Република България

Национална стратегия за киберсигурност

„Киберустойчива България 2020”

Министерски съвет

София, 2016

www.cyberbg.eu

National Cyber Security Strategy “Cyber Resilient Bulgaria 2020”
Sofia, 2016

Проект на Национална стратегия за киберсигурност „Киберустойчива България 2020“, разработен от Междуведомствена експертна работна група (МЕРГ), със заповед № Р-116/20.05.2015г. на министър-председателя на Република България. Отразени са препоръки и корекции, предложени в становища на академични, бизнес асоциации, професионални организации и гражданското общество в периода април-май 2016 г. в рамките на публичното обсъждане чрез сайтовете www.strategy.bg и www.cyberbg.eu, и на организираните представяния и публични дискусии.

Съдържание

Въведение

Ако не си част от решението,
значи си част от проблема.
Интернет [1]

Българското общество, като част от глобалното интернет семейство, се развива интензивно и уверено в цифровата и информационна ера. Държавата, бизнесът и гражданите разчитат на надеждното функциониране на комуникационните и информационните системи, технологиите и интернет средата, или на новото „пето“ пространство, в което вече живеем и се развиваме – **кибер пространството**. Дигиталните инфраструктури се превръщат от поддържаща среда в основен и критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на развитието на конкурентна и иновативна икономика, прозрачно управление и на модерно демократично гражданско общество. Същевременно, нарастващата и необратима **дигитална зависимост** на основните функции и дейности на обществото поражда нови значими **рискове и заплахи**. Кибер пространството носи нови уязвимости с непознат досега мащаб и потенциална сила на въздействие, които изискват повишаване на общата **кибер култура** и **колективна кибер сигурност** на цялото общество, прилагане на активни мерки за предпазване от известните видове заплахи (от небрежност до умишлени действия, използване на технически и човешки слабости), както и подготовка за „неизвестните неизвестни“ и постигане на **кибер устойчивост във всички сфери**.

Настоящата национална стратегия за кибер сигурност изразява колективния ангажимент и отговорност на всички заинтересовани страни и волята на ръководството на Република България да осигури модерна рамка и стабилна среда за развитие на националната система за кибер сигурност и постигане на **отворено, безопасно и сигурно киберпространство.** Визията за постигане на **„Кибер устойчива България 2020“** очертава етапите на развитие за израстване от базова информационна сигурност и кибер хигиена до зряло информационно общество, способно да устои на кибер и хибридни заплахи във всички сфери. Република България ще бъде надежден и устойчив партньор и участник в общите мрежи и системи и колективната сигурност с евро-атлантическите ни партньори, с иновативно и изпреварващо технологично развитие, съответно на приоритетите за развитие на икономиката и обществото, и с капацитет и способности да участва в предотвратяването и преодоляването на еволюиращите кибер заплахи и кризи.

Стратегията набелязва цели и мерки за развитие в девет **ключови области**:

1. Установяване и развитие на националната система за кибер сигурност и устойчивост
2. Мрежовата и информационна сигурност – фундамент на кибер устойчивостта
3. Защита и устойчивост на дигитално зависимите критични инфраструктури

[1] “If you are not part of the solution, you must be part of the problem” - приписва се в различни варианти на различни автори, основно на Eldridge Clever (1969); вкл. и като Африканска поговорка

4. Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество
5. Развитие и подобряване на регулаторната рамка
6. Засилване на противодействието на кибер престъпността
7. Кибер отбрана и защита на националната сигурност
8. Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността
9. Международно взаимодействие - кибер дипломация и оперативно взаимодействие

Изпълнението на целите и набелязаните мерки ще бъдат развити в План с пътна карта съобразно **набелязаните фази** за развитие.

Основните фактори за успешното и ускорено постигане на целите са:

- Обвързаност с приоритетите и целите на **Програмата на правителството за стабилно развитие на Република България (2014-2018 г.)**[2] и националните секторни стратегии;
- Идентифициране и ангажиране на **всички заинтересовани страни** и изграждане на модел и механизъм за координация на стратегическо, политическо, оперативно и техническо ниво, както и ефективна платформа за споделяне на информация и колективен отговор**;**
- Ефективно **проектно управление** за реализиране на набелязаните мерки и ясна оценка на постигнатите резултати и способности;
- Активно **международно взаимодействие** – използване опита на водещите 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.

Постигнатите резултати и изградени способности ще се валидират периодично със секторни и национални тренировки и учения, симулационни упражнения и активизиране на участието в международни учения. **Мониторингът** за изпълнение на плана, постигнатите цели и **актуализацията и осъвременяване** на Стратегията ще бъдат осъществявани от Съвета по сигурността при Министерския съвет с помощта на изградената система за координация на политическо, стратегическо и оперативно-техническо ниво.

[2] Програма на правителството за стабилно развитие на Република България за периода 2014-2018 г.http://www.government.bg/cgi-bin/e-cms/vis/vis.pl?s=001&p=0211&n=132&g=

Съкращения

ЕЕСМ	Единна електронна съобщителна мрежа
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
МИС	Мрежова и информационна сигурност
МСП	Малки и средни предприятия
НКОМКС	Национална координационно-организационна мрежа за кибер сигурност
НСЦ	Национален ситуационен център
НКСЦ	Национален кибер ситуационен 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)
ISAC/ISAO	Information Sharing and Analysis Center/Organization
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
ЕО	Европейска общност
ЕРОС	Европейска рамка за оперативна съвместимост
ЕС	Европейски съюз
ЕСОС	Европейска стратегия за оперативна съвместимост
КРС	Комисия за регулиране на съобщенията
МВР	Министерство на вътрешните работи
МВнР	Министерство на външните работи
МЕ	Министерство на енергетиката
МИ	Министерство на икономиката

МО	Министерство на отбраната
МОН	Министерство на образованието и науката
МС	Министерски съвет
МТИТС	Министерство на транспорта, информационните технологии и съобщенията
НАТО / NATO	North Atlantic Treaty Organization
НККС	Национален координатор по кибер сигурността
ООН	Организация на обединените нации
ОП	Оперативна програма
ОПДУ	Оперативна програма „Добро управление“ 2014-2020
ОПИК	Оперативна програма „Иновации и конкурентоспособност“ 2014-2020
ОПНОИР	Оперативна програма „Наука и образование за интелигентен растеж“ 2014-2020
РБ	Република България
СС при МС	Съвет по сигурността при Министерски съвет
СКУ	Съвет за кибер устойчивост

EDA / ЕДА	European Defense Agency / Европейска агенция по отбрана
ENISA	European Union Network and Information Security Agency
GOV CERT	Governmental CERT (Правителствен CERT)
ICANN	Internet Corporation for Assigned Names and Numbers
ITU	International Telecommunications Unit
MIL CIRC	Military Computer Incident Response Center
NCIRC	NATO Computer Incident Response Capability
NCI Agency	NATO Communications and Information Agency
NIST	US National Institute of Standards & Technology

1 България в съвременното кибер пространство

1.1 Дигитална зависимост, заплахи и кибер сигурност

Развитието на информационните и комуникационни технологии (ИКТ) и дигитализацията като глобален феномен промениха характера на съвременните общества от „технологични“ в „информационни“ в качествено нова, информационна ера. Държавата, бизнесът и гражданите разчитат на лесен достъп и надеждно функциониране на комуникационните и информационните системи и технологии и интернет средата, или на новото пространство, в което вече живеем и се развиваме – кибер пространството. **Кибер пространството** е електронният или „виртуален“ свят от взаимосвързани комуникационни и информационни системи, в чиито мрежи глобалната общност от над 3 милиарда граждани, или повече от 45% от населението на земята обменя информация, идеи, услуги, бизнес и приятелство, без територии и граници[3].

Модерните общества развиват и използват все по-целенасочено възможностите на кибер пространството и ИКТ за развитие във всички сфери - икономика, социален живот, култура, наука и образование, политически живот. Дигиталните инфраструктури се превръщат в гръбнак, или критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на модерна и иновативна икономика, прозрачно управление, на модерно и демократично гражданско общество.

Гражданите и обществото разчитат на достоверна и надеждна информация в интернет пространството, но също така имат нужда от доверие и защита на персоналните данни, на дигиталното „аз“, както и на адекватна защита на човешките права и свободи в кибер пространството. **Държавата** все повече разчита на интернет като канал за предоставяне на информация и услуги на гражданите и бизнеса, както и за бърз, прозрачен и широк контакт с обществото. Чрез електронното управление тя **необратимо пренася дейността** си в напълно дигитална среда.

В България близо 60% от домакинствата и над 90 % от предприятията имат достъп до Интернет, като 50% от предприятията използват 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 предимно по интернет. Интернет свързаността и скоростта на информационните канали непрекъснато расте – България е в групата на топ 20 в света по скоростен интернет, и между първите по степен на въвеждане на високо скоростен, което предоставя нови възможности за отдалечени и облачни услуги, но и нови възможности за мащабно и злонамерено използване.

Кибер пространството предоставя практически неограничени възможности за развитие на общество и бизнеса, но нарастващата и необратима **дигитална зависимост** на основните функции и дейности на обществото ера поражда нови значими **рискове и заплахи**. Умишлени или неумишлени действия могат да доведат до компрометиране на системи за управление и устройства, касаещи критичната инфраструктура или приложните системи, да възпрепятстват нормалното им функциониране или чрез

[3] http://www.internetlivestats.com/internet-users/, по-пълно определение е дадено в Речника (Приложение 3)

нерегламентирано проникване да манипулират или извличат данни и информация. Начините за откриване или блокиране на тези възможности не са традиционни и изискват нова култура на взаимодействие между участниците в кибер пространството.

Съвременната **икономика на знанието** не само зависи, но и се развива все по-перспективно в нови направления свързани с интензивното използване на информационните технологии, софтуерни системи за управление, както и на ефективни процеси, базирани на дигиталните инфраструктури. Веригите за доставки (или **веригите за създаване на стойност**) работят чрез информационните си системи и през интернет. Така към бизнес рисковете се добавят нови, **кибер рискове** с ключово значение, игнорирането на които може да доведе до катастрофални резултати.

Кибер атаките са директна заплаха за сигурността на гражданите и функциониране на държавата, икономиката, обществото, науката и образованието. Те могат да бъдат извършени от разстояние, с прости и ефективни механизми и минимални ресурси, да причинят значителни поражения с нанасяне на материални и дори човешки загуби. Кибер атаките нямат национални, културни или юридически граници. **Рисковете и заплахите** в кибер пространството са трудни за дефиниране поради сложността за определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата и трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите. Сред най-сериозните деструктивни въздействия са тези от хибриден характер - комбинация от кибер атака и физическа атака, кибер атака целяща критичен кинетичен процес, кибер атака по време на природно бедствие или неизправност в критични системи. Еднакво засегнати от случайни кибер инциденти или целенасочени кибер атаки са публичният и частният сектор, както и цялото общество в Република България.

Кибер атаките с най-голям потенциал за нанасяне на значителни щети са срещу различни **критични инфраструктури (КИ)** и уязвимости на техните системи за управление и комуникация. Нарушение в работата на общата и споделена **критична комуникационна и информационна инфраструктура (ККИИ)** оказва изключително въздействие върху обществото с непредвидими и потенциално катастрофални последици. Свързаността и зависимостта в кибер пространството позволяват пробивът в сигурността или дефект на една комуникационна и информационна система от даден сектор да доведе до **каскаден ефект** и отказ в други, отново със сериозни възможни последици и вреда на жизненоважни услуги. Реакцията при такива инциденти налага **координирани действия и превантивни мерки** за минимизиране на възможностите за прерастване в кризи, както и за адекватни последващи действия, които да доведат до своевременното възстановяване на нормалното функциониране на системите.

Източници на организирани кибер атаки може да са държавни, военни и терористични организации, индустриален шпионаж, кибер престъпници. Мотивацията варира от икономически ползи до любопитство или хулиганство, демонстриране на надмощие и др. Значителна част от кибер атаките са престъпления с цел финансови облаги от различно естество. Кибер атаки се извършват и с цел тормоз, измама, разпространение на детска порнография, нарушаване на права на интелектуална собственост. По природа те са „асиметрични“ – с малки усилия и инвестиции могат да бъдат нанесени огромни поражения, при това не винаги предсказуеми. Кибер пространството е привлекателно за престъпниците поради отдалечения достъп, липсата на ефективно правораздаване по отношение на **кибер престъпленията**. Улесняващи фактори са анонимността, недостатъчните международни регулации, неинформираността и небрежността на собствениците на информационни системи и крайните потребители. Противодействието срещу кибер престъпността се усложнява от разнообразието на атаки, очаквани поражения и мотивация на хората,

извършващи атаките. В последните години действията на кибер престъпниците са далеч по-изтънчени, поради придобитите значителни ресурси и капацитет, усъвършенстване на организационните и „бизнес“ структури, разпределението на роли и взаимодействието между криминални мрежи.

Съвременните атаки през интернет са комплексни, организирани и използват широк спектър от наречените „**съвременни упорити заплахи“** [4]**,** с продължителен скрит период. Те често са насочени към високо стойностни, но недобре защитени цели и могат лесно да ескалират от **кибер инцидент** в **кибер криза**. Източник на заплаха от особено голям мащаб са 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 **кибер тероризъм** и водене на **кибер войни** чрез прилагане на целия набор от методи, въздействащи върху комуникационните и информационните системи за нарушаване на физическата, персоналната, информационната и комуникационната сигурност. Използват се всякакви средства, като сложността и обхвата на въздействието може да засегне всички сфери на обществото и се превърне в **хибридна война** срещу държава или група от държави[5].

Тук попадат и заплахите, свързани с тенденцията на разпространение и засилване на **радикализацията и на тероризма** в глобален план, като **кибер пространството се превърна във важна арена** и източник на конкретни 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[6].

Най-уязвимо звено в кибер сигурността продължава да е **човекът.** Небрежност, незнание или недоброжелателност могат да доведат до изтичане и злоупотреба с чувствителна информация, фирмени и държавни тайни, лични данни. Липсата или непълното реализиране и спазване на фирмени и организационни политики и адекватни мерки за информационна сигурност са основното улеснение за кибер престъпниците.

Кибер сигурността е състояние на кибер пространството определяно от нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги.[7] Кибер сигурността се основава на ефективно изграждане и поддръжка на активни и превантивни мерки.

Координираното развитие на способностите на обществото чрез ангажиране на **всички заинтересовани лица** с цел противопоставяне на преднамерени или непреднамерени заплахи, адекватна реакция, овладяване и възстановяването от тях е **ново ниво на зрялост**, известно като **кибер устойчивост**, или „жилавост“ (*resilience*)[8]. Високата кибер устойчивост подготвя обществото за „неизвестните неизвестни“ и включва защита и ограничаване на вредните последствия от разрушителни въздействия, максимално запазване и функциониране на жизнено важните дейности и услуги, и своевременно възстановяване. Постигането ѝ изисква сигурност и надеждност на всички компоненти и **активи на кибер пространството**, или на цялата **дигитална екосистема**, на която разчитаме: информация, технологии, хора и съоръжения, както и специфични изисквания към дизайна и реализацията на комуникационните канали, системи и услуги, надеждната им свързаност и оперативна съвместимост. Устойчивостта се постига чрез системни и координирани действия и мерки за

[4] Advanced Persistent Threats (APT)

[5] Стратегия на НАТО за противодействие на хибридния модел на водене на война (01.12.2015г)

[6] Стратегия за противодействие на радикализацията и тероризма (2015-2025г), МС, 30 декември 2015г.

[7] По-пълно определение в Речника (Приложение 3)

[8] CERT-RMM: Resilience Management Model 2016 (http://www.cert.org/resilience/products-services/cert-rmm/) , също и в Речника (Приложение 3)

повишаване на нивото на всички компоненти и участници. За да могат гражданите и бизнесът да се възползват пълно от предимствата на глобалния дигитален свят и единния цифров (дигитален) пазар, кибер пространството трябва да е надеждно и сигурно, устойчиво на всякакви деструктивни въздействия.

1.2 Предизвикателства, рискове и възможности

България е част от глобалния процес на повишаващата се дигитална зависимост и тенденцията на нарастване, усложняване и все по-трудно предсказване на заплахите в кибер пространството. **Необратимото пренасяне на основни дейности** на българското обществото, бизнеса и държавните функции в кибер пространството поставя редица **предизвикателства и необходимост от неотложни действия**:

- Необходимост от обща визия за стратегическо развитие и постигане на кибер устойчивост на цялото общество , **национална стратегия и политики** за кибер сигурност и устойчивост ;
- Обединяване на **капацитета и способностите**, с включване на всички заинтересовани страни (държавни органи, бизнес, академични и неправителствени организации), идентифициране и развитие на способности за справяне с новите тенденции и заплахи;
- Осигуряване на необходимите организационни, технически, финансови и човешки ресурси и механизми за действия по **наблюдение** на състоянието на комуникационните и информационни системи и на кибер пространството, **реакция** и намаляване на въздействието от кибер заплахи и кибер атаки, както и **възстановяването** от тях;
- Периодичен **преглед и оценка на рисковете и заплахите** и подобряване на координираните мерки за защита;
- Усъвършенстване на **правната рамка и регулаторните механизми** за реализация на стратегията и националните политики;
- Балансиран подход между **запазване на свободата** и откритият характер в интернет и кибер пространството и гарантиране на **надеждност и сигурност** за граждани и бизнес - глобално предизвикателство, което изисква сътрудничество със съответните международни партньори и организации;
- Определяне на ясни и адаптирани към динамиката на заплахите в кибер пространството **ангажименти** на стопаните и операторите на **критична инфраструктура**, както и на доставчиците на **интернет услуги** и свързаност към сигурността на крайния клиент;
- **Компенсиране на относителното изоставане** от държавите в НАТО и ЕС в дейностите по кибер сигурността, постигане на базово ниво на кибер сигурност и поетапно ускорено развитие до кибер устойчивост на цялото общество и пълноценно интегриране в общата система на ЕС и НАТО.

Електронните услуги са широка и все по-пълно навлизаща форма за държавно управление, икономическо и обществено развитие. Редица дейности в държавата от публичния и публично-частния сектор добавиха „е-“ пред услугите си: „е-управление“ и „е-правителство“, „е-търговия“ и „е-бизнес“, „е-здравеопазване“, „е-банкиране“, подготвяме се за електронно гласуване като част от „е-демокрацията“. Те постепенно изместват традиционните форми и услуги, като нарастваща част от тях вече нямат „класическа“ алтернатива[9]. Предизвикателствата са не само за техническата защита и надеждност, но и в процеса на внедряване, изграждането на доверие и култура на ползване, както и на своевременно докладване на инциденти и проблеми.

[9] Актуализирана национална програма Цифрова България (2016 – 2020)

Изискванията за кибер сигурност и устойчивост са съществено важни при развитието на **електронното управление** в Република България и постигането на **оперативна съвместимост** в работата на администрацията в цифрова среда чрез налагането на общи стандарти и надграждане на елементи от инфраструктурата, което е приоритетна задача вече на няколко правителства. В основата са сигурната и надеждна защита на **електронната идентичност** и системите за предоставяне на услуги.

В областта на **политическия и обществения живот** нараства значимостта и съответните предизвикателства и рискове свързани с все по-широкото използване на социалните мрежи и интернет за политически и обществени дебати, обмен на мнения и дори официални становища по горещи въпроси, свързани с обществения и социален живот, действия и решения на държавните институции – президент, правителство, парламент. Този практически мигновен интерактивен канал за достъп до големи групи от хора е свързан с новите форми на **пряка „е-демокрация“**, но добавя и съответните по значимост, мащаб и бързодействие кибер заплахи. Новините вече се „раждат“ първо в интернет, а традиционните информационни канали ги цитират и коментират, и също разчитат на електронната мрежа, на нейната надеждност и достоверност. В световната практика са известни редица случаи на кражба и злоупотреба с акаунти и е-идентичност в социалните мрежи[10], свързани с отговорни държавни институции и политически фигури и разпространение на мнения и новини с потенциален или реален катастрофален ефект. България не е изключение от тези тенденции – използване на емейли и мобилни съобщения с подвеждаща информация, подмяна или фалшифициране на официални уебсайтове и домейни, злоупотреби със социални мрежи и профили с цел манипулация, създаване на паника, бизнес измами и обществени въздействия в значителни размери. Отворен стои въпросът за **надеждността на информационни източници** в интернет, за достоверност на новините, съобщенията и авторите.

Новите технологии и **тенденции за развитие** дават нови възможности за развитие на индустрия и услуги, но също водят и до нови, все още недостатъчно предвидими заплахи и предизвикателства. С поглед към 2020г, основните области са свързани с развитието на Уеб 3.0 технологиите, 4G/5G комуникациите, със съответен акцент върху защитата и контрола на личното пространство и данни, облачните услуги, все по-богатите мултимедийни форми за комуникация в социалните мрежи, интернет на „нещата“[11], роботизираните системи с изкуствен интелект и ефекта от навлизането на електронните пари. С мобилната високоскоростна свързаност гражданите и устройствата са практически непрекъснато в мрежата – от автомобила и самолета до умния хладилник и прахосмукачка, умните дрехи, както и кибер заместители на човешки органи. До 2020 година в света се очакват над 60 милиарда интернет-свързани устройства [12], като за голяма част от тях няма установени изисквания за сигурността им.

Основен проблем свързан с наследството от многобройни внедрени и действащи дори в критични сектори комуникационни и информационни системи е трудното „добавяне“ на сигурност и устойчивост. Когато **системите не са проектирани и реализирани** съобразно изискванията за сигурност, добавянето на кръпки за сигурност или защитни стени са само частични и временни мерки. Още в изискванията за системите трябва да бъдат заложени различни принципи за сигурност и устойчивост[13] и при реализацията им да се спазват съответни технически стандарти[14]. Взаимната свързаност изисква прилагането на тези

[10] Facebook, twitter – например, Генералния секретар на НАТО Столтенберг публикува позицията си за ситуацията в Сирия първо във Facebook, цитирана от всички медии

[11] IoT - Internet of Things - умни устройства, свързани в интернет

[12] Доклад на IDC, 2015г

[13] Security by Design, Privacy by Default

[14] Принципи и препоръки “Secure Coding” (CERT/SEI, Carnegie Mellon University)

принципи към всички системи, активи и участници, тъй като устойчивостта не може да е частична. Такъв подход предоставя възможности за реализиране на модерни комуникационни и информационни системи, както в публичния, така и в частния сектор, системна и цялостна модернизация. Възприемането им от бизнеса представлява изключително актуална глобална перспектива за развитие както на ИКТ и софтуерната индустрия, така в новите сфери на икономиката на знанието и свързани с интернет и дигиталните екосистеми.

Кибер сигурността е ключов елемент от **националната сигурност** на държавата – кибер пространството е специфична „виртуална“ територия без физически граници, в която също трябва да бъдат ***„гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите“***[15]. Кибер пространството се разглежда като **петия домейн** за провеждане на операции срещу националните интереси, териториалната цялост, националната сигурност на суверенните държави и правата и свободите на гражданите[16]. Увеличаването на рисковете и заплахите в **геополитическата и стратегическата среда за сигурност** и в частност на кибер пространството създават условия за увеличаване на уязвимостите на стратегическите граждански и военни комуникационно-информационни системи и системите за командване и управление на силите, участващи в мисии и операции на и извън територията на страната. Това налага адекватно и своевременно развитие и придобиване на способности за **кибер отбрана**, 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, подкрепата на международния мир и сигурност в съюзен и коалиционен формат и приноса на Въоръжените сили към националната сигурност в мирно време при овладяване на кризи от невоенен характер.

*„Кибер атака може да постави на колене една страна, без нито един войник да трябва да прекоси границата ѝ, и не е никак преувеличено да се заяви, че кибер атаките се превърнаха в нова форма на **постоянна война на ниско равнище**”*

Андерс Фог Расмусен, Генерален секретар на НАТО 2009-2014

[17]

Макар да е малка и приемана за сравнително неатрактивна като самостоятелна цел, поради пълната си интеграция и свързаност в редица партньорски мрежи на ЕС, НАТО, финансови и търговски мрежи, различни дигитални бизнес вериги, има реална възможност България да бъде набелязана като вход или елемент от кибер атаки към тези мрежи.

Сравнителен анализ, представящ силните и слабите страни, възможностите и заплахите пред България на настоящия етап е представен в Приложение 1.

[15] Законът за управление и функциониране на системата за защита на националната сигурност (ЗУФСЗНС, в сила от 01.11.2015г.)

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

[17] *NATO Secretary General 2009-2014, Anders Fogh Rasmussen* http://www.nato.int/cps/en/natolive/news_75358.htm?selectedLocale=en

2 Визия „Кибер устойчива България 2020“

2.1 Стратегически цели

Република България провежда единна национална политика за кибер сигурност, в съответствие със стратегиите и политиките на Европейския съюз и НАТО. Тя се изразява в защита на критичната комуникационно-информационна инфраструктура и възможността на гражданите, бизнеса, държавните и обществените институции да обменят и обработват свободно и надеждно електронна информация. При изпълнение на политиката ще се налагат принципи, норми и задължения за осигуряване на високо ниво на кибер сигурност, ще се развива компетентността на хората и капацитета на ведомствата и организациите да предпазват и борят с кибер заплахите.

Правителството на Република България ще гарантира сигурност в кибер пространството при спазване на **основните права и свободи на гражданите**, като основа за икономически и социален просперитет на държавата. Кибер сигурността включва както националните, така и политики и мерки на ЕС и НАТО за колективна защита и надеждност на кибер пространството.

С **хоризонт до 2020 година**, **генералната цел** на Националната стратегия за кибер сигурност и Плана за изпълнението ѝ е постигането на **кибер устойчивост на цялото общество и държава**, което се изразява в ефективна защита и адекватна реакция дори на предварително неизвестни и непредсказуеми заплахи и разрушителни въздействия в кибер пространството или други сфери на дигиталната екосистема, ограничаване на вредните последствия, максимално запазване и функциониране на жизнено важни функции и услуги, и своевременно възстановяване на нормалната дейност[18]. За постигането на тази генерална цел е необходимо да се премине през няколко фази, които системно и ускорено да развият България от изоставаща спрямо държавите в ЕС и НАТО до надежден и устойчив партньор и участник в общите мрежи и системи, с иновативно и изпреварващо технологично развитие, съответно на приоритетите за развитие на икономиката и обществото, с капацитет и способности да участва в предотвратяването и преодоляването на еволюиращите кибер заплахи и хибридни кризи.

2.2 Фази

Постигането на кибер устойчивост на национално ниво е качествено ново състояние и **ниво на зрялост** в кибер пространството. За достигането му са необходими систематични, планирани и координирани действия на всички заинтересовани страни, с ускорени темпове и поетапно определени приоритети в **три последователни и надграждащи се фази – иницииране, развитие и зрялост**.

Фаза 1 (инициираща): **кибер сигурни институции.**

Постигане на общо съгласие за приоритетите на националната стратегия за киберсигурност и плана за действие с пътна карта, установяване на координиран подход и изграждане на обща рамка на национална система за кибер сигурност, определяне на основните структури и базов капацитет, установяване на процеси и принципи за развитие, съгласувано с основните заинтересовани лица („стейкхолдери“), преодоляване на изоставането в ЕС и НАТО и осигуряване на **базово ниво на кибер сигурност**. Фокусът е върху постигането на необходимото общо ниво на информационна сигурност и надграждане до **кибер сигурност**

[18] *CERT(US) – Resilience Management Model, ISO 27000, NIST стандарти и др.*

на ниво отделни организации, основаването на **Национална координационно-организационна мрежа за кибер сигурност** със съответните механизми, процеси и техническа платформа за мониторинг на състоянието на критичните комуникационно-информационни инфраструктури и осигуряване на взаимодействие при масирани и мащабни кибер инциденти и атаки. Определяне на кибер кризата като елемент от Националната система за управление при кризи и работата на ситуационните центрове, провеждане на общи и специфични секторни учения с участието на държавни, бизнес и академични структури.

Фаза 2 (развитие - от капацитет към способности): кибер устойчиви институции и "кибер сигурно" общество.

Организиране на идентифицирания и създаден през Фаза 1 капацитет за реализиране на **устойчивост на ниво отделни организации** и способности за координиран отговор при кибер инциденти и кризи, систематични дейности по превенция. Институционализиране на устойчив механизъм за взаимодействие при мащабни кибер инциденти и кампании, заплахи от кибер и хибридни кризи. Мониторинг на цялостната кибер картина, 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): **кибер устойчиво 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, 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 кибер сигурността и устойчивостта.

Основните очаквани резултати по фази са описани в Приложение 2 съобразно зададените ключови области и мерки в т. 4, които очертават рамката за Плана за изпълнение на стратегията и Пътната карта за развитие.

2.3 Подход - общо усилие, ориентирано към резултати

Постигането на кибер устойчивост на национално ниво изисква координирани действия по сигурност и надеждност на всички компоненти и активи на кибер пространството: **информация, технологии, хора и съоръжения**, на дизайна и реализацията на комуникационните канали, услугите и системите за управлението им, тяхната свързаност и оперативна съвместимост.

Постигането на целите и дейностите за отделните фази се основава на идентифицирането, включването и активното ангажиране на **всички заинтересовани страни**. По примера на САЩ и развитите държави в Европа, първоначалната инициатива и рамката за **национална система за кибер сигурност** е ангажимент на държавата и е признак на **зряло държавно управление**. Успешното реализиране и развитие се базира на балансирано и разпределено участие, отговорности и инвестиции съвместно с бизнес, академични и неправителствени организации. В много направления индустрията води с капацитет и инициативи, и е по-активният елемент в моделите за публично-частни партньорства. 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 с поглед в перспектива, отговорностите, изискванията и препоръките за постигане на кибер сигурност и устойчивост.

Основните фактори за успешното и ускорено постигане на целите на стратегията са:

- Обвързаност с приоритетите и целите на **Програмата на правителството за стабилно развитие на Република България (2014-2018г)**[19], Национална програма за развитие: България 2020 с Тригодишен план[20] и националните секторни стратегии – постигането на адекватна сигурност на кибер пространството и дигиталната среда е съществен фактор за успешното реализиране на заложените приоритети и цели, развитие на икономиката на знанието, интелигентна специализация, секторните политики и програмите за развитие;
- Идентифициране и ангажиране на **всички основни заинтересовани страни („стейкхолдъри“)** [21] – ясно определяне на ролите, отговорностите и постигане на общо съгласие за приоритетите на дейностите по фази, както и прилагането на този принцип във всички нормативни и регулаторни рамки;
- Въвеждане на ефективно **проектно управление** за реализиране на набелязаните мерки и ясна 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 **международно взаимодействие** – използване на опита на водещите 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, ефективно обвързване на националните и международни проекти и програми, интегриране в международните мрежи за киберсигурност и действие при кибер кризи.

2.4 България – надежден международен партньор за сигурност и устойчивост на кибер пространството

В контекста на променената среда за сигурност и нововъзникващите предизвикателства, държавите са изправени пред сериозни заплахи за своята национална и колективна сигурност като мащабни кибер атаки, хибридни войни и необходимост от колективна надеждна защита на критичните инфраструктури. Република България, като част от евроатлантическото пространство, участва активно в процеса на разработване и последващо прилагане на политиките, стратегиите и инициативите на ЕС и НАТО. Опазването на **отворено, безопасно и сигурно кибер пространство** е съществено предизвикателство, на което България ще отговори чрез сътрудничество със своите международни партньори, съюзници и организации, частния сектор и гражданското общество. Ще прилага

[19] Програма на правителството за стабилно развитие на Република България за периода 2014-2018 г.http://www.government.bg/cgi-bin/e-cms/vis/vis.pl?s=001&p=0211&n=132&g=

[20] http://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=765

[21] Подход „мултистейкхолдер“ (multi stakeholder)

съществуващите международни правни норми в кибер пространството и ще допринася за изграждането на капацитет в областта на кибер сигурността. България има ясни поети ангажименти към Европейския съюз в областта на кибер сигурността и е заинтересована от тясно сътрудничество с държавите-членки и европейските агенции, работещи по въпроса. Основните задължения произтичат от:

- Европейската стратегия за кибер сигурност[22]
- Европейска политическа рамка за кибер отбрана[23]
- Европейска директива за сигурността на мрежите и информационните системи[24]
- Европейски регламенти и директиви свързани с хармонизиране на законодателството по отношение на кибер престъпността, защита на личните данни, електронна идентичност и управление, и други.

Главна обща цел е осигуряване на висока колективна степен на кибер сигурност в ЕС и НАТО посредством подобряване на националния капацитет на държавите в областта на кибер сигурността, подобряване на сътрудничеството между държавите, публичния и частния сектори, въвеждане на задължение компаниите в критични сектори (енергетика, транспорт, банкиране, здравеопазване, интернет услуги, други) да прилагат общи политики и практики за управление на риска и предоставяне на информация на националните органи за настъпили значими инциденти, да координират действията при отговор на комплексни заплахи и атаки.

Основни органи на ЕС по въпросите на кибер сигурността:

- Агенция на Европейския съюз за мрежова и информационна сигурност (EU Network and Information Security Agency: ENISA);
- Европол с Европейски център по кибер престъпления (EUROPOL - European Cybercrime Center);
- Европейска агенция по отбрана (European Defense Agency: EDA).

Ролята на ЕС в случай на **мащабна кибер атака**, застрашаваща правителства, институции, бизнеси и граждани на ЕС се изразява в **добрата координираност** и обмен на информация за успешно **колективно противодействие, превенция,** и санкциониране на извършителите.

В областта на кибер сигурността и кибер отбраната Република България участва активно и сътрудничи с Организацията за сигурност и сътрудничество в Европа (ОССЕ), ООН, международни организации за развитие на комуникациите и интернет (ITU, ICANN) и други.

[22] ENISA: European Cyber Security Strategy, 2013

[23] EU Cyber Defence Policy Framework

[24] The Directive on security of network and information systems (NIS Directive) -„Директива на ЕП и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза“ приета от ЕП на 06.07.2016г

3 Принципи

Главен принцип: 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. (Стратегия на Европейския съюз за киберсигурност „**Отворено, безопасно и сигурно киберпространство**“, 2013г.)[25]

За постигане на заложените цели в настоящата Стратегия и изпълнение на набелязаните мерки се следват следните **основни принципи**:

- Неделимост на кибер сигурността от националната сигурност;
- Защита на основните права, свободата на изразяване, на личните данни и личния живот на гражданите – мерките да не водят до ограничаване на тези права, ограничаване на възможности за достъп до интернет и пренос на информация;
- Пропорционалност - мерките за повишаване на кибер защитата и разходите да са съизмерими със съответните рискове и заплахи;
- Споделена отговорност - интегриран и кохерентен подход за разпределяне на ролите и отговорностите свързани с кибер сигурността по всички нива и органи на държавното управление, гражданите, бизнеса и институциите;
- Периодична оценка на състоянието на кибер заплахите и рисковете, оценка на нивото на кибер сигурността и съответните способности на базата на стандартизирани методи и класификация на рисковете, и адекватно осъвременяване на стратегията и мерките;
- Прозрачност при формиране и провеждане на политиките за кибер сигурност и устойчивост;
- Ангажираност на всички заинтересовани страни и развитие на ефективни и ефикасни механизми на публично-частните партньорства;
- Съгласуваност с международните ангажименти и принципи на сътрудничество и взаимодействие, активно участие в създаването на общ капацитет и способности за защита на кибер пространството;
- Обвързване на целите и мерките с конкретен план за действия, отговорности и показатели, който непрекъснато се подобрява и развива.

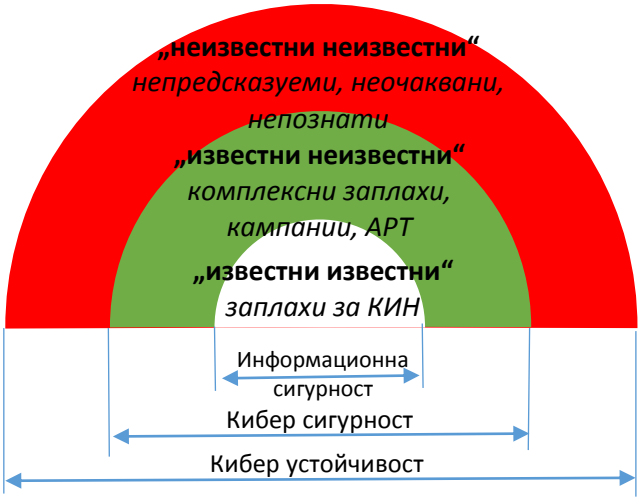
[25] (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

4 Области на действие, цели и мерки

Постигането на **стратегическата цел - кибер устойчиво общество и държава**, изисква системна и последователна политика и работа във всички области, образуващи състоянието на **кибер устойчивост,** което се характеризира с:

- Ефективна защита и комплексна адекватна реакция дори на предварително неизвестни заплахи и разрушителни въздействия в кибер пространството или от комплексен (хибриден) характер в различни сфери на дигиталната екосистема;
- Максимално запазване и функциониране на жизнено важни дейности и услуги, ограничаване на вредните последствия;
- Своевременно възстановяване на нормалната дейност.

Областите на действие и съответните целите могат да се определят съобразно двата основни аспекта:



- осигуряване на общоприетата „триада“ от областта на информационната сигурност - **Конфиденциалност-Интегритет-Наличност (КИН)** [26]
- нивото на познаване на заплахите и съответните рискове – класификацията за **„известните неизвестни“**, използвана също и в областта на националната сигурност[27]

Тези два аспекта позволяват ясно структуриране на целите и областите на действия, както и три нива на зрялост на организации, държава и общество - **информационна сигурност, кибер сигурност и кибер устойчивост**[28].

На Фигура 1 са показани трите надграждащи се нива:

- **„известни известни“** – защита и предпазване на информационните активи и комуникационна инфраструктура от известни слабости, заплахи и пробиви, свързани с основната „триада“ на **информационната сигурност (КИН)**
  - **„известни неизвестни“ (не-КИН)** - комплексни и комбинирани заплахи, свързани с информационната сигурност, ИКТ, мрежите и системите, разнообразието от **съвременни упорити заплахи** (APT[29]), атаки срещу репутацията на организации и личности, кампании за дезинформация, и други непредсказуеми последствия от масовото пренасяне на дейностите ни в кибер пространството, пробиви в КИН в особено големи мащаби (национални, регионални и световни), изискващи разширено и системно прилагане на КИН за

[26] Confidentiality, Integrity, Availability (CIA)
[27] Насим Талеб, Черният лебед - https://en.wikipedia.org/wiki/Black_swan_theory;
[28] Eurocontrol: Manual for National ATM Security Oversight (2012)
[29] Advanced persistent threats (APT)

всички активи в дигиталната екосистема - информация, технологии, хора и съоръжения, за постигане на **кибер сигурност;**

- **„неизвестни неизвестни“** или подготовка за неизвестното - неочаквани заплахи в киберпространството, динамично променящи се рискове и комплексни въздействия с непредсказуеми последствия, които изискват гъвкавост и устойчивост на системите, организацията и процесите, и съответни стандарти при разработването и внедряването им, състоянието на **кибер устойчивост**.

4.1 Установяване и развитие на националната система за кибер сигурност и устойчивост

Цели:

Главна цел: Постигане на ефективна и ефикасна система за кибер сигурност и устойчивост.

Цел 1: Изграждане на механизъм за координирани действия на **политическо и стратегическо ниво** за развитие на необходимия капацитет и способности за кибер сигурност и устойчивост.
Цел 2: Осигуряване на актуална **кибер картина** и разбиране на ситуацията[30] в кибер пространството.
Цел 3: Взаимодействие за **ефективна и координирана превенция, реакция и възстановяване.**

„Кибер престъпността е глобална и анонимна заплаха за информационните системи. Деструктивните въздействия върху информационните системи и мрежи могат да доведат до криза чрез затрудняване и/или блокиране нормалното функциониране на важни за икономиката, финансовата система и държавното управление системи или отделни компоненти“

Стратегия за национална сигурност на Република България, 2011г.

Сигурността на кибер пространството е неотделима част от националната сигурност съгласно **Стратегията за национална сигурност на Република България**[31]. Националната система за кибер сигурност и устойчивост е интегрален елемент от **системата за управление и защита на националната сигурност**. Различни държавни органи и институции в Република България имат определени роли и задължения за различни аспекти на сигурността и защитата на комуникационни и информационни системи на национално и секторно ниво. Нарастващ брой организации, включително неправителствени и от частния сектор, декларират жизнена необходимост и готовност да участват активно за повишаване на общата кибер сигурност за развитие на единен цифров пазар и общество. Капацитет развиват софтуерните и ИКТ фирми, изследователски звена, професионални организации, както и отделни специалисти. **Настоящата стратегия цели обединението и развитието** на тези дейности и ресурси в **обща структура и процеси за координирани действия на всички нива** – политическо/стратегическо, оперативно и тактическо/техническо,

[30] Situational awareness
[31] Стратегия за национална сигурност на Република България, Държавен вестник бр.19, от 08.03.2011 г.

които да 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 кибер пространството, взаимодействие и ефективно използване на техническия капацитет за превенция, координиран отговор и възстановяване, за анализ на тенденциите и създаване на способности за активно и ефикасно противодействие.

Мерки:

4.1.1 *Стратегическо ниво - политики, стратегии и планове*

Основната нормативна база за изграждане и функциониране на националната система за кибер сигурност е **Законът за управление и функциониране на системата за защита на националната сигурност** (ЗУФСЗНС, в сила от 01.11.2015г.), както и международните ангажименти на Република България, поети с влезли в сила международни договори, по които Република България е страна в ЕС, НАТО, ООН и др. Определени аспекти са регламентирани и в други нормативни актове - Закон за електронните съобщения, Закон за електронното управление, Закон за Държавна агенция „Национална сигурност“ (ДАНС), Закон за защита на класифицираната информация (ЗЗКИ) и наредбите към него, Закон за електронния документ и електронния подпис, и др.

Народното събрание на Република България осигурява приемането на нормативните актове, свързани с кибер сигурността и осъществява парламентарен контрол за нейното състояние, в рамките на контрола за управлението и функциониране на системата за защита на националната сигурност.

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

Политиката по кибер сигурността и развитието на кибер устойчивост се определя от **Правителството на Република България** и се реализира от различни държавни институции, изпълняващи отделни функции в тази област. В Програмата на Правителството за **стабилно развитие на Република България**, секторните програми и планове са отразени съответните цели, изисквания, насоки и очаквани резултати за създаване и развитие на национална система за кибер сигурност и устойчивост. Министерският съвет осигурява политическата база за развитие, приема и периодично актуализира Националната стратегия за кибер сигурност. За реализацията на утвърдената Стратегия МС приема план за изпълнение и следи за реализиране на приоритетите и целите и осигуряване на необходимите ресурси за изпълнение на заложените дейности.

Функциите на **Съвета по сигурността (СС)** към Министерския съвет на Република България включват развитие на способностите на системата за защита на националната сигурност за противодействие на заплахите, управление при кризи, осигуряването и защитата на информационната сигурност от посегателства. Съветът по сигурността при МС **формулира позицията на Република България** пред международни институции и организации по въпросите на кибер сигурността и **решенията за управлението и функциониране** на системата за защита на националната сигурност.

За постигане на Цел 1 към Министерския съвет на Република България се предвижда създаване на нещатен постоянен консултативен **Съвет по кибер устойчивост (СКУ)**, с основни **направляващи и стратегически функции**:

- изработва и обосновава позицията на Република България пред международни институции и организации по въпросите на кибер сигурността и я предлага за одобрение на Съвета по сигурността;
- изработва и предлага национална стратегия за кибер сигурност, пътната карта и плана за постигане на кибер устойчивост, както и тяхната периодична актуализация;
- следи тенденциите и развитието на кибер заплахите, рисковете, методите за противодействие и необходимите способности, приоритетите за изграждането и развитието на човешки, технологичен, инфраструктурен, финансов, организационен и доктринален компоненти и при необходимост внася предложения пред Съвета по сигурността за решения;
- подготвя за Съвета по сигурността (СС) и Министерски съвет (МС) периодичен доклад за състоянието на сигурността в кибер пространството, развитие на рисковете, и обобщена оценка на достигнатото ниво на зрялост за кибер устойчивост;
- предлага мерки за хармонизация и взаимодействие с регулаторни органи и институции;
- изготвя предложения за хармонизиране и координиране на секторните политики за постигане на кибер устойчива икономика и общество;
- изработва и предлага за утвърждаване от СС общите принципи и изисквания към мрежата за киберсигурност (НКОМКС), правилата за нейното функциониране и разширяване;
- съдейства за наблюдаване на изпълнението на проектите от Плана и пътната карта и изпълнява функциите на програмен борд (съгласно моделите за проектно управление)[32] за портфолиото от проекти на национално ниво;
- съдейства на Националния координатор по кибер сигурността за идентифициране и провеждане на неотложни координирани мерки в областта.

СКУ се председателства от Министъра на вътрешните работи и Министъра на отбраната (членове на СС) и включва представители на Министерство на транспорта, информационните технологии и съобщенията, Министерство на правосъдието, Министерство на финансите, Министерство на икономиката, Министерство на енергетиката, ДАЕУ, ДАНС, ДКСИ, ДАР, органите за реализиране на електронно управление и други ведомства, представители на бизнес, академични и неправителствени организации, определени с акта за формиране. Функцията на секретар се изпълнява от Националния координатор по кибер сигурност. Към СКУ могат да се сформират постоянни или временни междуведомствени експертни работни групи (МЕРГ), с включване на експерти от държавни ведомства, академични и бизнес организации (като МЕРГ за развитие на Стратегията и Плана, МЕРГ за развитие на модела и мрежата НКОМКС и други).

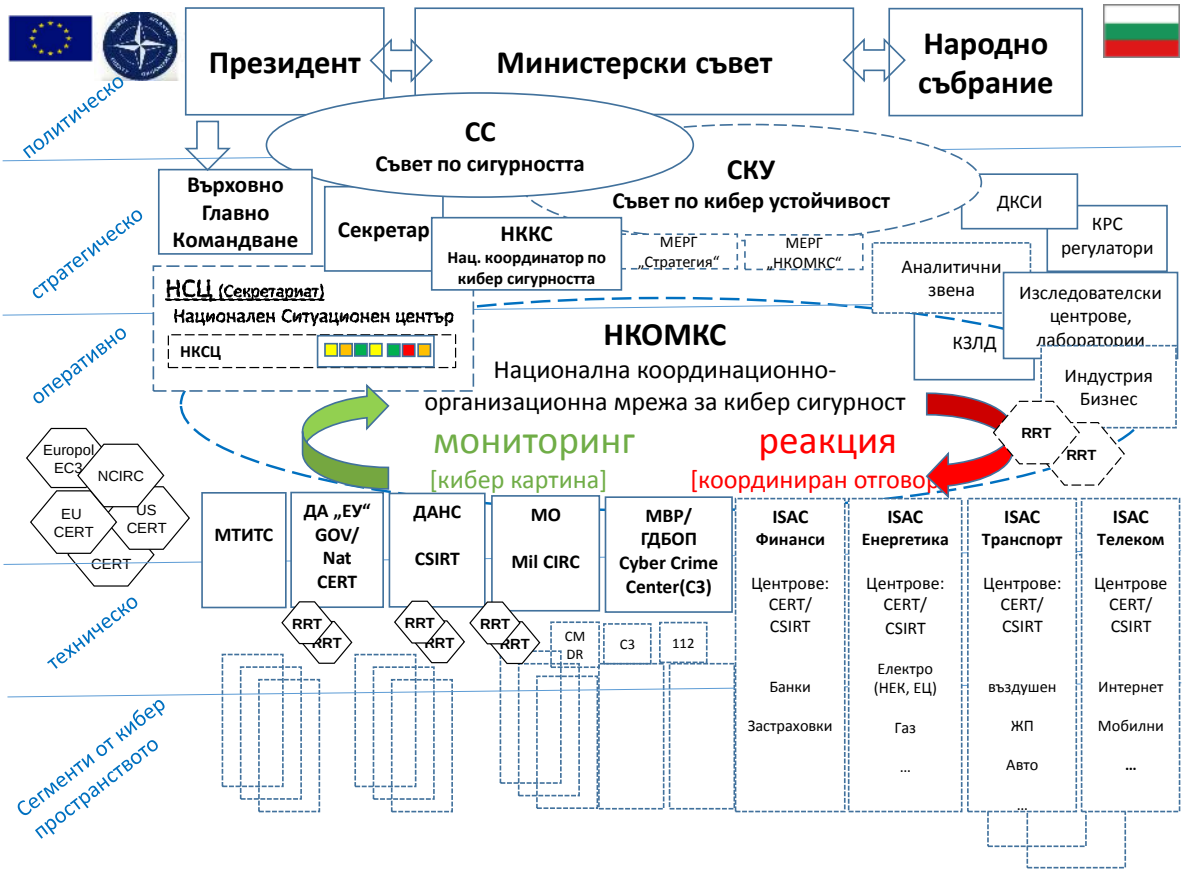
Към Министерски съвет се определя **Национален координатор по кибер сигурността (НККС)**, който ръководи изработването на Национална стратегия за кибер сигурност, план за действие по кибер сигурността и изпълнява други задачи, свързани с кибер сигурността [33].

Отговорността за разработване на адекватни секторни политики, стратегии за постигане на кибер сигурност и устойчивост, както и мерки за развитие на съответни способности имат всички министерства и ведомства, както и публични и частни стопани и оператори на критични инфраструктури, доставчици на обществени информационни и далекосъобщителни услуги. Техен ангажимент е ефективното участие в националните мерки и планове, осигуряването на съответните ресурси за развитие на капацитет и способности за последователно постигане на информационна сигурност, кибер сигурност и устойчивост на цялото общество, бизнеса и държавата.

[32] Програмен борд (Program board) – съгласно методиката за проектно управление PRINCE 2
[33] ПМС №300/19.09.2014г.

Подходът за поетапно постигане на поставените цели и максимално бързо достигане на **базово ниво на национална кибер сигурност** 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 кибер устойчивост** (Фаза 2 и 3).

Общият модел на Националната система за киберсигурност и устойчивост е представен на Фигура 2, следва описание на роли, отговорности, мерки и дейности за създаване и развитие на основните компоненти на модела.



Фигура 2. Модел на националната системата за кибер сигурност и устойчивост.

4.1.2 *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, Организацията на Северноатлантическия договор (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 координация на **оперативно ниво** се създава **организационна мрежа - Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)** със съответна техническа платформа**,** както и Национален кибер

ситуационен център (НКСЦ) в рамките на Националния ситуационен център (Секретариата на Съвета по сигурността) със следните основни функции:

- Мониторинг на актуална и пълна национална **кибер картина** - състояние на кибер пространството 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 CERT), анализ на възможни причини и източници, оценка на въздействието, както и ефективност на предприетите мерки и действия.
- **Координирана реакция (отговор)** и оперативно взаимодействие при масирани инциденти, комплексни атаки и кризи – осъществява се с организационно-технически средства и се базира на актуалната кибер картина, анализ на състоянието и чрез технически протокол и организационни мерки предоставяне на информация за състоянието на национално ниво, възможни комбинирани заплахи и хибридни въздействия, потенциален кинетичен и каскаден („домино“) ефект, и препоръки за превантивни действия на оперативно и тактическо/техническо ниво, активизиране на планове и действия от кибер отбраната, привличане на експерти (от работните групи към СКУ, международни и др.)

НКОМКС представлява „**нервната система**“ на националната система за кибер сигурност, 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 кибер сигурност (и общо в защита на националната сигурност). НКОМКС е отворена за постепенно включване на всички заинтересовани организации и институции (държавни, бизнес и неправителствени), които стопанисват, управляват, функционират и отговарят за различни активи, компоненти и сегменти на кибер пространството. За целта се дефинират и прилагат изисквания за оперативна 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 кибер пространството по отношение на аспектите на кибер сигурността и функционирането на КИС (**вътрешен мониторинг**), и екипи за **незабавна реакция** при кибер инциденти или нарушение във функционирането на КИС. Тези функции организационно и технически се изпълняват от центрове и екипи за кибер сигурност, известни като **CERT (също CSIRT/CIRC и други)**[34], 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 кибер състоянието си за целите на националния мониторинг и съответно **получават актуалната кибер картина 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**

[34] CERT – Computer Emergency Response Team/Computer Emergency Readiness Team; CSIRT - Computer Security Incident Response Team; CIRC – Computer Incident Response Capability/Center (NATO).

автономно в рамките на своите компетентности, планове и способности. На базата на получаваната обща оценка на ситуацията и на цялостната кибер картина, 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 кибер картина и препоръките по НКОМКС. Наблюдаването на динамиката и развитието на кибер картината в НКОМКС ще се извършва от **екипи за оперативен анализ** (ситуирани в CERT, или специализирани звена), които осигуряват оперативна оценка на тенденциите за развитие на кибер заплахите 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 специализирани комбинирани екипи за реакция** на масирани инциденти от интердисциплинарен характер и хибридни атаки, ангажиране на изследователски лаборатории, специализирани екипи за разследване и разкриване на кибер престъпления, кибер отбрана и активно противодействие на кибер тероризъм 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**“[35]. **Гръбнакът** на НКОМКС се изгражда на базата на организации и центрове, отговорни за кибер сигурността в различни сегменти на кибер пространството (национални, секторни и ведомствени CERT/CSIRT):

- Национален CERT за публични (некласифицирани) мрежи в рамките на ДАЕУ, който е и правителствен CERT (GOV CERT)
- Център за кибер отбрана (Mil CIRC – Computer Incident Response Capability) в МО
- CSIRT за класифицираните мрежи в ДАНС
- CSIRT за наблюдение и защита от деструктивни въздействия на критична инфраструктура и стратегически обекти в ДАНС
- Център за борба и противодействие на кибер престъпността в МВР (ГДБОП)
- Национален център за контра тероризъм в ДАНС
- CERT-ове за различни сектори и подсектори
- 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 държавните CERT-ове, 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 кибер престъпления, секторни и бизнес CERT/CSIRT**.

В **Националния ситуационен център (НСЦ)** се разполага основният национален център за непрекъснат мониторинг на кибер картината в държавата и осигуряване на координирана реакция - **Национален кибер ситуационен център (НКСЦ)**. Той осигурява оперативна оценка на обобщената степен на заплаха на национално ниво, разпространяване на препоръки за

[35] Service Oriented Model/Architecture, Collaboration Networks

превантивни действия и организиране на координирани действия при кибер кризи или непосредствена заплаха от такава. Оперативно-техническите действия се поемат от съответните CERT/CSIRT 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 публично-частно партньорство (ПЧП). .

Принципите за проектиране и развитие на НКОМКС и изискванията към организациите и центровете за мониторинг се определят от Съвета по кибер устойчивост (СКУ) в съответствие с развитието на модела и архитектурата на националната система за кибер сигурност и изискванията за оперативна съвместимост.

Изискванията за обмен на информация, техническа и кибер защита на НКОМКС се осъществяват по разработени за целта правила, протоколи и нива на поверителност, които 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 кибер устойчивост на национално ниво.

Мрежата се изгражда логически и технически на различни слоеве (пръстени) със съответни нива на защита и устойчивост. Части от информацията в съответен вид може да бъде споделяна по допълнителни разширени канали на базата на определени принципи и норми за споделяне на информация в публично-частни общества и организации (визирани в т. 4.4). НКОМКС не замества и не дублира мрежите и каналите за обмен не техническа информация между CERT/CSIRT на национално и международно ниво, а ги надгражда и може да реферира към информацията през тях, със съответните нива на защита, достъп и оперативна съвместимост. Развитието на способности, разпределението на информационните ресурси на НКОМКС като хардуер, софтуер, комуникации и личен състав се извършва съобразно законовоопределените функции по секторни политики на ДАНС, МВР, МО, МТИТС, ДАЕУ. Моделът предвижда НКОМКС да се проектира и реализира поетапно от ДАНС и МО, във взаимодействие с ДАЕУ, МТИТС и МВР. ДАЕУ осигурява технически устойчива преносна среда за функционирането на НКОМКС и администриране на некласифицираната мрежа, както и организацията по присъединяването на бизнес и академични организации и центрове към мрежата. Определянето на протоколите за споделяне на информация и нивата на поверителност в мрежата НКОМКС и изискванията към класифицираната мрежа се извършва от компетентния национален орган ДКСИ, като се използват модели и установени стандарти за взаимодействие и федериране на мрежи с различни нива на защита на НАТО, ЕС, САЩ и др. Взаимодействието между посочените органи се извършва на базата на стандартни оперативни процедури, които се утвърждават от СС на МС.

[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)

4.1.3 *Национален координатор по кибер сигурност*

Националният координатор по кибер сигурността (НККС) се определя от Министър председателя и осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво, като:

- Изпълнява функциите на секретар на Съвета по кибер устойчивост (СКУ) и ръководи изработването и развитието на Национална стратегия за кибер сигурност, плана за реализирането ѝ, организира тяхното прилагане и мониторинга за изпълнението им;
- Направлява изграждането и развитието на мрежата на НКОМКС чрез ефективно публично-частно партньорство и осигуряване на нейната надеждност, сигурност и устойчивост;
- Организира създаването и развитието на Националния кибер ситуационен център (НКСЦ) и осигурява непрекъснато наблюдение и оценка на националната кибер картина, координация на действията и комплексна реакция при заплаха от кибер криза и заплахи от хибриден характер;
- При необходимост, в състояние на повишена заплаха (кибер или от хибриден характер) подпомага сформирането на смесени екипи за анализ, реакция и възстановяване;
- Координира организирането на общи и частични учения в областта на кибер сигурността или от хибриден характер;
- Изпълнява възложените му от Председателя на Съвета по сигурността дейности и задачи и подпомага работата на Секретаря на Съвета по сигурността.

Националният координатор по кибер сигурността изпълнява функциите си с помощта на екипа на НКСЦ в Националния ситуационен център (Секретариата на Съвета по сигурността) и други специализирани звена.

4.1.4 *Национална система за управление при кибер кризи*

Националната система за управление при **кибер кризи** е част от **Националната система за управление при кризи**[40] и включва ангажиране на мрежата НКОМКС с участващите в нея организации, центрове и екипи за реакция, Националния координатор по кибер сигурността (НККС) и експертния капацитет на СКУ. Тя осигурява работата на **Националния ситуационен център** и справянето с кризи и бедствия на национално ниво в два аспекта:

1) За предотвратяване и справяне с **кибер кризи** – непрекъснат мониторинг на националната кибер картина за ранно идентифициране и оценка на степента на заплахи, препоръчване на превантивни действия, ескалиране на предупрежденията и координация за овладяване на кибер кризи;
2) При **общи кризи** или **мащабни заплахи** от хибриден характер (включително бедствия и аварии) - завишен мониторинг на кибер картината във връзка с безпроблемното функциониране на системите, необходими за справянето с тях, и предотвратяване на разширяването им в кибер пространството (във взаимодействие с Единната спасителна система[41] и други специализирани системи за управление при кризи със съответното ниво на защита и устойчивост).

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

[41] Закон за защита при бедствия (2011г), в процес на промяна

Кибер кризите 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 кибер пространството 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 „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 кибер кризи най-често се проявява индиректно чрез сигнали за нарушения в различна степен на функции на съответните комуникационни и информационни системи и оттам – на съответните услуги, дейности, бизнес. Процедурите на най-високо ниво (**деклариране на кибер криза**, ескалиран е, поискване и оказване на помощ, международно взаимодействие), следват установените в Националната система за управление при кризи и съответните планове[42], 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 кибер кризи следват насоките от **Европейските стандартни оперативни процедури (SOP)**[43] за взаимодействие при кибер кризи и модела на **взаимодействие и управление на кризи на НАТО**. От тях произтичат част от **основните стандартни изисквания** към мрежата НКОМКС, което да осигури нейната оперативна съвместимост и отвореност и на международно ниво.

Дейностите за осигуряване на готовност, превенция, откриване, отговор, смекчаването, възстановяването, международното сътрудничество се разработват в **националния план за действие при кибер кризи**[44] и в съответни планове на ниво регион, сектор, организации. Това включва координация и взаимодействие със съответните **ведомствени и регионални ситуационни центрове,** както и определяне на ролите и ангажиране на **компетентните органи по мрежова и информационна сигурност и съответните CERT/CSIRT. Те се** съгласуваност и развиват в синхрон със съответните планове за **защита на националната сигурност и кибер отбрана**. Хибридният характер на заплахите изисква **комплексен подход** при реакцията и защитата, и задължително добавяне на адекватен **кибер фокус във всички планове за управление при кризи**, както и допълнителни способности в съответните организации.

За своевременни превантивни действия при непосредствена заплаха и реакция при кибер кризи ще бъде установен **механизъм на координирания отговор**. Той се базира на разработени **стандартни оперативни процедури** и на способностите в CERT-овете и **специализираните екипи** за бързо реагиране - RRT (Rapid Reaction Team). За посрещане на национални кибер кризи и кризи от хибриден характер се разработва механизъм и способности за сформиране и координация на **национални смесени екипи за бързо реагиране.**

[42] National Contingency plans

[43] SOP – European Standard Operational Procedure for cooperation during cyber crisis; част от European Cyber Crisis Cooperation Framework (ECCCF)

[44] National Cyber Contingency plan

4.1.5 *Повишаване на ролята и отговорностите на държавните структури и на заинтересованите страни*

Изграждането на действаща национална система за кибер сигурност и устойчивост изисква преглед и предефиниране на ролите и отговорностите на правителствените и държавни органи, бизнеса и неправителствените организации, което включва:

- Подобряване на взаимодействието и координацията на най-високо държавно ниво в определяне на **националните политики и приоритети** за сигурност на кибер пространството – народно събрание, правителство, президент, съдебна власт;
- Регламентиране на отговорностите съобразно ролите на собственик, управляващ, стопанин и оператор за съответните сегменти на кибер пространството на **министерства и ведомства**, пряко ангажирани в системата за националната сигурност или отговорни за критични инфраструктури, **операторите на критични инфраструктури** и произтичащите задължения по осигуряване на мрежова и информационна сигурност, надеждност и защита на комуникационните и информационните системи (КИС), създаване на вътрешна организация и технически капацитет за **мониторинг** на състоянието им, регистриране на инциденти, **реакция и възстановяване**;
- Преглед и разпределение на отговорностите и функциите за всички сегменти на кибер пространството на национално ниво и във връзка с международните ни ангажименти и сътрудничество, развитие на регулаторните и насърчителни механизми;
- Подготовка и **включване в националната система за кибер сигурност** и управление на споделения (кибер) риск на всички организации и заинтересовани лица (държавни, бизнес, 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.

4.2 Мрежовата и информационна сигурност – фундамент на кибер устойчивостта

Цели:

Мрежовата и информационна сигурност (МИС) е един от трите основополагащи стълба на кибер сигурността съгласно Европейската стратегия за кибер сигурност, заедно с другите два - правоприлагане и кибер отбрана. Основната цел е постигането на **високо общо ниво на МИС във всички сегменти на киберпространството**, повишаване на сигурността на националните и на частните мрежи и информационни системи, и постигането на информационна сигурност на всички нива – граждани, фирми, държавни и бизнес организации, доставчици и потребители на услуги. В условията на нарастваща и необратима дигитална зависимост, дефицитите в МИС водят до компрометиране на основни услуги, спиране на дейности, загуби.

Постигането на МИС осигурява фундамента, техническата и организационна база за изграждане и непрекъснато развитие на общата кибер сигурност и постигане на кибер

Програма на ЕС в областта на цифровите технологии

*Европейската стратегия за киберсигурността и предложението за директива подкрепят програмата в областта на **цифровите технологии за Европа**, чиято цел е европейските **граждани и предприятия да се възползват максимално от тези технологии.***

устойчивост (съгласно общата схема на Фигура 1).

Мерки:

4.2.1 *Постигане на високо общо ниво на мрежова и информационна сигурност*

В съответствие с препоръките за прилагане на Стратегията за кибер сигурност на ЕС и на директивата на Европейския парламент относно повишаване на сигурността на мрежите и информационните системи[45], и за осигуряване на високо общо ниво на МИС във всички сегменти на кибер пространството, следва да бъдат предприети следните систематични мерки:

- Развитие на **стратегия, политики и** конкретни мерки за и съответните регулаторни механизми за постигане на високо равнище на МИС, развитие на плановете за взаимодействие в съответствие с общите изисквания за МИС в ЕС и НАТО;
- Установяване на национални и специализирани **компетентни органи** и развитието им по предложение на СКУ, като на настоящия етап те включват следните компетентни органи:
    - МИС в публични информационни и комуникационни системи и мрежи, потребители и доставчици на обществени услуги – Държавна агенция „Електронно управление“ (ДАЕУ);
    - МИС в класифицирани информационни и комуникационни системи и мрежи и за информационните и комуникационни системи и мрежи на стратегическите обекти и дейности, посочени в регламентиращите документи – Държавна агенция за национална сигурност (ДАНС);
    - В областта на кибер престъпността и правоприлагането – Министерство на вътрешните работи (МВР);
    - В сферата на кибер отбраната (национална отбрана, въоръжени сили) – Министерство на отбраната (МО);
    - В сферата на защита на личните данни – Комисия за защита на личните данни (КЗЛД).
- Определяне на **национална точка за контакт за МИС** за общо взаимодействие в ЕС, включително и за трансгранично взаимодействие[46], и осигуряване на механизъм за координация и взаимодействие с националните органи и съответните **контактни точки в областта на противодействие на кибер престъпността и на отбраната** на базата на националната мрежа НКОМКС;
- Ускорено развитие на капацитета и създаване на нови **центрове за реакция на инциденти** (CERT/CSIRT) в областта на МИС на **национално, секторно, ведомствено или друго целесъобразно ниво**, с технически и организационен капацитет за предотвратяване, реакция и ограничаване на въздействието на инциденти и рискове в областта на МИС, по модела и препоръките на ЕС, НАТО, ITU и др. В допълнение на националните CERT/CSIRT (образуващи гръбнака на националната система и мрежата за кибер сигурност НКОМКС, посочени в т. 4.1), да бъдат създадени и развити секторни и ведомствени CERT/CSIRT, със съответни екипи за бързо реагиране (RRT);
- Доколкото инцидентите в областта на МИС от различен мащаб са свързани с **престъпни действия** (или бездействие), е необходим **ефективен механизъм на взаимодействие с правоприлагащите органи** (визирани в раздел 4.6) още на ранен етап и признаци –

[45] „Директива на ЕП и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза“ , 06.07.2016г.

[46] CERT в ДАЕУ, за некласифицирани мрежи и данни

активно включване в националната координационна мрежа НКОМКС и съдействие за ефикасна и комплексна реакция, но и за осигуряване на нужния доказателствен материал за идентифициране на източниците и съответно правоприлагане, както и за целите на анализ и подобряване на превантивните действия;

- Провеждане на **национална програма за „кибер хигиена“** по МИС във всички сфери и във връзка с взаимодействието държава-бизнес-общество (в т. 4.5) - с помощта на мрежата от CERT/CSIRT, екипите за реакция, ИТ и техническите екипи, всички организации, публични и частни, да разработят и въведат като част от вътрешните си политики ефективни действия (правила, обучения, демонстрации и др.) за повишаване на информационната сигурност и изискванията за КИН (конфиденциалност, интегритет, наличност - ядрото на схемата от Фигура 1), като работа с компютър, интернет, системни приложения, мерки за защита и предпазване от изтичане на информация, употреба на електронната идентичност, средства за автентикация, персонална и колективна защита.
- Като основна линия от кибер хигиената да бъдат предприети мерки и стимули за използване на официално придобити, **лицензирани и поддържани от производителите софтуерни и хардуерни системи** във всички групи публични и частни организации, и за крайните потребители;
- Да бъдат набелязани специфични мерки и повишаване на взаимодействието с органите за **защита на личните данни** във връзка с компрометиране на лични данни в следствие на кибер инциденти, атаки или безстопанственост, включително за извършване на правни и регулаторни промени, дефиниране на прагове и действия за **докладване при масово изтичане на лични данни от публични и частни организации**, и съгласуваност за своевременно определяне на съответни **отговорности и мерки за предотвратяване**;

4.2.2 *Сигурност и устойчивост на комуникационните и информационни системи на държавните институции, администрация и електронното управление*

- Установеният постоянно действащ **консултативен орган** – Съвет за мрежова и информационна сигурност на информационните системи на административните органи, да конкретизира политики и дейности по дефиниране и привеждане в практиката на **минимални изисквания по отношение на МИС** в публичните комуникационни и информационни системи и доставчиците на обществени услуги, и прилагане на международни стандарти в областта на информационната сигурност и кибер устойчивост;
- Осигуряване на капацитет, техническа и организационна помощ за постигането на минималните изисквания за МИС от страна на **Правителствения CERT** и осигуряване на **постоянна поддръжка (24/7)**, извършване на съответни периодични одити, както и периодичен контрол на състоянието от страна на специализираните звена за национална сигурност (ДАНС);
- Реализиране на програма за обективен преглед (одит, „инвентаризация“) на всички информационни активи, ресурси и средства по единна методика и съобразно установени международни стандарти и въвеждането им в единен регистър на информационните ресурси към ДАЕУ, въвеждане на правила и мерки за **„санитаризиране“ и завишена кибер хигиена**, оптимизиране на комуникационните и информационни системи, архитектурата на свързаност и достъпността от интернет, начален одит и периодични проверки и осъвременяване (включително и на **средствата и методите за кибер защита**);
- Реализиране на стандартизиран пакет от мерки за **сигурността и достъпността на уеб сайтовете и уеб-базирани системи и услуги** на правителството и държавната администрация – задължително използване на сървърни сертификати за сигурен комуникационен канал (HTTPS-only, с поддържано съответно стандартизирано ниво на

сигурност), национален доверен удостоверител на сървърни сертификати, развитие на системата за удостоверяване на домейн имената за крайни потребители (DNSSEC)[47], и постоянното им развитие и обновяване съобразно препоръките на международните интернет организации;

- Въвеждане на **адекватни завишени изисквания** за кибер сигурност към **системите и мрежите за електронното управление**[48] и надеждно осигуряване на КИН (конфиденциалност, интегритет, наличност) за информация и документи във ведомствените мрежи, както по мрежата за оперативна съвместимост, с граждани и фирми. Поетапно и системно въвеждане на **принципите и изискванията за устойчивост към развитието на системите и при дизайна на нови такива,** включително и при проектиране на нови технологични платформи (като „облачните“); прилагане на модела „дизайн за сигурност“, включително чрез разработване на **софтуер с отворен код** и прилагане на правила за добросъвестно докладване на проблеми със сигурността;
- Въвеждане на **единна система и унифицирани критерии за оценка на кибер рисковете** по цялата верига на оперативната обвързаност, и преглед на цялостната архитектура и изисквания за оперативна съвместимост на системите и услугите от гледна точка на тяхната кибер защита и устойчивост, непрекъснато подобряване на изискванията за осигуряване **на еднакво ниво на кибер сигурност и устойчивост** при декларираното равнопоставено използване в системата на електронното управление на „класически“, „виртуализирани“, „облачни“, „мобилни“ и други нови технологии[49];
- Въвеждане на комплекс от мерки за гарантиране и непрекъснато подобряване на сигурността и надеждността на **електронната идентичност на гражданите**, като основен фактор за успешно развитие на електронното управление и в съответствие с приоритетите на развитие на „Цифрова България“ [50]. Осигуряване на защитено и оптимизирано съвместяване на електронна идентичност (eID) с други компоненти като квалифициран електронен подпис (КЕП), криптирано и защитено съхраняване на здравна и друга чувствителна информация, както и съответни изисквания към базираните на тях услуги, пълна и неподменима отчетност на достъпа до лична информация, повишаване на културата за използването им от всички заинтересовани – държава, граждани, бизнес, доставчици на услуги;
- Подготовка (техническа, законодателна, организационна, обучителна) за въвеждане на **електронно гласуване и упражняване на електронна демокрация** от гражданите, с постигане на ниво на защита и сигурност еквивалентно или по-високо от установените „класически“ форми;
- Съвместно с **доставчиците на интернет достъп и услуги за държавни институции** да бъде определен и въведен комплекс от мерки за повишаване на сигурността и защитата при операторите, определяне на **минимални и препоръчителни изисквания** за сигурност и устойчивост, ангажименти за идентифициране и защита при кибер атаки, предпазване от съвременните упорити заплахи (APT – като DDoS и др. [51]), отговорности за изпълнение на плановете за кибер отбрана, както и координирано и пълноценно включване в националната мрежа НКОМКС.

4.2.3 *Ангажиране на частния сектор в подобряване на МИС*

[47] DNSSEC – DNS Secure Extensions, препоръки на ICANN (2015)
[48] Съгласувано със Закона за електронно управление (последно изменение и допълнение, 01.07.2016г)
[49] Стратегия за развитие на електронното управление в Република България 2014 – 2020 г.
[50] Актуализирана национална програма Цифрова България (2016 – 2020)
[51] Advanced Persistent Threats (APT), Distributed Denial of Service (DDoS)

Преобладаващата част от мрежовите и информационните системи са частна собственост или се управляват и експлоатират от частния сектор. България е на едно от лидерските места в Европа и света по осигуряване на **широколентов достъп** за граждани и бизнес, 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 сигурни и надеждни интернет базирани услуги. Комплексът от общи действия включва, но не се ограничава и апелира за инициативи от бизнеса и неправителствените организации:

- Разработване на **собствен технически и организационен капацитет от доставчиците на интернет и услуги** за запазване на устойчивостта на киберпространството, за оценка на рисковете, и мерки за гарантиране на МИС, съответно на съществуващите рискове с оглед на последните постижения в тази сфера, гарантиране на непрекъснатост и надеждност на услугите;
- Ангажиране на **интернет доставчиците** за ефикасното реализиране на национални проекти за „**кибер хигиена**“ в интернет пространството и реализиране на сигурни и надеждни комуникационни канали, идентификация на домейни и достоверност на информацията по цялата комуникационна верига и други съответни на препоръките на международните организации (като проектите за сигурна интернет връзка и проверка на домейни: HTTPS-only и DNSSEC, визирани в раздел 4.2.2);
- Организиране на съвместна кампания на публични и частни доставчици на интернет-базирани услуги за въвеждане и публикуване на политиките и мерките за осигуряване на МИС, кибер защита и непрекъснатост на услугите като съществен елемент от **конкурентните предимства**, **прозрачността, балансиране на регулаторните механизми и пазарните принципи** за постигане на сигурно и надеждно пространство за крайните интернет потребители (граждани и фирми);
- **Ускоряване на трансфера и възприемане в публичния сектор** на добрите практики 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.

4.2.4 *Преход от кибер сигурност към кибер устойчивост*

- Изграждането на CERT-ове и екипи за реакция на инциденти в обектите и сегментите на кибер пространството, свързани с **критични инфраструктури е обща отговорност** на собствениците, стопаните и операторите, като ангажимент на държавата е да създаде и актуализира съответната регулаторна рамка, и подпомогне включването им в националната мрежа НКОМКС (на секторен, клъстерен или друг принцип, в съответствие в механизмите за споделяне на информация и взаимодействие, описани в т. 4.4), а техническите и организационни мерки трябва да гарантират ниво на сигурност, съответстващо на **оценката на рисковете** и за постигане на **непрекъсваемост на услугите**;
- **Развитие на минималния необходим капацитет** на отделните CERT/CSIRT за включване в националната система за кибер сигурност, определен от правилата на националната мрежа НКОМКС. Разширяване на обхвата, способностите и функциите им в посока **Оперативен център за сигурност (SOC, Security Operations Center)**[52] включително и за

[52] В допълнение на дейностите по реакция на инциденти и атаки, центровете SOC покриват всички аспекти на сигурността, като повишаване на осведомеността, устойчивост, откриване, оповестяване, докладване и управление на кризи

изготвяне и споделяне на **обобщена информация за националната кибер картина**, и способности за участие в **общата координирана реакция**;

- Поетапно въвеждане на **максимални срокове за докладване и максимално време за реакция** при кибер инциденти на различните нива (в съответните CERT/CSIRT, и обобщено към националната кибер картина) в зависимост от техния характер, интензивност, реално и прогнозирано въздействие[53], и осигурени съответните способности и средства приоритетно в публичния сектор, и чрез механизма на регулация и саморегулация в частния сектор. Развитие на способностите и за осигуряване на **максимални срокове за възстановяване на нормалното функциониране на системите.** Всички срокове, максимални времена и механизми за тяхното въвеждане следва да се определят в **публично-частен диалог** и да посрещат своевременно предписанията, но **да не се ограничават** само до изпълнението на Директивите на ЕС или други регламентиращи документи, а да следват и дори изпреварват бизнес тенденциите, потребностите и съответните рискове;
- Повишаване капацитета, способностите и отговорностите на мрежата от CERT-ове (държавни, секторни, публично-частни, академични и др.) за **покриване на всички сегменти на кибер пространството** и осигуряване на помощ и реакция при инциденти за всички участници (граждани и фирми, малък и среден бизнес, администрация), създаване на **национална асоциация на CERT/CSIRT**, която да организира и стимулира развитието им, разширяването и международното сътрудничество, ефективното оперативно взаимодействие през мрежата НКОМКС и по модела на ПЧП.

4.3 Защита и устойчивост на дигитално зависимите критични инфраструктури

Цели:

Главна цел: Подобряване на защитата и устойчивостта на комуникационните и информационни системи и системите за управление на критичните инфраструктури за да се гарантира, че основните функции ще бъдат надеждно и безпроблемно осъществявани.

Особено важен проблем възниква от все по-голямата обвързаност на информационните и комуникационните системи със секторите и системите от критичната инфраструктура, като **енергетика, транспорт, финанси, здравеопазване, телекомуникации, снабдяване с храни и вода, отбрана и редица други**[54]. Повечето от тези **зависещи и основаващи се на специализирани ИКТ системи, услуги, мрежи и инфраструктури** формират жизнено важна част от икономиката и обществото като или предоставят съществени продукти и услуги, или представляват основната платформа за други **критични инфраструктури (КИ)** и в крайна сметка ни позволяват упражняване на правата и свободите ни като граждани. Тези ИТ системи (или още КИС – комуникационни и информационни системи) се определят още като **критични комуникационно-информационни инфраструктури (ККИИ)**, тъй като тяхното разстройване или разрушаване може да доведе до срив в държавата и обществото и нарушаване на тяхното нормално функциониране. При неблагоприятни въздействия (кибер атаки, човешки грешки, технически дефекти и други) срещу тези системи непредвидените негативни последствия и възможните каскадни ефекти за другите сектори и обществото като цяло могат да бъдат многократно по-големи в количествено и качествено изражение от ползите, за чието създаване те са проектирани и създадени.

Мерки:

[53] С цел достигане до 24ч за инциденти от общ характер, и на 2-4 часа за признаци за кибер атаки или непосредствена заплаха от такива, и развитие за мониторинг в реално време

[54] Списък със секторите на критичната инфраструктура в България съгласно ПМС № 256 от 17.10.2012 г.

4.3.1 *Подобряване на взаимодействието между държавата и операторите на критични инфраструктури*

- Разпределение на ангажиментите и засилване на сътрудничеството на държавата с операторите на критични комуникационни и информационни инфраструктури (ККИИ) и критични инфраструктури (КИ), които в немалка част са частна собственост, прилагане на инструмента на ефективно и действащо публично-частното партньорство (ПЧП);
- Включване на операторите на критичните инфраструктури в процесите на националното управление при кибер криза, в определянето и изграждането на цялостната архитектура на сигурността, и изграждане на собствена адекватна такава за управление на риска и при кризи, да ги актуализират непрекъснато и определят вътрешни отговорници и органи по сигурността;
- На основата на партньорство и взаимно разбиране на отговорностите, за операторите на КИ и ККИИ трябва да се определят и внедрят **общи и специфични стандарти за кибер сигурност**, които да бъдат разширени впоследствие и в посока **кибер устойчивост**, и покриване на целия жизнен цикъл за **управление на кибер рисковете** и реализиране на целия комплекс от дейности по идентифициране на организационната структура и активи, тяхната защита, забелязване на инциденти, реакция, възстановяване и съответни поуки и подобряване[55];
- Оперативните процедурите и средствата за **комуникация и координацията при кризи** следва да бъдат развити и институционализирани, а субординацията за решенията нормативно установена, включително и по отношение на задълженията и сроковете за докладване на тежки инциденти, оценка на въздействието, искане и приемане на помощ за реакция, като съответните правни аспекти бъдат определени взаимно с всички заинтересовани страни, както и в съответствие с изискванията за съвместимост и взаимодействие в международните партньорски организации и мрежи;
- **Споразуменията между държавата и операторите** на критичните инфраструктури следва регулярно да се преглеждат по отношение на развитието на предизвикателствата в кибер пространството и да се актуализират и променят своевременно, което включва и плановете за действие при кризи и тяхната кибер защита;
- Да се реализира национална програма и инициират проекти в допълнение към програмите за развитие на отделните сектори за изграждане на **необходимия капацитет и покриване на изискванията за включване на** операторите на КИ и ККИИ към националната система за киберсигурност и мрежата НКОМКС, което изисква създаването на **секторни, отраслови, или клъстерни центрове и екипи за реакция** (CERT/CSIRT) съгласно описания модел в т. 4.1;
- Развитие на програма и стимули за създаване на секторни или клъстерни организации за **споделяне на информация** и повишаване на **колективната кибер сигурност** в областта на критичните инфраструктури (ISAC, т. 4.4) – приоритетни сектори за Фаза 1 и 2 - **енергетика, транспорт, финанси, здравеопазване, телекомуникации и интернет доставчици**.

4.3.2 *Развитие и модернизация на системите за управление и защита на критични инфраструктури*

[55] 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

- Приоритетно **модернизиране на процесите, технологиите и системите** и подобряване на защитата и сигурността на системите за управление от типа ICS/SCADA[56], адекватни на съвременните изисквания за кибер сигурност и устойчивост, в съответствие с **международно признати стандарти** и модели, съответен одит и сертификация[57];
- 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 – те представляват особено уязвима и лесна цел за злонамерени действия, дефекти и опасна нестабилност;
- Изграждането на капацитет и способности за **реакция на кибер инциденти** трябва планирано да се развие до комплекс от мерки за постигане на **кибер устойчивост** на КИ и ККИИ на базата на определяне и прилагане на изисквания за „**дизайн за устойчивост**“[58] и непрекъснато подобряване на процесите и системите.

4.3.3 *Своевременна защита на новите области на кибер пространство*

Бързото и широкото навлизане на цифровите технологии в ежедневния живот и бизнес предопределят и **непрекъснатото разширение на оценката за „критичност“ на комуникационните и информационни системи в съответствие с нарастващата дигитална 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[59]**, **онлайн медии**, и др.
- Особено отговорно е бързото и необратимо разширение в дигиталното пространство на сферата на **финансовите и банкови услуги, е-разплащанията и дигиталните валути, сферата на електронно здравеопазване и осигуряване**, и други. Независимо от това, дали тези области са формално причислени към списъците за критични инфраструктури (и във връзка с реализацията и развитието на Европейската директива за МИС), тяхното бързо развитие и навлизане в живота на граждани и фирми изисква **своевременната интеграция в националната система за кибер сигурност** и обхващането им от изискванията и механизмите за координация за кибер сигурност и устойчивост. Прилагането ма мерките е на базата на баланс на механизма на регулация и саморегулация и **добавяне на кибер сигурността и устойчивостта към изискванията и предимствата в конкурентната бизнес среда** .

4.4 Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество

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 - изисква идентифициране на интересите и

[56] Industrial Control Systems – ICS, Supervisory Control and Data Acquisition – SCADA и други
[57] Като ISO/IEC BS 25999 и ISO 22301; ITIL и ISO 20000; CERT-RMM и др
[58] Resilience by design, Resilient architectures (CERT-RMM, Resilience Management Model, Carnegie Mellon)
[59] App-store и др.

очакванията в краткосрочен и дългосрочен план, разпределение на отговорностите и ангажиментите.

Бързото навлизане и използване на цифровите технологии и интернет е силно конкурентно предимство и стратегия за развитие на съответните организации, бизнес и групи от обществото, но **грижата за надеждността и сигурността на кибер пространството е обща и изисква споделяне на информация, изграждане на съвместен капацитет, повишаване на общото разбиране и „култура“ за кибер сигурност и стремеж към кибер устойчивост, както и съвместното развитие на сигурна, надеждна и атрактивна кибер среда за развитие на конкурентна икономика и общество**.

Мерки:

4.4.1 *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 оценяване 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 кибер сигурност и устойчивост** – от съдействие за набелязване на мерки за изпълнение на поставените цели, през участие в проекти за развитие на капацитет и способности и до пълно включване с поемане на отговорности, участие в публично-частни партньорства (ПЧП);
- Стимулиране и подпомагане на създаването на адекватни групови и **колективни платформи за споделяне на информация и колективен отговор** - на базата на секторен подход (за отделни сектори и подсектори – като енергетика, транспорт, финанси), на клъстерен принцип – бизнес и териториални връзки и зависимости, вериги за доставки и по-общите – за създаване на стойност, и развитие на съответни пакети и стимули за всички заинтересовани страни;
- Адаптиране, развитие и прилагане на форми и методи за институционализация (публични, частни и публично-частни партньорства) - създаване на секторни и клъстерни центрове и организации за споделяне на информацията и анализ (на базата на опита на САЩ и държавите от ЕС – различните модели на ISAC и ISAO[60]) 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 центрове за реакция (секторни, клъстерни и специализирани CERT/CSIRT) по общия модел за развитие на националната система и мрежа за кибер сигурност и устойчивост (описан в 4.1);
- Развитие на методите и средствата за изграждане на **доверие за обмен на информация** използване на протоколи и правила, съгласно утвърдени международни и национални

[60] САЩ, Кралство Нидерландия и др: ISAC – Information Sharing and Analysis Centers, ISAO – Information Sharing and Analysis Organizations

стандарти и модели за постигане на доброволно, но силно ангажирано и отговорно участие[61].

- Разработване на национална класификация и общ „език“ за споделяне на чувствителна информация, хармонизирана с международните норми и практики, националното законодателство и развитието на обхвата за всички аспекти на кибер пространството – заплахи, инциденти, реакция и превантивни мерки, оценка на риска и нива на готовност, еквивалентни нива на чувствителност на информацията (национален и международен аспект, държавни класифицирани и частни мрежи и организации). Съгласуване на изисквания към информационни канали, източници на информация и отговорности, които да стимулират включването на публични и частни организации в националната мрежа НКОМКС и ангажираност на оперативно и техническо ниво за справяне с инциденти и кризи; [62]
- Дефиниране и изпълнение на общ пакет от мерки за гарантиране на сигурността и **надеждността на информационните канали**, в съответствие с мерките за повишаване на мрежовата и информационна сигурност (раздел 4.2) – 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 кибер сигурност** като основен механизъм на взаимодействие и ангажираност държава-бизнес-общество и за изграждане и разширяване на Националната координационно-организационна мрежа (НКОМКС);
- Активно взаимодействие и включване в Европейската инициатива за договорно „Публично-частно партньорство за кибер сигурност“[63], развитие на „Единен цифров пазар“[64] и мрежите и програмите на НАТО[65] – 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.

4.4.2 *Развитие на индустриален технологичен капацитет и споделени способности*

- Развитие и разширяване на обхвата на програми за **технологично развитие на индустрията, модернизация и интелигентна специализация**[66] в областта дигитализираната икономика и услуги – стимулиране на развитието на системи с дизайн за сигурност и устойчивост и решения гарантиращи адекватни нива на кибер сигурност и защита, изграждане и развитие на съответния **индустриален, фирмен и професионален капацитет**;

[61] Стратегия за кибер сигурност на Кралство Нидерландия - “Voluntary, but not without engagement” (Netherlands)

[62] Като нивата за ограничено споделяна на ISAC/ISAO на базата на „светофар“ (TLP), и кодовете за нива на заплаха „зелен-жълт-оранжев-червен“ (време, бедствия) – широко използвани в национални и международни мрежи

[63] European cPPP – Contractual Public-Private-Partnership for Cybersecurity (2016) – ECSO: European Cyber Security Organisation

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

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

[66] 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

- Приоритетно развитие на съвместни инициативи, програми и проекти в новите области на цифровата икономика и дигитално зависимото общество (сигурност на облачните платформи и услуги, мобилни и умни устройства, интернет свързани устройства, и съответни приложения) – използване на механизмите за публично-частни партньорства, Европейски и международни 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, 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 сигурността, симулационни среди за проверка и повишаване устойчивостта към атаки и пробиви и решаване на задачи и предизвикателства дефинирани от бизнеса и държавата;
- Създаване на ефективен **механизъм за споделяне на ресурси, капацитет и способности** между частния, публичен и академичен 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 програмите за интелигентен растеж и развитие;
- Мерки за стимулиране на големите софтуерни, ИКТ компании и мултинационални технологични компании в България за развитие на професионални компетентности и капацитет, ускорено реализиране на механизъм за споделяне и включването им в развитието на националната система за кибер сигурност като основен фактор и съвременни средства и ресурс на световно ниво, включително и за повишаване на общата сигурност на интернет пространството в България, подкрепа за малкия и среден бизнес и интернет обществото, национални и международни центрове за компетентност.

4.4.3 *Фокус върху малкия и среден бизнес*

- Иницииране на фокусирани програми и добавяне на основни мерки към програмите за развитие на **конкурентоспособността на малкия и среден бизнес, включително и микро - предприятията,** за повишаване на осведомеността и „кибер културата“, със специфични пакети от препоръки и изисквания за **включване в единния цифров пазар** (на национално и международно ниво), осъзнаване на цифровата зависимост от каналите за информация, управление на доставките, комуникационните и информационни системи, внедряване на базови или адаптирани за МСП стандарти за информационна и кибер сигурност;
- Развитие на механизмите за насърчаване и организирано **включване в мрежите за споделяне на информация и превенция** на базата на секторен или клъстерен подход, и осъзнато споделяне на **кибер рисковете по веригите за доставка** и целия поток на взаимосвързан цифровизиран бизнес и пазари;
- Дефиниране и прилагане на адаптиран подход за стимулиране на саморегулация и инициативността, и културата на „**дигиталните лидери**“ – развитие на кибер-компонента в бизнес отношенията и комуникации 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 кибер аспектите) , „малки за големи“ (малките фирми участват преобладаващо във вериги за доставки и допринасят за общата кибер сигурност, или за „несигурността“) – активно ангажиране на бизнес и ИКТ асоциациите, приоритетно подпомагане от държавните институции, национални и международни програми;

- Организиране на специфични секторни и между-секторни **упражнения, симулации и учения** с цел повишаване на ангажираността на малкия и среден бизнес, и включването им в обхвата на национални и международни такива.

4.4.4 *Установяване на обща комуникационна стратегия за информираност относно кибер въздействия и противодействия*

- Във взаимодействие с всички заинтересовани страни да бъде разработена **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 кибер пространството да установят съответни вътрешни комуникационни политики, процедури и механизми, които осигуряват своевременна осведоменост на ръководството за заплахи за кибер сигурността и състоянието на поверените им системи и ресурси, оценка в контекста на националната кибер картина (поддържана от националната мрежа НКОМКС), както и своевременно съгласуване на управленско ниво и чрез платформите за споделяне на информация (в точка 4.4.1) за осигуряване на своевременна информираност на обществеността чрез медии, социални мрежи и други канали.

4.4.5 *Сигурна, свободна и надеждна интернет среда*

- Компетентните държавни институции в широко взаимодействие с неправителствените организации[67] и на базата на препоръките на световните интернет организации да продължат да развиват управлението и стопанисването на дейностите свързани с управление и достъпността на граждани и бизнес до интернет свързаност и информация, като развиват ефективен регулаторен и само-регулаторен механизъм за гарантиране на баланса между достъпност и надеждност, сигурност и поверителност, защита на личните данни и чувствителна информация и дейностите в интерес на националната и колективна сигурност - особено внимание следва да се обърне на запазването на неформалните и 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 и изпреварващо развитие и **прилагане на препоръките на международните интернет институции и организации** – демократичното развитие и управлението на интернет пространството да нареди Република България измежду първите държави в света с пълно изградена инфраструктура за **сигурна криптирана комуникация и валидация на интернет домейните** (като инициативите „https-only” и DNSSEC);

[67] Интернет общество, ИКТ и софтуерни асоциации, интернет доставчици и доставчици на електронни услуги, бизнес и работодателски организации

- Въвеждане на мерки за осигуряване на **надеждност, достъпност и сигурност на отворените данни (open data)** – прилагане на специфични изисквания и стандарти към доставчиците (публични и частни) и базираните на отворени данни системи и услуги[68].

4.5 Развитие и подобряване на регулаторната рамка

Цели:

Спецификата и динамиката на развитие на обществото и пренасяне на основни дейности в киберпространството изискват **адекватна, модерна и адаптивна правна и регулаторна рамка** за определяне на роли и отговорности на участниците в кибер пространството, която да 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. Хармонизация с нормативната база на международните организации и партньорства за пълноценно развитие на колективната кибер защита и изпълнение на поетите ангажименти (към ЕС, НАТО и други двустранни, регионални и международни споразумения).

Мерки:

4.5.1 *Осъвременяване на правната и регулаторна рамка*

- По инициатива на Съвета по сигурността при МС и под ръководството на националния Съвет за кибер устойчивост да се извърши общ преглед и обобщи състоянието на правната и нормативна база, дейности и инициативи в процес на изпълнение, идентифицираните пропуски, поетите ангажименти с включване на всички заинтересовани страни за развитие на **адекватна правна основа, регулаторни мерки и механизми за само-регулация** – регламентиране на дейностите, задачите и отговорностите на различните организационни структури в съответствие с модела за функциониране на национална система за кибер сигурност и принципите на споделена отговорност и координиран отговор, механизмите за споделяне на информация и взаимодействието на публичния и частния сектор, публична отчетност и отговорност във връзка със изпълнение на задължения и предприемане на мерки за кибер защита, третиране на всички звена от веригите на свързаност и създаване на добавена стойност в цифровата икономика и общество;
- Хармонизиране на **националното законодателство и нормативна база спрямо това на евро-атлантическите партньори** с оглед тенденциите в развитие на заплахите, злоумишлените и престъпни действия и регламентиране на съвместни действия за превенция, противодействие и правоприлагане[69];
- Преглед и осъвременяване на правната рамка и санкциите свързани с различни видове и категории на зловредни действия или бездействие в кибер пространството спрямо всички субекти, гарантиране на **адекватна наказуемост и мерки за превантивно въздействие**;

[68] Във връзка с прилагането на Директива 2013/37/ЕС на Европейския парламент и на Съвета от 26.06. 2013 относно повторната употреба на информацията в обществения сектор и Решение № 103/2015г. на МС за Списък с набори от данни по приоритетни области, които да се публикуват в отворен формат

[69] Директива 2013/40 на Европейския парламент и на Съвета относно атаките срещу информационните Системи - предприемането на подходящи мерки за по-ефективната им защита от кибер атаки, да се подобри сътрудничеството между компетентните правоприлагащи и съдебни органи в Съюза, да се зачитат правата на човека и основните свободи на гражданите

- Законодателно подсигуряване на своевременното **разследване на кибер престъпления**, съобразно тяхната специфика и проявление като самостоятелни или като елемент от хибридни въздействия, и координирани мерки за **ранно идентифициране, откриване на източниците и превантивни мерки**;
- Съобразно високата степен на обществена значимост и заплаха за сигурността на обществото и държавата, актуализиране и завишаване на санкциите за престъпни деяния спрямо критичната комуникационна и информационна инфраструктура, управление на критични инфраструктури и въздействия в кибер пространството с последствия от голям мащаб;
- Използване на международния опит и методики по прилагане на международното право в областта на кибер сигурността и кибер отбраната[70];
- Осигуряване на баланс между мерките във връзка със сигурността на кибер пространството и националната сигурност и защитата на персоналните данни и неприкосновеността на личното пространство на граждани и бизнес – действията и мерките да се съгласуват след осигуряване на общо разбиране и обществена подкрепа, и като важен елемент от повишаване на общата кибер култура и споделена отговорност;
- Извършване на периодичен преглед и предприемане на изпреварващи мерки и действия във връзка с динамиката на развитие на дейностите в кибер пространството;
- Установяване на правна и нормативна база за развитие на ефективни публично-частни партньорства (ПЧП) в областта на кибер сигурността и отбраната за осигуряване на пълноценно включване на държавни и бизнес организации за изграждане на националната мрежа за кибер сигурност (НКОМКС) със съответните механизми за споделяне на информация и отговорности, включително и за регламентиране на времена за докладване, реакция и съответни санкции;

4.5.2 *Установяване на ефективен механизъм на регулация, саморегулация и сертификация*

- При развитие на правната и нормативна база да се следва принципа на адекватност на мерките спрямо ефекта от въздействията и рисковете, както и съответствие с възможностите, мащаба и обхвата на различните категории организации (публични, бизнес, обществени);
- Прилагане на комплексен и цялостен подход за развитие на съответните мерки и регулаторни механизми, както и допълване на действащите такива в посока кибер сигурност и устойчивост - реализиране на балансиран подход между режима на регулация и саморегулация, чрез информирано приемане на предоставените възможности и рискове от всички участници в процесите и съответно на трите основни категории съобразно отчитане на масовостта и обхвата на възможни негативни въздействия:
  - **задължителни** нормативи (закони, наредби), стандарти – приложим за мрежи и системи на държавното управление, критични инфраструктури, критични комуникационни и информационни структури, държавно регулирани сектори и ресурси;
  - комбиниран **задължителни/доброволни** - секторни регламенти и приети стандарти, бизнес и услуги с големи мащаби и ефект върху големи групи и категории граждани и възникващите нови цифрови екосистеми и бизнес вериги;

[70] Център на НАТО по кибер отбраната – CCDCOE, в гр. Талин, Естония

- **доброволни** и на базата на осведоменост, неформални правила и препоръки, кибер култура - малък и среден бизнес, частични мерки за **саморегулация** по веригите на доставки, и прилагане на разумен баланс между насърчителни мерки и санкции;

- Дефиниране на специфични регламентиращи и нормативни пакети за основните участници от страна на индустрията и бизнеса в националната система за кибер сигурност и координиращата мрежа НКОМКС – доставчици на интернет свързаност и услуги, оператори на критични комуникационни и информационни инфраструктури (съобразно мерките в т. 4.2.4);
- На базата на дискусия с всички заинтересовани страни, определяне на групи от стандарти, установени международни модели, практики и методики за унифицирана оценка на категориите рискове, нивата на заплахи и степен на въздействие при инциденти, нивото на дигитална зависимост и критичност за бизнес процесите и прилагането им за **определяне на минимални изисквания** за различните комуникационните и информационни системи и електронни услуги, както и съгласуване на доброволни и само-регулиращи мерки като основно конкурентно предимство в цифровото общество и икономика;
- Стимулиране на развитието и прилагането на адекватни схеми за **оценка (одит), сертификация и акредитация** на организации, способности и системи:
  - на ниво организации (публични и частни) и специалисти – на базата на установени и международно признати стандарти, модели на зрялост и ръководства за прилагане[71]; модели на компетентности и оценка на професионална квалификация;
  - на ниво сектори и национална система за сигурност – приети специфични стандарти и утвърдени изисквания за оперативна съвместимост и за включване в НКОМКС, други утвърдени или доброволно приети на принципа на саморегулация;
  - международно ниво – в съответствие с изискванията и стандартите, сертификация и акредитация за взаимодействие със системите на ЕС, НАТО и други партньорски организации и държави.

4.6 Засилване на противодействието на кибер престъпността

Цели:

Цел 1: Установяване на ефективен и ефикасен процес по **превенция и защита, реакция, разследване и адекватно правоприлагане**

Цел 2: Повишаване на **организационна база и способностите на органите** за разкриване, разследване и санкциониране на престъпни дейности в кибер пространството, и установяване на **ефективно взаимодействие с всички заинтересовани страни** (публични и частни) от националната система за кибер сигурност.

Правоприлагането и борбата с кибер престъпността е **вторият основополагащ стълб** на кибер сигурността съгласно Европейската стратегия за кибер сигурност. Икономическите, материални и морални щети, произтичащи от кибер престъпни и злонамерени действия намаляват силно доверието на обществото в цифровите и електронни услуги и развитието на модерно общество и икономика. Кибер престъпни въздействия са реална заплаха за човешкия живот и жизнени ресурси в особено голям размер. Широката осведоменост за рисковете сред обществото е от изключително значение за превенцията на този вид

[71] Като ISO/IEC 2700x, 27032; BS 25999 и ISO 22301; ITIL и ISO 20000; COBIT; CERT-RMM; PCI DSS и др.

престъпност. Адресирането на проблемите свързани с постоянно развиващите се лица на кибер престъпността 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.

Мерки:

4.6.1 *Превенция на кибер престъпността*

- Повишаване на информираността на обществото за съществуващи и нововъзникващи кибер заплахи и свързаните с тях ескалиращи възможности за престъпни деяния срещу граждани, бизнес, общество и държава;
- Изследване, анализ и дефиниране на мерки и действия за превантивната защита, от съществуващи и нововъзникващи заплахи, и съгласуваност с общите мерки за повишаване на мрежовата и информационна сигурност и устойчивост на непознати въздействия и атаки (описани в т. 4.2.1);
- Сътрудничество чрез публично-частни партньорства, с оглед на взаимосвързаността и взаимозависимостта на съществуващите и изграждане инфраструктура и услуги в кибер пространството и тяхната защита;
- Осигуряване на високи нива на защитеност на потенциално заплашените обекти;
- Взаимодействие и ангажираност на неправителствени организации, бизнес асоциации и общности, образователни институции за целенасочени програми към различни групи от населението с оглед тяхната роля и уязвимости в кибер пространството, с особено внимание към подрастващите, тяхната пристрастеност и зависимост от дигиталното пространство и слаба осведоменост за многоликите кибер престъпни деяния, както и за наказуемостта им;
- Провеждане на кампания и систематични мерки за ограничаване на използването и разпространението на нелицензирани дигитални продукти (софтуер, медия) – от една страна те представляват престъпление по отношение на авторски права (т.е. „цифрово престъпление“), но от друга представляват сериозна заплаха (както и сигурна гаранция) за разпространение на зловреден код и последващи нелегитимни действия (включително и „съучастие“ в кибер престъпни деяния в голям мащаб, чрез бот-нет мрежи, откраднатa идентичност и други).

4.6.2 *Повишаване административния, организационен и технически капацитет и способности на компетентните структури*

Устойчивата тенденция към нарастване броя на компютърните и компютърно-свързаните престъпления, както и все по-лесния достъп на правонарушители до средства за извършване на такива престъпления, включително и предоставянето на кибер престъпни услуги и лесно достъпни технически средства[72], води до невъзможността за правилна и навременна реакция от страна на правоохранителните и правоприлагащите органи. Вмененото на тези структури по закон задължение за преследване и наказване на правонарушители е трудно изпълнимо, и изисква комплекс от мерки за повишаване на **административния, технически и организационен капацитет и способности** на тези структури:

- Осигуряване, както чрез използване на съществуващите методи за обучение чрез публично-частни партньорства, така и чрез нови такива, на **високи нива на компетентност** у ангажираните с противодействието на кибер престъпността служители;

[72] Предоставяни вече и като услуга - Cybercrime-as-a-service

- Във връзка с устойчивата тенденция на **растеж на кибер престъпленията** е необходимо актуализиране на необходимите ресурси и рамка - брой служителите, натоварени с противодействието ѝ и съвременно техническо обезпечаване на компетентните структури, пряко ангажирани с противодействието на кибер престъпността;
- Подсигуряване на **ефективна и адекватна структура** за задоволяване нуждите на **правоприлагащите и правоохранителните органи** от навременни и изчерпателни анализи на компютърни и информационни системи;
- С цел постигането на ефективно и навременно разследване на кибер престъпления с международен характер, повишаване на информационния обмен с **партньорски структури и организации**;
- С оглед на трансграничния характер на кибер престъпността е необходимо, активно участие в различните международни и регионални инициативи и проекти за противодействието ѝ;
- Развитие на **центъра за борба с кибер престъпността** като един от основните елементи на националната координационна мрежа НКОМКС, осигуряване на непрекъсната услуга (24/7) и прилагане на инициативата за “e-SOS” (или „кибер 112“) за **реакция на сигнали за кибер престъпления** и оперативно и техническо взаимодействие с национални, регионални и международни организации и органи (съгласно Модела описан в т.4.1 и Фигура 2).

4.7 Кибер отбрана и защита на националната сигурност

Цели:

Цел 1: Защита и противодействие на различни видове **атаки и организирани действия с деструктивен характер в кибер пространството,** които застрашават сигурността и стабилното функциониране и развитие на държавата и обществото, както и партньорски държави по силата на взаимни договорености и ангажименти. Кибер атаките могат да бъдат самостоятелни или компоненти от хибридни въздействия или комплексни кризи, с различни източници, включително неидентифицирани.

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 съобразно Визията за развитие „Кибер устойчива България 2020“ (т. 2) ще доведе до повишаване на сигурността и устойчивото и конкурентно развитие на гражданското общество, бизнес и държавата в кибер пространството. Те са органично свързани с развитието на националната система за кибер сигурност и устойчивост, и с изграждане на модела за координация и взаимодействие на национално ниво (описан в т. 4.1), и осигуряват развитието в **два аспекта**:

- Защита и кибер устойчивост 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 кибер пространство** 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 жизнено важните ресурси за функциониране на държавата и обществото в извънредни ситуации.

Кибер атаките и въздействия чрез кибер пространството са съществен елемент от съвременните **хибридни модели за водене на война**[73]. Формулираните цели и мерки в настоящата Стратегия са в съответствие и ще бъдат развивани и изпълнявани в пълен синхрон със Стратегията за ролята на НАТО за противодействие на хибридния тип война (2015), политиките на ЕС, както и в националната Стратегия за противодействие на хибридния модел за водене на война. Кибер отбраната е **третият основополагащ стълб** на кибер сигурността съгласно Европейската стратегия за кибер сигурност (2013г).

Мерки:

4.7.1 *Кибер отбрана и въоръжени сили*

Министерството на отбраната има водеща роля за осъществяване на кибер отбраната на страната. За ефективното й реализиране е необходимо да се поддържат и развиват съществуващите и да се изграждат нови високотехнологични способности за кибер отбрана, съвместими с тези на НАТО и ЕС, както и адекватни структурни и организационни реформи и развитие на ресурси, което включва:

- Развитие на **политиките, визията за развитие и ръководни документи за кибер отбрана на въоръжените сили** в съответствие с разглеждането на кибер пространството като пета област (пети домейн) във връзка с националната сигурност, и необходимостта от развитие на адекватни способности за защита и активно противодействие на хибридни заплахи, кибер и хибридни войни и развитие на съвета Комуникационна и информационна поддръжка и кибер отбрана (КИПКО) към Министъра на отбраната;
- Реализиране на **инвестиционни проекти за кибер отбрана** и използване на възможностите на членството ни в НАТО и ЕС за участие в съвместни инициативи и развитие на общ капацитет и способности, включително инициативите на НАТО/ЕС „Интелигентна отбрана“, „Обединяване и споделяне“, както и включване на процеса по изграждане на способности за кибер отбрана в цялостния процес на отбранителното планиране;
- Изграждане на **оперативен център за кибер отбрана (milCIRC)** по модела и с помощта на центъра на НАТО NCIRC, осигуряване на непрекъснато наблюдение (24/7) и пълна оперативна интеграция в националната мрежа НКОМКС, развитие на колективни способности за реакция на кибер и хибридни въздействия от национален и международен мащаб;
- Координирано споделяне на информация за кибер инциденти и взаимопомощ с държавни институции, НАТО и ЕС и сътрудничество с бизнеса и академичната общност;
- Изграждане на **експертен капацитет по кибер отбрана** и повишаване на подготовката на личния състав, чрез **периодични обучения и участие в учения** в тази област, разширяване на участието в центъра за компетентност на НАТО за кибер отбрана и други партньорски центрове;
- Подобряване и развитие на **взаимодействието с индустрия и изследователски организации**, основаване на клъстер „Кибер отбрана“ – активно включване в международни програми на НАТО и ЕС по линия на изследователски проекти, във връзка единен цифров пазар, както и програмата на НАТО за партньорство с индустрията[74], за стимулиране и менторство на МСП, както и кибер-инкубатори;

[73] Определение в Речника (Приложение 3)

[74] NATO Industry Cyber Partnership - http://www.nicp.nato.int/index.html

- Адаптиране и прилагане на модела на ЕС[75] за **обединение и споделяне на ресурси на национално ниво** за специалисти, технологии, база и развитие на формите на ангажираност – използване на механизма за резерв на въоръжените сили за създаване на специализиран „кибер резерв“ и други форми на ангажиране на кибер специалисти от индустрията, академичните среди и професионалните среди.

4.7.2 *Противодействие на хибридни заплахи и кибер тероризъм*

- Мерки и средства за **повишаване на осведомеността** за цялостната среда от а заплахи и състоянието на кибер картината 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);
- Мерки за повишена защита, устойчивост на системите за мониторинг и контрол на националните граници, контролно-пропускателните пунктове, координирано управление на пристанища (в съответствие с National Single Window)[76], летища, ръководство на въздушно движение, и осигуряване на непрекъснато оперативното 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 кибер пространството 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 критични инфраструктури атаки, и създаване на способности за формиране на екипи за бързо реагиране (RRT) със смесена крос-секторна и международна експертиза;
- 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 от състояние на повишена интензивност и мащаб на инциденти, заплаха от кибер и хибридна криза, извънредни ситуации с характеристики и степен на възможно въздействие от мащаба на кибер или хибридни войни - съгласуваност, координация и тестване на механизмите за **получаване и предоставяне на международна помощ и колективни действия**;
- Развитие и специализация на България като център за компетентност и върхови постижения в областта на **кибер отбраната и управление при кризи и хибридни заплахи** - на базата и по модела на многонационалния център за компетентност на НАТО за управление на кризи и реакция при бедствия в София[77], и използване на всички възможни програми и източници (ЕС, НАТО, двустранни и международни програми) за развитието на центрове и лаборатории за изучаване и симулиране на съвременните устойчиви заплахи,

[75] Европейска агенция за отбрана (European Defense Agency, EDA) - http://www.eda.europa.eu/what-we-do/eda-priorities/pooling-and-sharing
[76] Directive 2010/65/EU National Single Window (NSW) for maritime transport
[77] NATO CMDR COE – NATO Crisis Management and Disaster Response Center of Excellence

атаки срещу критични инфраструктури и методи и системи за защита, развитие на кибер устойчиви софтуерни и ИКТ системи.

4.7.3 *Кибер разузнаване*[78]

- 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 кибер картина, интегриране с НКОМКС;
- Развитие на способности за подпомагане на установяването на източниците на въздействия при атаки (“attribution”) и предприемане на адекватни форми за защита и противодействие.

4.8 Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността

Цели:

Цел 1: Постигане на висока **осведоменост на всички целеви групи** и заинтересовани страни и **еднакво разбиране и оценка за заплахите** във връзка с нарастващата всеобща дигитална зависимост и необходимостта от адекватни мерки на всички нива за постигане на информационна и кибер сигурност, развитие на обща кибер култура.

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

Цел 3: Създаване на благоприятна среда за развитие на изследванията и иновативни приложения и превръщането на България във **водещ център за разработване на кибер устойчиви системи на бъдещето**.

Мерки:

4.8.1 *Осведоменост, образование и обучение*

- **Ангажиране на всички заинтересовани страни** в повишаване на общата осведоменост и разбиране на възможните директни и индиректни последствия от кибер въздействия, пробиви в сигурността и небрежност – включване на **аспектите на кибер хигиената като** задължителна **„комплементарна двойка“ на предимствата и удобствата на дигиталната среда** във всички програми за стимулиране на развитието на цифровата икономика, гражданско информационно общество, електронно управление, технологии и иновации;
- Мерки за повишаване на **кибер културата** и отговорното използване на дигитален обмен на информация, предоставяне и използване на електронни услуги по цялата верига на доставки (малък, среден и голям бизнес, граждани) и създаване на добавена стойност, и общата и споделена отговорност за кибер хигиена – ефективно използване на механизмите и **платформите за споделяне на информация** (раздел 4.4.1) ;
- Добавяне на аспектите на кибер сигурността и отговорното и безопасно използване на интернет и ИКТ 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

[78] Cyber Intelligence

обучение, засилване на взаимодействието и ангажираността на индустрия, общество и семейство;

- Допълване и развитие на **педагогическите програми и обучението на учителите и преподавателите** на всички нива с елементите на кибер сигурността и възпитаване на отговорното използване на ИКТ и интернет;
- Осъвременяване и модернизация на програмите в **професионалното и университетско образование** в две основни направления:
    - създаване на специалисти за ИКТ, софтуерна и технологична индустрия, и в различните сфери на мрежова и информационна сигурност и кибер устойчивост – покриване на изисквания за дизайн и разработване на кибер сигурни и устойчиви информационни системи (сигурност , методи и принципи за „сигурно кодиране“, оценка на рисковете, стандарти и методи;
    - дигитални лидери (**е-лидери)** и кадри за развиващата се дигитална икономика и интелигентна специализация на България, съобразно новите технологични тенденции и изискванията за кибер устойчивост на дигитално зависимите бизнес модели, производства и услуги;
- Ефективно използване на формите на **продължаващо обучение, допълнителна квалификация и преквалификация** на всички нива за допълване и актуализиране на компетентностите в сферата на кибер сигурността и използване 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;
- 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 кибер сигурността[79], конкурси, „хакатони“).

4.8.2 *Изследвания, иновации и дигитално лидерство*

- Стимулиране на развитието на изследователска и научно-приложна дейност в съвременните и предизвикателни области на информационната и ИКТ сигурност и създаването на устойчиви системи и модели в съответствие с областите на Стратегическата изследователска програма за киберсигурност (ЕС)[80] – поддържане на високо ниво на международно сътрудничество с водещи световни центрове и специалисти и фокус на горещи и актуални области във връзка с настоящите и бъдещи предизвикателства, технологии, развитие на инфраструктурата, методите и моделите за използване;
- Ангажираност на всички заинтересовани страни за идентифициране на перспективните 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 академични звена в различни сектори и обвързване на **магистърски и докторски програми с реални бизнес и индустриални приложения**;

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

[80] EU, 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)

- Създаване на ефективни механизми за ангажиране на научния и изследователски потенциал (както в България, така и от чужбина) за намиране на **иновативни решения за дейността на държавата и публичния сектор** - електронното управление и услуги, сигурност на е-идентичност и електронно гласуване, криптиране, сигурност на облачните и мобилни услуги, и други въпроси на кибер сигурността, 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 информационното общество в България;
- Развитие и стимулиране на формите на **публично-частни партньорства и клъстери** за създаване на смесени изследователски и приложни лаборатории, технологични паркове и центрове, които да създават възможности и помагат създаването на конкурентни и сигурни ИКТ решения, продукти и услуги, както и да подпомагат бързото и безопасно навлизане на новите цифрови технологии в бизнес и общество и стимулиране на **дигиталното предприемачество, инкубирането на стартиращи конкурентни бизнеси**.

4.9 Международно взаимодействие

Цели:

Цел 1: България ще изпълнява **активна роля в международното сътрудничество в областта на кибер сигурността** 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 кибер сигурността и разработване на съвместни проекти за сътрудничество по линия на НАТО, ЕС и ООН.
Цел 2: България ще продължи да изпълнява **съюзните си ангажименти по линия на НАТО** в областта на кибер отбраната и активно ще участва в прилагането на Меморандума за разбирателство в областта на кибер отбраната и одобрената по време на срещата на върха на Алианса в Уелс Инициатива за сътрудничество с индустрията в областта на кибер отбраната.
Цел 3: Ангажиментите на България по линия на ЕС са обвързани със заложените приоритети в основополагащи документи като Европейската стратегия по кибер сигурност и Европейската политическа рамка за кибер отбрана. Основна цел е изграждането на гарантиран максимално защитен достъп до интернет. С оглед подобряване на националните способности и справянето с кибер заплахите, България следва активно да сътрудничи с органите на ЕС, занимаващи се с въпросите на кибер сигурността (Европейската агенция за сигурност на мрежите и информацията, Европол, Европейската агенция по отбрана), и да развива регионалното и двустранно сътрудничество и взаимодействие.

Мерки:

4.9.1 *Кибер дипломация*

Важен елемент от ангажиментите на България за осигуряване на свободно и сигурно кибер пространство е работата в областта на кибер дипломацията. Заключенията на Съвета „Общи въпроси” по кибер дипломацията (февруари 2015 г.) определят като ключово по-нататъшното развитие на **общ и всеобхватен европейски подход към кибер дипломацията**.

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

- Спазване и насърчаване на спазването на **правата на човека в кибер пространството** (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 кибер пространството, отстояване на позицията, че международното право е приложимо и в интернет);
- Интернет управление (като неделима част от общия и всеобхватен подход на ЕС по кибер дипломацията);
- Засилване на **конкурентоспособността и просперитета на ЕС** (с акцент върху по-нататъшното насърчаване на **Единния европейски дигитален пазар** и засилване на сигурността в областта на информационните технологии, включване на дигиталната 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 кибер капацитет - разработване на общ подход за изграждане на кибер капацитет 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 кибер капацитет и развитие на кибер устойчивост;
- Стратегическо сътрудничество с ключови партньори и международни организации-провеждане на ефективна координация на политиката за кибер сигурност с оглед избягване на дублирането на дейности и инициативи, осъществяване на тясно сътрудничество с международните организации, работещи в областта на кибер сигурността;
- Активизиране и развитие на сътрудничеството с Организацията за сигурност и сътрудничество в Европа (ОССЕ) и “Мерки за укрепване на доверието и сигурността“ [81], инициативи и програми на ООН, международни организации и мрежи.

4.9.2 *Взаимодействие на оперативно и техническо ниво, учения*

- Установяване и осъвременяване на нормативната база и международните договорености за ефективно прилагане на оперативното взаимодействие между органите и структурите от националната система за кибер сигурност и мрежата за координация и взаимодействие (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 публично-частно ниво в сектори и области свързани с критични инфраструктури, критични комуникационни и информационни инфраструктури, стратегически ресурси, както и в новите развиващи се чувствителните области на интернет базирани услуги (електронна търговия, здравеопазване, финанси и други);

[81] Confidence building in the OSCE - http://www.osce.org/secretariat/106440

- Развитие и участие в регионални инициативи и проекти в областта на кибер сигурността, устойчивостта и защита на критични инфраструктури 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.

5 Реализиране, контрол и актуализация

Националната стратегия и Визията за развитие „Кибер устойчива България 2020“ е разработена от междуведомствена експертна работна група с включени представители на всички заинтересовани страни и е съгласувана със Съвета по сигурността, Министерски съвет на Република България.

Паралелно с набелязването на основните области на действие, мерки и етапи за развитието до 2020 година се разработва План за изпълнението на Стратегията, който ще бъде завършен до 3 месеца след публично обсъждане и приемане на Стратегията от Министерския съвет. В изготвянето на Плана, приоритизиране на проектите и инициативите и дефинирането на Пътна карта ще бъдат включени и ангажирани организации представляващи всички заинтересовани страни – държавна, бизнес и индустрия, академични и изследователски организации, неправителствени организации. Изпълнение на плана е отговорност на определените водещи институции и организации, като реализацията на всички инициативи се базира на принципите и методите на проектно управление и ориентирани към резултат действия на базата на предварително зададени индикатори. За валидацията на резултатите от изпълнението на набелязаните мерки се организират и провеждат специализирани национални и регионални учения и тестове, както и засилване на участието в международни и партньорски такива. Координацията на изпълнението се осъществява от Националния координатор по кибер сигурността, а мониторинга за постигнатите резултати – от Съвета по сигурността чрез консултативния Съвет по кибер устойчивост и годишен доклад за прогреса. В доклада по целесъобразност се предлагат актуализация на Стратегията, Плана за изпълнение и Пътната карта.

За повишаване на осведомеността и ангажираността на всички заинтересовани страни и групи от населението и бизнеса, както и партньорски държави и структури да бъде изготвено адекватно по форма и съдържание представяне на стратегията и визията, набелязаните мерки, 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 партньорски държави от ЕС и НАТО, както и на други държави и организации на базата на двустранни договорености и взаимоотношения в областта на кибер сигурността (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 за участието в съвместни програми и инициативи.

Приложение 1: SWOT анализ за състоянието и предизвикателствата пред България в кибер пространството

Силни страни (Strengths)	**Слаби странни (**Weaknesses)
Висока степен на проникване на ИКТ Високоскоростен интернет и свързаност Традиционно силни ИКТ сектор и софтуерна индустрия Наличие на високо квалифициран човешки ресурс за работа с ИКТ Развити партньорски отношения между публичния, неправителствения сектор и ИКТ бизнеса Експертен персонал в сектор „сигурност и отбрана“ от различните ведомства Използване на поне един чужд език от голяма част от населението Български ИКТ компании и специалисти са ангажирани за доставчици на услуги в областта на cyber forensics Развито информационно общество	Липса на ясни политики и общи правила за осигуряване кибер сигурност Недостатъчно развита и адекватна правна рамка по отношение на кибер сигурността Отсъствие на свързаност между отделни системи, ангажирани с кибер сигурността Ниска степен на образованост и разбиране на важността на кибер сигурността Малкият и среден бизнес не припознава информационната и кибер сигурност като проблем и приоритет Ниска технологична култура в част от структурите на централна и местна изпълнителна власт Липса на действаща система за ранно предупреждение за кибер атаки Използване на софтуерни и хардуерни решения без елементи или ангажименти по сигурността (вкл. и такива от чуждестранни компании)
Възможности (Opportunities)	**Заплахи (**Threats)
Развитие на технологиите – повишаване на ефективността при намаляваща цена Сравнително лесно преодоляване на технологична изостаналост Практически неограничен достъп до знание, ноу-хау, добри практики Членство в НАТО и ЕС Интензивно сътрудничество с партньорски служби от други държави Привличане на неангажиран човешки ресурс (вкл. и от сивия сектор, хакери, white hats и др.) Наличие на добре подготвени кадри с висше образование с ИКТ профил Динамичен глобален пазар на продукти и услуги в сферата на кибер сигурността Системно развитие на информационна култура в училищата Повишаване заинтересоваността за информационната и кибер сигурност в компаниите, особено МСП и по веригите за доставка	Икономически най-изостаналата държава в ЕС Ръст на кибер престъпленията в световен план при засилваща се глобална несигурност Нарастващ интерес към РБ като обект за кибер атаки (член на ЕС, НАТО и др.) Постоянно повишаване на количеството, интензитета и сложността на кибер атаките (включително незабелязани) Хибриден характер на заплахите – взаимовръзка, домино ефект Нарастване на дигиталната зависимост - проникване във всички сфери на живота (IoT - всички устройства са свързани в интернет) Невъзможно поддържане на „частична сигурност“ Заплаха за средата за развитие на аутсорсинг на услуги към България Изтичане на интелектуалния потенциал (особено в сферата на ИКТ) Ползване на нелицензиран, пиратски софтуер (особено от граждани и МСП) Експанзия на облачните услуги, при които сигурността не винаги е гарантирана Висока степен на използване на социални мрежи (канал за възможно проникване, шпионаж, тероризъм) Развитие на организираната кибер престъпност Огромен ръст в предлагането услуги и онлайн забавления Прехвърляне на нелегалния (сив) пазар в кибер пространството (трафик на хора, органи, наркотици, оръжие и др.) Интернет е неконтролируем канал за дезинформация (лесно създаване на паника, психоза, финансова нестабилност, и др.)

Приложение 2: Фази за реализиране на стратегията

Фаза 1: Иницииране и постигане на базов капацитет за кибер сигурност (2016-2017г.)

Основна цел на дейностите е установяване на координиран подход и изграждане на обща национална рамка и принципи за развитие, национална стратегия и план за действие с пътна карта за развитие и приоритети, съгласувани с основните заинтересовани страни, **преодоляване на изоставането** в ЕС и НАТО и осигуряване на **базово ниво на информационна и кибер сигурност**. През този етап ще бъде постигната необходимата минимална информационна и кибер сигурност на ниво отделни организации и мрежи и способности за реакция при кибер инциденти и атаки, като се постигнат следните **основни показатели**:

- Финализиране на национална стратегия за кибер сигурност, национален план за изпълнението ѝ с пътна карта „2020“;
- Установен работещ „мултистейкхолдер“ модел за включване и ангажиране на всички основни заинтересовани страни от държава, бизнес, академия, неправителствени организации и общество за **координирани действия по развитие** и непрекъснато осъвременяване на стратегията, политиките и мерките;
- Въвеждане и прилагане на **проектен подход** за управление на дейностите по изпълнение на националния план за кибер сигурност и методика за **приоритизиране** на дейностите и проектите, стартиране на проектите с най-висок приоритет или с неотложен характер;
- Създаване на **Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)**[82] по модела на **публично-частните партньорства** (ПЧП) - определяне на роли, отговорности и способности за развитие на държавните и неправителствените участници, установяване на общ механизъм, **дефиниране на процеси** и протоколи за **взаимодействие и мониторинг** на кибер картината на национално ниво на базата на координирана мрежа от центрове за кибер сигурност (CERT/CSIRT и други органи) и борба с кибер престъпността, развитие и осигуряване на основен изискуем капацитет и способности и интегриране в **Националната система за управление при кризи**[83];
- Преглед на комуникационните и информационни системи в публичния сектор и **критичните инфраструктури** с национално значение по отношение на кибер сигурността, определяне на **минимални изисквания**[84], подготовка и приоритетно включване в мрежата **НКОМКС** на основни сектори от енергетиката, транспорта, банков и финансов, мобилни комуникации, както и на интернет доставчици, доставчици на електронни услуги и други от национално значение (и във връзка с изпълнение на Директивата на ЕП за сигурност на мрежовите и информационни системи);

[82] **NCCN, National Cybersecurity Coordination Network**

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

[84] Минимални изисквания: определени общо от НКОМКС, за отделни сектори - от специализирани държавни органи

- Подготовка и провеждане на пилотни секторни национални учения/упражнения от типа на CyberSHockwave[85] по формулата на ПЧП и в допълнение на ученията в ЕС и НАТО;
- Изпълнение на указанията и **директивите на ЕС и препоръките на НАТО** за постигане на **мрежова и информационна сигурност (МИС)** – разработване на национална стратегия, план и действия по изграждане на капацитет и способности за справяне с масирани кибер инциденти, атаки и кризи;
- Активизиране на **международните партньорства** и ефективното им използване за развитие и взаимодействие – преглед и развитие на действащи национални точки и звена за оперативно и техническо взаимодействие, развитие на адекватни на международните изисквания капацитет и способности;
- Преглед и организиране (координиране) на наличния експертен и технически капацитет в държавни, неправителствени, академични и частни организации, изработване и валидиране на модел за мобилизиране и включването им в НКОМКС (идентифициране на националния капацитет за кибер сигурност). Установяване на система от стимули за развитие на общ капацитет в изследователски центрове, технологични паркове, фирми и неправителствени организации;
- Дефиниране на основните **изисквания, стандарти и модели** за проектиране и разработване на комуникационни и информационни системи за системите за държавно управление и администрация, съгласувани и препоръчителни и за бизнеса в посока „дизайн за сигурност“, “поверителност чрез дизайн“, “дизайн за устойчивост“ [86];
- Разработване на национална програма за осведоменост (awareness) и ангажираност към дейностите по кибер сигурността с всички слоеве на обществото, специален фокус върху младежите и образованието, малкия и среден бизнес (МСП и микро-предприятия), образователните и обучителни програми на всички нива;
- Развитие на демократичния модел за управление на Интернет – домейни (вкл. и на кирилица „.бг“) и свързаните с тях заплахи, въвеждане на мерки и принципи за сигурност и надеждност (от типа на препоръчаните от ICANN “https only”, DNSSEC) за правителствените сайтове и системи, както и стимули и мерки за разширение в бизнес секторите.

Фаза 2: Развитие – от капацитет към способности (2018-2019г.)

Развитие на организационен и национален капацитет и подготовка на различни нива – реализиране на **устойчивост на ниво организация/ведомство** и способности за реакция при кибер инциденти и кризи, засилване на дейностите по превенция. Ще бъдат постигнати следните резултати:

- Институционализиране на процесите за **мониторинг и взаимодействие** на **Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)** и поетапно включване на секторни и индустриални центрове за кибер сигурност (CERTS/CSIRT и др.) - фокус върху приоритетни критични инфраструктури и пълната интеграция и осигуряване на функционирането на **Националната система за**

[85] Cybershockwave http://bipartisanpolicy.org/press-release/cyber-shockwave-shows-us-unprepared-cyber-threats/

[86] security by design, privacy by design, resilience by design

управление при кризи; Осигуряване и усъвършенстване на адекватна правно-регулаторна рамка;

- Въвеждане на обща методика по оценка на рисковете свързани с кибер заплахи, анализ на уязвимости, въздействие и значимост, потенциални цели, съгласувани и в съответствие с тези в НАТО, ЕС, ООН, ITU; разработване на рамка за оценка на споделените кибер рискове по мрежите/вериги за доставка, и определяне на съответни отговорности;
- Повишаване на капацитета на националните, секторни и ведомствени центрове за кибер сигурност (CERTS/CSIRT и др.) и развитието им в пълноценни Оперативни центрове за сигурност (SOC)[87] за следене на състоянието на комуникационните и информационни системи, ранно откриване на заплахи и излъчване в НКОМКС, както и способности за координирана реакция при кибер инциденти, атаки и кризи до неутрализирането им и предприемане на дейности по възстановяване – постигане на устойчивост на ниво организация, ведомство, цялостна верига на доставки или бизнес мрежа;
- Развитие на капацитет за симулация на сложни кибер инциденти, атаки и кризи и провеждане на комплексни национални учения/упражнения от типа на Cyber Shockwave[88] по формулата на ПЧП и в допълнение на упражненията в ЕС и НАТО. Организиране на учения с държавите от региона и други международни партньорски мрежи;
- Идентифициране на необходимост и развитие на технологичен и изследователски капацитет и способности в приоритетни области за държавата, гражданите и бизнеса – осигуряване на иновативна и съвременна база за електронни услуги (вкл. за електронно управление), надеждни електронни разплащания (вкл. мобилни), електронно здравеопазване, кибер защита/отбрана, и други възможни ниши за развитие на индустрия, научни и приложни изследвания – във връзка със стратегията за интелигентна специализация на Р България 2014-2020[89] и Програмата „Цифрова България“[90] и съответните Оперативни програми;
- Използване на председателство на ЕС от Република България за повишаване на осведомеността и ангажиментите и международното сътрудничество в областта на кибер сигурността;
- Разширение на изискванията и препоръките за изграждане на доверие в Интернет – прилагане на план за преминаване на “https only” за всички Интернет услуги, и преминаване към “DNSSEC only” за държавните домейни и предлагани електронни услуги.

Фаза 3: Зряло и кибер устойчиво общество (2020 + г.)

Постигане на ниво на зрялост което осигурява **кибер устойчивост на национално ниво** и ефективно взаимодействие и интеграция на международно ниво (ЕС, НАТО). Чрез ангажиране на всички заинтересовани страни, България приоритетно създава способности както в

[87] SOC - Security Operations Center

[88] Cybershockwave http://bipartisanpolicy.org/press-release/cyber-shockwave-shows-us-unprepared-cyber-threats/

[89] Иновационна стратегия за интелигентна специализация на Република България 2014-2020 г. ОПИК - Оперативна програма „Иновации и конкурентоспособност“ 2014-2020

[90] Програма „Цифрова България 2020“

държавния, така и в частния и изследователския сектор в идентифицирани ниши за постигане на водещи позиции в региона и партньорските мрежи. Очаквани резултати от тази фаза са:

- Пълен капацитет на **Национална координационно-организационна мрежа за кибер сигурност (НКОМКС)** с постигнато ефективно взаимодействие със секторни и индустриални центрове за кибер сигурност (CERTS/CSIRT/CIRC и др.) и пълната интеграция в **Националната система за управление при кризи**, в системите на ЕС и НАТО и международни партньорски мрежи;
- Специализация и утвърждаване на България като водещ партньор в ЕС и НАТО в определени **приоритетни области** на базата на стимулиране и развитие на върхови технологии и процеси, свързани с кибер сигурността и икономиката на знанието;
- България да предлага една от най-атрактивните среди в Европа за развитие и установяване на свързан с интернет бизнес – сигурна и надеждна среда за аутсорсинг на услуги, хостване на интернет бизнес, специализация в разработване на сигурен софтуер и кибер устойчиви системи, развитие на интернет-свързани устройства (Internet of Things - IoT) и приложения;
- Успешно реализирани е-услуги и системи в държавното управление и бизнеса и разкриване на нови направления за развитие на бизнес в регионален и световен аспект;
- Установени специализирани изследователски и приложни центрове с уникални компетентности и технологична база за симулации, обучение, тестване и активна защита на ИКТ системи, системи за управление в индустрията и критични инфраструктури (Industrial Control Systems ICS, SCADA, други).

Приложение 3: Речник

Определения[91]

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).

Кибер пространство - интерактивна среда от електронни мрежи и информационна инфраструктура използвана за създаване, унищожаване, съхранение, обработка, обмяна на информация, управление на обекти, системи и услуги.

Кибер пространство (2) - сферата, в която информационната среда съставена от независими мрежи на информационни системни инфраструктури включително интернет, телекомуникационни мрежи, компютърни системи, вградени процесори и контролери се използват за обработване, съхраняване и пренасяне на информация и дейности на потребители.

Кибер престъпление – престъпни цели (действия), които се определят в качеството на такива в националното и/или международното законодателство насочени към и/или използващи кибер пространството.

Кибер престъпност (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).

Кибер сигурност - състояние определено и измерено чрез нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги. Кибер сигурността се основава на ефективно изграждане и поддръжка на активни и превантивни мерки.

(Според ISO 27000) – опазване на **конфиденциалността, интегритета** (целостта) и **наличността** на информацията (триада на информационната сигурност - КИН, или CIA – Confidentiality Integrity Availability)

(ЕС) – Под кибер сигурност обикновено се разбират предпазните мерки и действия, които могат да бъдат приложени за предпазване на кибер пространството както в гражданската, така и във военната област, от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура или могат да нарушат работата им. Целта на кибер сигурността е да се съхрани наличността и целостта на мрежите и инфраструктурата, както и поверителността на информацията, която се съдържа в тях.

Кибер атака - злонамерена дейност, която цели да разруши, да осигури контрол над компютърна среда/инфраструктура, да наруши интегритет на данни или откраднe контролирана информация.

[91] 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.

Кибер инцидент - неоторизирани или неочаквани дейности в КИС, при които автоматизираните мерки не са достатъчни за предотвратяване на негативни въздействия, но за които експертите по кибер защита могат да предупредят.

(НАТО) - неочаквано събитие в кибер пространството, което, с или без криминален умисъл, би могло да промени кибер сигурността 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 кибер сигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията

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

Риск – потенциалната възможност дадена заплаха да бъде реализирана, като се експлоатира уязвимостта на активите, за да се причини вреда.

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 процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата.

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

Computer emergency response team (CERT) - организация, която изучава уязвимостите в кибер пространството и подпомага жертви на хакерски атаки, осигурява 24/7 услуги, споделя информация за повишаване на кибер сигурността и координира отговори на заплахи на кибер сигурността (известни в различни организационни форми – CSIRT, CIRC и др.)

Кибер отбрана - Интегрирана система, свързана с изпълнението на всички мерки, по защитата на комуникационно-информационните системи на въоръжените сили от кибер атаки за осигуряване постигането на военно-стратегическите цели.

Кибер война - Кибер война е всеки политически мотивиран конфликт в кибер пространството, характеризиращ се с кибер атаки срещу компютърните и информационните системи на противника.

Кибер война (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.

Хибридна заплаха[92] – 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, кибер атаки, 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.

[92] Национална „Стратегия за противодействие на хибридния модел на водене на война“ (в процес на приемане)