,

80 Виж 6122/15 от 11.02.2015 г. Приложение: Заключения на Съвета относно кибердипломацията

и държавите-членки следва да работят заедно за постигането на стратегическите цели, заложени в Заключенията:

- Спазване и насърчаване спазването на **правата на човека в киберпространството** (предоставяне на помощ на жертвите на интернет престъпления, борба с организираната престъпност, провеждане на разследвания и запазване на електронни доказателства, осигуряване на безопасен и евтин достъп за всички граждани, насърчаване на прилагането и по-доброто използване на европейските насоки за свободата на словото, в т.ч. онлайн, и европейските насоки за защитниците на правата на човека);
- Норми на поведение и **прилагане на нормите на международното право в областта на международната сигурност** (постигане на съгласие и обща визия за прилагане на съществуващото международно право в киберпространството, отстояване на позицията, че международното право е приложимо и в интернет);
- Интернет управление (като неделима част от общия и всеобхватен подход на ЕС по кибердипломацията);
- Засилване на **конкурентоспособността и просперитета на ЕС** (с акцент върху по-нататъшното насърчаване на **Единния европейски цифров пазар** и засилване на сигурността в областта на информационните технологии, включване на цифровата икономика в националния дневен ред, тясно сътрудничество с международни партньори за защита на данните, уеднаквяване на стандартите и изграждане на доверие с трети страни);
- Изграждане и развиване на киберкапацитет - разработване на общ подход за изграждане на киберкапацитет и превръщането му в неделима част от по-широк, глобален подход във всички кибер области, вкл. чрез тясно взаимодействие със съответните органи на ЕС, използване на различни финансови програми и инструменти за устойчиво изграждане на киберкапацитет и развитие на киберустойчивост;
- Стратегическо сътрудничество с ключови партньори и международни организации за провеждане на съгласувана, ефективна и координирана политиката за киберсигурност с оглед избягване на дублирането на дейности и инициативи, осъществяване на тясно сътрудничество с международните организации, работещи в областта на киберсигурността;
- Активизиране и развитие на сътрудничеството в рамките на Организацията за сигурност и сътрудничество в Европа (ОССЕ)[81], с инициативи, програми и дейности на ООН, на международни организации и мрежи.

7.2 Взаимодействие на техническо, оперативно и стратегическо ниво

- Установяване и осъвременяване на нормативната база и международните договорености за ефективно прилагане на оперативното взаимодействие между органите и структурите от Националната система за киберсигурност и НКОМКС със съответните органи и институции от ЕС, НАТО и на двустранна база с държави партньори за развитие на съвместни способности;
- Институционализиране и договаряне на рамката за взаимодействие във връзка с платформите за споделяне на информация, както на държавно така и на смесено

81 Изпълнение на Решения на ПС на ОССЕ относно мерките за укрепване на доверието в киберпространството (PC Decisions 1039, 1202).

публично-частно ниво в сектори и области, свързани с КИ, ККИИ, стратегическите ресурси, както и с новите развиващи се чувствителни области на интернет базираните услуги (електронна търговия, здравеопазване, финанси и др.);

- Развитие и участие в регионални инициативи и проекти в областта на киберсигурността, киберустойчивостта и защита на КИ и споделени трансгранични активи и дейности;
- Осигуряване на нормативната база и договорености за провеждане на международни (включително и регионални) съвместни учения и тестове, споделяне на ресурси, капацитет и информация.

8. Реализиране, контрол и актуализация

Актуализираната Национална стратегия за киберсигурност е с хоризонт до 2023 г. Разработена е на базата на преглед и оценка на Националната стратегия за киберсигурност „Киберустойчива България 2020" от междуведомствена експертна работна група, назначена от министър-председателя, с включени представители на всички заинтересовани страни. Съветът по киберсигурността ще я предложи за приемане на Министерския съвет на Република България.

За изпълнение на Стратегията ще се разработи **Пътна карта**, която се приема от Министерския съвет, в шест месечен до 6 месеца след приемане на Стратегията. За приоритизиране на проектите и инициативите, включени в пътната карта ще бъдат ангажирани всички заинтересовани страни – държавни, бизнес и индустрия, академични, изследователски и неправителствени организации с отчитане на необходимото финансиране по организации и централно за изпълнение на Стратегията. Изпълнението е отговорност на определените водещи институции и организации, като реализацията на всички приоритетни действия и мерки ще се базира на принципите и методите на проектното и програмно управление, оценявани на базата на ключови показатели/индикатори и ориентирани към резултати. За валидацията на резултатите от изпълнението на проектите ще се организират и провеждат специализирани национални и регионални учения и тестове, както и ще се повишава участието в международни и партньорски такива.

Координацията на изпълнението на Стратегията и Пътната карта се осъществява от Националния координатор по киберсигурността, в качеството му на секретар на Съвета по киберсигурност. За оценка на напредъка на изпълнението, постигнатите резултати в отделните области, реализиране на приоритетите и насоките за действие, се изготвя годишен доклад, като при необходимост се предлага актуализация на Стратегията и съответно на Пътната карта.

За повишаване на осведомеността и ангажираността на всички заинтересовани страни и групи от населението и бизнеса, както и за партньорски държави и структури да бъде изготвено адекватно по форма и съдържание представяне на Стратегията, Пътната карта и тяхното периодично обновяване с използване на достъпни информационни, графични, медийни и интерактивни средства.

Стратегията, заедно с необходимите препратки и пояснения, се предоставя на всички държави-членки на ЕС и на съюзниците в НАТО, както и на други държави и организации на базата на двустранни договорености и взаимоотношения в областта на киберсигурността (ОССЕ, ООН, ITU, държави от региона и др.). Визираните мерки и

дейности се съгласуват и актуализират със съответните органи и партньорски организации от ЕС и НАТО, като за изпълнението на набелязаните съвместни задачи и дейности се осъществяват необходимите допълнителни договорености, както и участие в съвместни програми и инициативи.

Разработването на изцяло нов национален стратегически документ ще стартира след влизане в сила на новите законодателни актове на ЕС[82] [83], и като се вземе под внимание Съобщението на ЕК до Европейския парламент и Съвета относно Стратегия на ЕС за киберсигурност за цифровото десетилетие[84].

Ангажиментът на държавите-членки за приемане на нови Национални стратегии за киберсигурност произтича от заложените в съответната директива[85] изисквания към съдържанието и обхвата им, както и за периодичното оценяване на изпълнението, най-малко на всеки четири години, въз основа на ключови показатели и при необходимост приемане на съответни изменения и допълнения в тях.

82 COM(2020) 823 final /16.12.2020 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity

83 COM(2020) 829 final /16.12.2020 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities

84 Joint communication to the European parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade

85 DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity

Приложение:Речник

Определения[86]

Екип за реагиране при инциденти с компютърната сигурност (ЕРИКС) Computer emergency response team/CERT. - структура, която изучава уязвимостите в киберпространството и подпомага жертви на хакерски атаки, осигурява 24/7 услуги, споделя информация за повишаване на киберсигурността и координира отговори на заплахи на киберсигурността.

Заплаха - факт или събитие с потенциал, който може да нанесе сериозни вреди на дейността на организации, активи, хора или даже на държавата, чрез неоторизиран достъп, разрушаване, разкриване и промяна на данни, и/или отказ от услуги. (ISO 27000: потенциална причина за нежелан инцидент, който може да причини вреда на дадена система или организация).

Киберсигурност - състояние е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия в киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им. Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана /Съгласно чл. 2, ал.1 и ал.2, на ЗКС/

Киберпространство – глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни. /Съгласно т. 17 от ДР на ЗКС/

Киберпрестъпление – обществено опасно деяние /действие или бездействие/, извършено виновно и обявено от закона за наказуемо, насочено към или извършено в киберпространството.

Киберпрестъпност (ЕС) - обхваща традиционни престъпления (например измами, фалшифициране и кражба на самоличност), престъпления, свързани със съдържанието (напр. онлайн разпространение на детска порнография или подбуждане към расова омраза), и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ на услуга и зловреден софтуер).

Кибератака – опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив. /Съгласно т. 10 от ДР на ЗКС/

86 Забележка: Съгласно консултация с Института за български език на БАН, използваните комбинирани термини свързани с „кибер“ могат да бъдат изписвани поотделно или заедно (слято). За единство в настоящия документ и приет стандарт на разделно изписване, и образуване на съответни абревиатури.

(НАТО) – Действия, предприети за нарушаване, отхвърляне, влошаване или разрушаване на информация, намираща се в компютър и/или компютърна мрежа, както и на самите компютри и/или компютърни мрежи.

(ISO 27000) - Опит за разрушаване, разкриване, променяне, забрана, кражба ли получаване на неупълномощен достъп до или реализация на неупълномощено използване на актив.

Кибервойна - Кибервойна е всеки политически мотивиран конфликт в киберпространството, характеризиращ се с кибератаки срещу компютърните и информационните системи на противника.

Кибервойна (2) - Военни действия, водени във виртуалното пространство със средства и методи на информационните технологии. В по-широк смисъл, това представлява поддръжката на военни операции, провеждани в традиционните оперативни пространства – сухопътно, морско, въздушно и космическо – чрез действия, извършвани във виртуалното пространство.

Киберинцидент – събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информация. /Съгласно т. 12 от ДР на ЗКС/

(НАТО) - неочаквано събитие в киберпространството, което, с или без криминален умисъл, би могло да промени киберсигурността чрез фактическо или потенциално излагане на опасност на конфиденциалността, целостта или наличността на информационната система или на информацията, която системата обработва, съхранява или пренася, нарушаване или потенциално нарушаване на политиките за сигурност, процедурите за сигурност или политиките за приемливо използване.

(ISO 27000) – Събитие или поредица от нежелани или неочаквани събития, свързани със киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията

Киберкриза – сериозна заплаха за функционирането на основни структури на държавата и икономиката, и/или фундаментални ценности и норма на обществото**,** предизвикана от зловредни действия в киберпространството, която поради недостиг на време и при несигурни обстоятелства налага вземане на жизненоважни решения на национално ниво**.**

Киберотбрана – комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положени, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност. /Съгласно т. 16 от ДР на ЗКС/

Киберрезерв – допълнителен ресурс от експерти в областта на киберсигуронстта, защитата на информацията и информационните технологии, с компетентности, свързани с осигуряване на защитна и устойчивост на комуникационните и информационните системи. /Съгласно т. 18 от ДР на ЗКС/

Критична инфраструктура – стратегически обекти и дейности от значение за националната сигурност - Съгласно чл.1, ал.1 на ПМС№181 от 20 юли 2009 г., стратегическите обекти и дейности, които от значение за националната сигурност, се определят в единен списък и са част от критичната инфраструктура. Законово определение на КИ се съдържа в §1, т. 15 на ДР на Закона за защита при бедствия: "*Система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни последици за Република България в резултат на невъзможността да се запазят тези функции*".

Критична комуникационна и информационна инфраструктура - системи, услуги, мрежи и инфраструктури, които са жизненоважна част от националната икономика и общество и осигуряващи важни стоки и услуги, деструктивното въздействие върху които би могло да има сериозно влияние на жизненоважни функции на обществото. Критична информационна инфраструктура са както мрежите, каналите и системите за управлението и поддържането им.

Мрежова и информационна сигурност – способност на мрежите и информационните системи да са противопоставят на определено ниво на въздействие, засягащи отрицателно наличието, истинността, целостта, или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системни или достъпни чрез тях. /Съгласно чл.2, ал.3 на ЗКС/

Нарушение - неоторизирано действие, което преодолява механизмите за сигурност на системите.

Национален екип за реагиране при инциденти с компютърната сигурност – структура в състава на ДАЕУ, изпълняваща функции определени в чл. 19 на ЗКС

Риск – потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на информационните активите, за да се причини вреда. /Съгласно т. 30 от ДР на ЗКС/

Секторен екип за реагиране при инциденти с компютърната сигурност – структура към административен орган по чл. 16,ал.1 на ЗКС, изпълняваща функции определени в чл. 18 на този закон

Устойчивост (Resilience, NIST) – способност, свойство (на организацията) бързо да се адаптира и да се възстановява от известни или неизвестни промени в околната среда

чрез цялостно и последователно реализиране на управлението на риска, управление при извънредни ситуации и планиране на непрекъснатост на дейностите/операциите.

Уязвимост - неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата. /Съгласно т. 34 от ДР на ЗКС/

Хибридна заплаха[87] – идентифицирано намерение и способност от държавен или недържавен субект, който може да използва хибридна стратегия. Оценява се, че за да използва хибридна стратегия, един недържавен субект притежава способността да прилага всички, или почти всички елементи на силата, характерни по-скоро за една суверенна държава.

Хибриден модел на водене на война – използва се за обозначаване на съвременни конфликти, обединяващи конвенционални и неконвенционални действия, кибератаки, психологическо и икономическо въздействие, кампании за дезинформация, инфилтрация на информационната среда, създаване на паника, финансиране на нарочно създадени политически субекти, с цел промяна на външнополитическата линия на набелязаните противници и други действия за постигане на политически и стратегически цели. Хибридният модел е специфична проява на дадена хибридна стратегия, използвана от конкретен противник. Всяка хибридна стратегия е уникална, поради което всеки отговор трябва да е адаптиран към нейните особености.

Цифрова зависимост – критична зависимост на изпълнението на основните функции и дейности на институции, организации, бизнеси и обществото като цяло от ИКТ.

Цифрова инфраструктура – инфраструктура, която включва ТОИ, доставчици на DNS услуги и регистри ня имената на домейни от първо ниво. /Съгласно т. 36 от ДР на ЗКС/

Съкращения

ИКТ	Информационни и комуникационни технологии
ИТ	Информационни технологии
КЕП	Квалифициран електронен подпис
КИ	Критична инфраструктура
КИН	Конфиденциалност, интегритет, наличност (информационната сигурност)
КИС	Комуникационни и информационни системи
ККИИ	Критична комуникационна и информационна инфраструктура
МЕРГ	Междуведомствена експертна работна група

87 Национална „Стратегия за противодействие на хибридния модел на водене на война“

МИС	Мрежова и информационна сигурност
МСП	Малки и средни предприятия
НКОМКС	Национална координационно-организационна мрежа за киберсигурност
НСЦ	Национален ситуационен център
НКСЦ	Национален киберситуационен център
НПО	Неправителствена организация
ПЧП	Публично-частно партньорство
APT	Advanced Persistent Threats
CIA	Confidentiality, Integrity, Availability (КИН - информационна сигурност)
CERT	Computer Emergency Response Team (също Computer Emergency Readiness Team)
CSIRT	Computer Security Incident Response Team
ICS	Industrial Control Systems
IoT	Internet of Things (Интернет свързани устройства, Industrial internet)
ITU	International Telecommunications Union
ISAC/ISAO	Information Sharing and Analysis Center/Organization
MIL CIRC	Military Computer Incident Response Center
NCIRC	NATO Computer Incident Response Capability
NIS	Network and Information Security
SCADA	Supervisory Control And Data Acquisition

Организации, институции

ДАЕУ	Държавна агенция „Електронно управление“
ДАНС	Държавна агенция за национална сигурност
ДАР	Държавна агенция „Разузнаване“
ДАТО	Държавна агенция „Технически операции”
ДКСИ	Държавна комисия по сигурността на информацията
ЕК	Европейска комисия
ЕС	Европейски съюз
ECOC	Европейска стратегия за оперативна съвместимост
КРС	Комисия за регулиране на съобщенията
МВР	Министерство на вътрешните работи
МВнР	Министерство на външните работи
МОН	Министерство на образованието и науката
МС	Министерски съвет
МТИТС	Министерство на транспорта, информационните технологии и съобщенията

НАТО / NATO	Организацията на Северноатлантическия договор/North Atlantic Treaty Organization
НККС	Национален координатор по киберсигурността
ООН	Организация на обединените нации
ОП	Оперативна програма
РБ	Република България
СС при МС	Съвет по сигурността при Министерски съвет
СКС	Съвет за киберсигурност
EDA / ЕДА	European Defense Agency / Европейска агенция по отбрана
ENISA	European Union Network and Information Security Agency
ICANN	Internet Corporation for Assigned Names and Numbers
NCI Agency	NATO Communications and Information Agency
NIST	US National Institute of Standards & Technology/