АКАДЕМИЯ на МВР

Факултет ПОЛИЦИЯ

Специалност: ЗАЩИТА на НАЦИОНАЛНАТА СИГУРНОСТ

Задочно 2022/2023

ДИПЛОМНА РАБОТА

НА ТЕМА:

КИБЕРПРЕСТЪПНАСТТА КАТО ЗАПЛАХА ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Научен ръководител: проф. д-р Павел Николов

Дипломант: Георги Сачков

Факултетен № МССТ 6390

gogors@abv.bg

0884 322 733

Презентация

СОФИЯ 2023 г.

МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ

АКАДЕМИЯ

ФАКУЛТЕТ „ПОЛИЦИЯ“

УТВЪРЖДАВАМ:
НАУЧЕН РЪКОВОДИТЕЛ
доц. д-р Павел Христов
(акад. длъжност, имена, подпис)
София, 19.09. 2022 г.

З А Д А Н И Е

за разработване дипломна работа от дипломанта
Георги Рудолфов Сачков "Полиция" - ЗНС фак. № МССТ 6390
(трите имена, курс, факултет, специалност, фак. №)

1. Тема: Киберпрестъпността като заплаха за националната сигурност.

(чл. 37, ал. 2 от Правилник за организация на учебната дейност – възлага се не по-късно от края на първия месец от последния семестър на обучението му)

2. Научният ръководител и темите на дипломната работа се предлагат от ръководител на катедрата и се утвърждават от декана.

3. Кратка анотация на темата (цел, съдържание):

.....

.....

4. Научно-методическо ръководство на дипломанта:

(чл. 39 от Правилник за организация на учебната дейност т. 1-6)

- подготви и предложи за обсъждане и приемане от катедрения съвет на заданието за разработване на дипломна работа в 2 екземпляра;
- връчи утвърденото задание на дипломанта и след подписване от последния да върне единия екземпляр за съхранение в катедрата;
- ръководи дейността на дипломанта по съставянето на библиографската справка и разработването на календарния и структурния план;
- следи хода на разработването на дипломната работа и да консултира дипломанта по научни и методически проблеми;
- информира ръководителя на катедрата при възникване на проблеми при разработването на дипломната работа от дипломанта и при изоставане от планираните срокове;

СЪДЪРЖАНИЕ

УВОД

С развитието на технологиите и проникването на глобалната информационна мрежа във всички аспекти на живота ни светът постепенно се придвижва към едно ново състояние на перманентна свързаност, което изцяло променя не само начините, по които комуникираме, но и фундаментално предефинира редица обществено-икономически взаимоотношения. Този процес драматично рефлектира върху социалните връзки, създавайки обективни предпоставки за актуализиране на базови понятия, върху които съществува трайно обществено съгласие и са възприети като константни през годините[1].

Пример за такава фундаментална промяна е налице и в сектор „Сигурност“, където постепенно еволюира самата парадигма за това понятие, поставяйки редица въпроси пред ангажираните с изготвяне на политиките по опазването й, като например: Какво представлява днес и какво точно предполага понятието „сигурност“ в различните си измерения - за съвременния човек от една страна, за бизнес организациите от друга и за модерната държава от трета? Как да се изгради ефективна система за сигурност в един глобално обвързан, динамичен и взаимозависим свят? Какви структури са нужни и как следва да бъдат разпределени различните отговорности по опазването й ? Всички тези въпроси предполагат неоднозначни отговори, които следва да бъдат търсени чрез широк обмен на нови гледни точки и ангажимент за извличане на обратна връзка от реалния живот, чрез събиране на доказателствата за това какъв подход или кои мерки работят и какво вече не е актуално като тенденция или решение.

Актуалност на темата

Все по-често ставаме свидетели на случаи, които илюстрират растяща неадекватност на мерките и инструментите за прилагането им от политиките по информационна и киберсигурност. Примерите от последните години с изтичането на данни от НАП на над хиляди български компании и милиони физически лица са само върха на един огромен айсберг, който има потенциал да

[1] https://trud.bg/Явор Колев

причини мащабни негативни последици не само от икономически характер, но и в чисто физически план за гражданите в страната ни. Разбира се тези заплахи отдавна са известни, при това не само на експертната общност, но и за широката общественост, но изглежда политиките и мерките за превенцията им сякаш изостават драстично от скоростта на развитието на процесите и съответно предизвикателствата на киберпространството.

Актуалната тенденция в подхода към киберсигурността като фундаментален компонент на националната сигурност е холистичен, като стремежът е да бъдат обхванати множество аспекти - икономически, социални, образователни, правни, технически, дипломатически, военни и разузнавателни. Това е основната причина да се търсят нови възможности за изработка на по-ефективни мерки и политики за гарантиране на сигурността в киберпространството, както на индивидуално, така и на национално, а и на международно ниво.

Актуализацията на Националната стратегия за киберсигурност „Киберустойчива България 2020“ е съобразена с приетата наскоро Националната програма за развитие България 2030 . В рамките на приоритета „Институционална рамка“ програмата посочва, че мрежовата и информационна сигурност е пряко свързана с доверието на потребителите в електронните услуги, а безопасното и широко използване на продукти и услуги, базирани на данни зависи от постигането на най-високи стандарти за киберсигурност.

Обект, предмет, цели и задачи

Основен обект е процесът на формиране на националните политики по сигурността и прилагане на предвидените от тях мерки, обезпечаващи ефективното им функциониране в условията на ускорено развитие на ИКТ. Разглеждат се актуалните тенденции и възникващите предизвикателства свързани с тях в областите на информационната и киберсигурност, като се анализират съществуващите решения, примери и добри практики от различни държави с традиции и установен напредък в тази област.

Като основен предмет се разгръща изследователският потенциал върху ускоряващите се информационно-технологични промени и възникващите като резултат от тях социални следствия, които оформят специфични предизвикателства при създаването на политики, подходи и решения за управление на националната сигурност в аспекта на киберпространството.

Фокусът се поставя върху изследване процесите на преплитане на виртуалния и физическия аспект в съвременния социум, като пряк резултат от интензивното информационно-технологично натрупване и начинът, по който виртуалното пространството постепенно започва да оказва силно въздействие върху съзнанието (и респективно действията) на модерния човек, като по този начин пренарежда социалните отношения през 21-ви век.

Цели

Като основен приоритет имам за цел да се оцени степента, в която актуалните политики в областта на националната сигурност адресират нарастващите предизвикателства в информационната среда, зададени от ускоряващата се технологична среда, в която оперират.

Друга съществена цел е свързана с прилагане на научен подход в изследването на един нов феномен – постепенното преплитане на киберпространство и реалност, като се изследва въздействието му върху когнитивните процеси на потребителите, с оглед разкриване на нови и малко познати аспекти на сигурността в информационните общества, като част от един много по-мащабен проблем, чиито рамки далеч надхвърлят технологично превъзходство и доминация на една държава /политически съюз/ над друга.

Задачи

Основните задачи са свързани с провеждане на няколко отделни компонента, които са логически подредени съобразно естеството на взаимовръзките им и респективно се представят в три обособени части като отделни глави.

Изследователска хипотеза и основната теза е свързана с разбирането, че в края на второто десетилетие на 21-ви век в следствие на повсеместното проникване на информационно-комуникационните технологии протича интензивен процес на трансформиране на обществата от пост-индустриален тип в нов вид глобално- информационен мрежови социум, характеризиращ се преди всичко с огромна степен на свързаност и взаимозависимост на процесите.

Методи и подходи – инструментариум

Основните методи са изследванията, включващи изследване на съществуващата литература в областта, преглед на различни стратегически и юридически документи, провеждане на проучвания.

Метод за характеризиране на всяко престъпление е да се определят елементите „извършване / поведение / провеждане", „обстоятелство" и „резултат".

Там, където един от тези елементи се локализира или произведе съществени щети на друга територия, ще е наличен международен характер на съответното киберпрестъпление.

На следващо място от инструментариума е да се използват групи, с представители на различни сфери на бизнеса, държавната администрация и академичната общност. Основна цел е дефинирането от една страна същността на проблема с личните данни, а от друга – важността на опазването на неприкосновеността им и идентифицирането на проблемите, с които те се сблъскват в процеса.

Инструментариумът за разследване на киберпрестъпленията осигурява директно взаимодействие с доставчиците на услуги и лицата, предоставящи услуги по регистрация на домейни, с цел придобиване на информация за идентифициране на заподозрени, сътрудничество за разкриване на информация за абонираните лица и трафичните данни, сътрудничество за разкриване на информация в спешни случаи, допълнителни инструменти за сътрудничество и защита на данните и др.

Глава I – Киберсигурност. Мрежова и информационна сигурност

Основни термини и понятия съгласно закона[2]:

- „**Административен орган**“ е органът, който принадлежи към системата на изпълнителната власт, както и всеки носител на административни правомощия, овластен въз основа на закон.
- „**Група за сътрудничество**“ е групата по смисъла на чл. 11 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.).
- „**Действия при инцидент**“ са всички процедури, подпомагащи установяването, анализа и ограничаването на инцидент, както и реагирането на такъв инцидент.
- „**Длъжностно лице**“ е понятието по смисъла на чл. 93, т. 1 от Наказателния кодекс е това, на което е възложено да изпълнява със заплата или безплатно, временно или постоянно:

а) служба в държавно учреждение с изключение на извършващите дейност само на материално изпълнение;

б) ръководна работа или работа, свързана с пазене или управление на чуждо имущество в държавно предприятие, кооперация, обществена организация, друго юридическо лице или при едноличен търговец, както и на нотариус и помощник-нотариус, частен съдебен изпълнител и помощник-частен съдебен изпълнител. .

- „**Доставчик на DNS услуги**“ е субект, предоставящ DNS услуги по интернет. DNS (Domain Name System) е Система за имена на домейни, която представлява йерархично разпределена мрежова система за именуване на домейни, разпределяща заявки за имена на домейни.
- „**Доставчик на цифрови услуги**“ е юридическо лице, предоставящо цифрова услуга.

[2] Закон за киберсигурност

- „**Зловреден интернет трафик**“ са аномалии на интернет трафика, предизвикани от хардуерни или софтуерни повреди на интернет пакети със злоумишлено модифицирани опции.
- „**Информационна защита**“ е комплекс от организационни, юридически, технически и технологични мерки за мониторинг, анализ, активна превенция, намаляване влиянието на уязвимости, споделяне на информация за тях, включително отстраняване на последствията от инциденти.
- „**Инцидент** със „значително увреждащо въздействие“ се определя, като се вземат предвид следните показатели:

а) брой ползватели, разчитащи на услугите, предоставяни от субекта;

б) зависимост на други сектори – от посочените в приложение № 1, от услугата, предоставяна от субекта;

в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност;

г) пазарният дял на субекта;

д) географският обхват на областта, която би била засегната от даден инцидент;

е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга. Когато е целесъобразно, се вземат предвид и характерните за сектора показатели, за да се определи дали даден инцидент би имал значително увреждащо въздействие.

- „**Кибератака**“ е опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив.
- „**Киберзаплаха**“ е възможността за злонамерен опит да се повреди или прекъсне компютърната мрежа, системата, услугите и данните.
- „**Киберинцидент**“ е събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да

предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

- „**Киберинцидент със значителен приоритет**“ е киберинцидент, който оказва сериозно въздействие върху дейността на правителството, върху предоставянето на съществени услуги на голяма част от българското население или върху икономиката на Република България.
- „**Киберинцидент с висок приоритет**“ е киберинцидент, който има сериозно въздействие върху голяма организация или върху по-широко/местно управление или който представлява значителен риск за предоставянето на съществените услуги на голяма част от българското население или върху икономиката на Република България.
- „**Киберинцидент със среден приоритет**“ е киберинцидент, който има сериозно въздействие върху средна организация или който представлява значителен риск за голяма организация или за по-широко/местно управление.
- „**Киберотбрана**“ е комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност.
- „**Киберпространство**“ е глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни.
- „**Киберрезерв**“ е допълнителен ресурс от експерти в областта на киберсигурността, защитата на информацията и информационните технологии с компетентности, свързани с осигуряване на защита и устойчивост на комуникационните и информационните системи.
- „**Компютърна услуга „в облак“** е цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно.

- „**Лица, осъществяващи публични функции**“ са нотариусите, частните съдебни изпълнители, държавните и общинските учебни заведения, държавните и общинските лечебни заведения, възложителите от Закона за обществените поръчки, които не са административни органи или организации, предоставящи обществени услуги и други лица и организации, чрез които държавата упражнява своите функции и на които това е възложено със закон.
- „**Мащабен инцидент**“ е налице, когато са регистрирани инциденти със среден приоритет в мрежите и информационните системи на повече от 4 от субекти, с висок приоритет в мрежите и информационните системи на повече от два от субекта и със значителен приоритет на повече от един от субект. Класификацията на инциденти в зависимост от типа на атаката се определя по методика на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).
- „**Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност**“ е мрежата по смисъла на чл. 12 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.).
- „**Мрежа и информационна система**“ е:

а) електронна съобщителна мрежа е съвкупност от преносни системи, независимо дали са базирани на постоянна инфраструктура или на централизиран административен капацитет, и когато е приложимо, оборудване за комутация или маршрутизация и други ресурси, включително неактивни мрежови елементи, които позволяват пренос на сигнали посредством проводници, радиовълни, оптични или други електромагнитни способи, включително спътникови мрежи, фиксирани (с комутация на канали и с пакетна комутация, включително интернет) и мобилни мрежи, електропроводни системи, доколкото се използват за пренос на сигнали, мрежи, използвани за радио и

телевизионно разпръскване, и кабелни мрежи за разпространение на радио и телевизионни програми, независимо от вида на пренасяната информация.;

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или

в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от гореуказаните, с цел обработване, използване, защита и поддръжка.

- „**Онлайн място за търговия**“ е цифрова услуга, която дава на потребители или търговци възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия.
- „**Онлайн търсачка**“ е цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с исканото съдържание.
- „**Организация, предоставяща обществени услуги**“ е всяка организация независимо от правната форма на учредяването и, която предоставя една или повече услуги като: образователни, здравни, водоснабдителни, канализационни, топлоснабдителни, електроснабдителни, газоснабдителни, телекомуникационни, пощенски, банкови, финансови и удостоверителни по смисъла на Регламент (ЕС) № 910/2014 или други подобни услуги, предоставени за задоволяване на обществени потребности, включително като търговска дейност, по повод на чието предоставяне могат да се извършват административни услуги.

- „**Повторно**“ е нарушението, извършено в срок една година от влизането в сила на наказателното постановление, с което на нарушителя е наложено наказание за същото по вид нарушение.
- „**Представител**“ е физическо или юридическо лице, установено в държава – членка на Европейския съюз, което е изрично определено да действа от името на доставчик на цифрови услуги, който не е установен в държава – членка на Европейския съюз, и към което национален компетентен орган или екип за реагиране при инциденти с компютърната сигурност може да се обърне вместо към доставчика на цифрови услуги във връзка със задълженията на доставчика на цифрови услуги по този закон.
- „**Регистър на имена на домейни от първо ниво**“ е субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от първо ниво (top-level domain – TLD).
- „**Риск**“ е потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на информационните активи, за да се причини вреда.
- „**Съществени услуги**“ са услуги, които имат съществено значение за поддържането на особено важни обществени и/или стопански дейности в един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода или цифрова инфраструктура.
- „**Спецификация**“ е техническа спецификация по смисъла на чл. 2, т. 4 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ, L 316/12 от 14 ноември 2012 г.).

- „**Точка за обмен в интернет** (ТОИ)“ е мрежово средство, което дава възможност за свързване на повече от две независими автономни системи преди всичко с цел улесняване на обмена на интернет трафик. Чрез ТОИ се осъществява свързване само на автономни системи. Свързването чрез ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин.
- „**Уязвимост**“ е неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата.
- „**Цифрова услуга**“ е услуга по смисъла на чл. 1, параграф 1, буква „б“ от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ, L 241/1 от 17 септември 2015 г.), от категориите, посочени в приложение № 2.
- „**Цифрова инфраструктура**“ е инфраструктура, която включва ТОИ, доставчици на DNS услуги и регистри на имената на домейни от първо ниво – Доставчици на DNS услуги.

1. Киберсигурност

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

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

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

1.1. Мерки за мрежова и информационна сигурност

Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране.

Минималният обхват на мерките за мрежова и информационна сигурност, както и други препоръчителни мерки, се определят с наредба на Министерския съвет по предложение на председателя на Държавна агенция „Електронно управление“, която включва следните минимални организационни мерки:

- разпределение на отговорностите за мрежовата и информационната сигурност;
- прилагане на политика за мрежовата и информационната сигурност;
- управление на:

а) риска;

б) информационните активи, включително човешките ресурси;

в) инцидентите;

г) достъпите (физически и логически);

д) измененията;

е) непрекъснатостта на дейността и/или услугите (съществени, цифрови);

ж) взаимодействията с трети страни.

1.2. Законово се определят обхвата и изискванията към

а) административните органи;

б) операторите на съществени услуги и доставчиците на цифрови услуги – за всеки сектор, подсектор и услуги;

в) лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги, когато тези лица предоставят административни услуги по електронен път;

г) организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път.

1.2.1. Оператор на съществени услуги е публичен или частен субект от категории, който отговаря на следните критерии:

а) да предоставя съществена услуга, и

б) предоставянето на тази съществена услуга да зависи от мрежи и информационни системи, и

в) инцидентите в мрежовата и информационната сигурност да имат значително увреждащо въздействие върху предоставянето на тази услуга.

1.2.2. Административните органи определят операторите на съществени услуги съгласно критериите и в съответствие с методика, приета от Министерския съвет, и уведомяват председателя на Държавна агенция „Електронно управление“ за това. Методиката се приема по предложение на председателя на Държавна агенция „Електронно управление“.

1.2.3. Когато оператор предоставя съществена услуга в две или повече държави – членки на Европейския съюз, административният орган провежда консултации

със съответните държави преди вземането на решение относно определянето на оператора.

1.2.4. Операторите на съществени услуги спазват изискванията за мрежова и информационна сигурност, предвидени в този закон, само по отношение на предоставяните от тях съществени услуги.

1.2.5. Когато в правен акт на Европейския съюз или в закон, който е специален за конкретен сектор или услуга, се предвижда операторите на съществени услуги или доставчиците на цифрови услуги да гарантират мрежовата и информационната си сигурност или да уведомяват за инциденти, се прилагат тези актове, при условие че техните изисквания са най-малкото равностойни като резултат на задълженията, предвидени в този закон.

1.3. Изключения, при които не се прилага

а) за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация;

б) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Държавна агенция „Технически операции“, Служба „Военна информация“ и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители;

в) по отношение на предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги по смисъла на Закона за електронните съобщения;

г) за доставчици на удостоверителни услуги при електронни трансакции на вътрешния пазар.;

д) за доставчици на цифрови услуги, които са микро- и малки предприятия от Закона за малките и средните предприятия.

1.4. Регистър

Председателят на Държавна агенция „Електронно управление“ създава, води и поддържа регистър на съществените услуги, който съдържа:

а) видове съществени услуги;

б) списък на операторите на съществени услуги и предоставяните от тях услуги;

в) сфера на дейност;

г) брой потребители, разчитащи на услугата, предоставяна от оператора;

д) географски обхват на областта, която може да бъде засегната от даден инцидент.

- Списъкът се преразглежда и актуализира на всеки две години от съответните административни органи, за което те уведомяват председателя на Държавна агенция „Електронно управление“.

- Редът за водене, съхраняване и достъп до регистъра се определя с наредбата.

- Регистърът не е публичен.

1.5. Система за киберсигурност

- Системата за киберсигурност е част от системата за защита на националната сигурност.

- Управлението и организацията на системата за киберсигурност се осъществяват от Министерския съвет. За подпомагане изпълнението на тези дейности към Министерския съвет се създава Съвет по киберсигурността.

- Министерският съвет приема с решение Национална стратегия за киберсигурност и Национална стратегия за мрежова и информационна сигурност.

1.6. Стратегии

- Националната стратегия за киберсигурност е стратегическа рамка на политиката за киберсигурност, която включва:

= цели, принципи и приоритети;

= области на действие и мерки:

а) система за киберсигурност;

б) мрежова и информационна сигурност;

в) противодействие на киберпрестъпността;

г) киберотбрана;

д) киберразузнаване;

= взаимодействие между държава, бизнес и общество;

= развитие и подобряване на регулаторната рамка;

= повишаване на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността;

= международно взаимодействие;

= кибердипломация;

= взаимодействие на техническо, оперативно и стратегическо (политическо) ниво.

- Националната стратегия за мрежова и информационна сигурност е стратегическа рамка на политиката за мрежова и информационна сигурност, която включва:

= цели и приоритети относно мрежовата и информационната сигурност;

= управленска рамка за постигане на целите и приоритетите по т. 1, включително функциите и отговорностите на държавните органи и на други участници;

= мерки във връзка с подготвеността, реагирането и възстановяването в мрежите и информационните системи, включително сътрудничеството между публичния и частния сектор;

= съществена информация за образователните и обучителните програми и програмите за повишаване на осведомеността във връзка с мрежовата и информационната сигурност;

= посочване на плановете за научноизследователска и развойна дейност относно мрежовата и информационната сигурност;

= план за оценка на риска с цел набелязване на рисковете;

= списък на различните участници в изпълнението на стратегията.

- Национална стратегия за мрежова и информационната сигурност се изготвя, когато Националната стратегия за киберсигурност не съдържа информацията стратегическата рамка.

1.7. Съвет по киберсигурност

- Съветът по киберсигурността е консултативен и координиращ орган към Министерския съвет по въпросите на киберсигурността.

- Председател на Съвета по киберсигурността е заместник министър-председател, определен от министър-председателя.

- Членове на Съвета по киберсигурността са:

= министърът на вътрешните работи;

= министърът на отбраната;

= министърът на външните работи;

= министърът на финансите;

= министърът на транспорта, информационните технологии и съобщенията;

= министърът на енергетиката;

= министърът на здравеопазването;

= министърът на околната среда и водите;

= началникът на отбраната;

= главният секретар на Министерството на вътрешните работи;

= председателят на Държавна агенция „Национална сигурност“;

= председателят на Държавна агенция „Разузнаване“;

= директорът на Служба „Военна информация“;

= началникът на Националната служба за охрана;

= председателят на Държавна агенция „Електронно управление“;

= секретарят на Съвета по киберсигурността;

= секретарят на Съвета по сигурността към Министерския съвет;

= представител на президента на републиката, изрично определен от него с указ.

- Президентът на републиката, председателят на Народното събрание и министър-председателят може да участват лично в заседанията на Съвета по киберсигурността.

- В определени случаи и по отделни въпроси в работата на Съвета по киберсигурността по покана на неговия председател може да участват председатели на постоянни комисии на Народното събрание, народни представители и ръководители на ведомства и организации.

1.8. Дейност на Съвета по киберсигурност

Съветът по киберсигурността:

- анализира тенденциите на киберзаплахите, рисковете, методите за противодействие и за развитието на необходимия капацитет, приоритетите за изграждането и развитието на човешки, технологични, инфраструктурни, финансови и организационни компоненти и при необходимост предлага решения и действия по отношение на тях;

- предлага на Министерския съвет Национална стратегия за киберсигурност и пътната карта към нея, както и изготвя периодичната им актуализация;

- предоставя информация на Съвета по сигурността към Министерския съвет относно състоянието на сигурността в киберпространството за включване в проекта на годишен доклад за състоянието на националната сигурност от Закона за управление и функциониране на системата за защита на националната сигурност;

- осъществява взаимодействие с компетентните органи в областта на киберсигурността, включително с националните компетентни органи, с Националното единно звено за контакт, с регулаторни органи и с други институции;

- дава предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото;

- предлага на Министерския съвет Национален план за управление на киберкризи;

- взаимодейства със Съвета по сигурността към Министерския съвет.

1.9. Национален координатор по киберсигурност

- Министър-председателят определя национален координатор по киберсигурността, който е и секретар на Съвета по киберсигурността.

- Националният координатор по киберсигурността:

= ръководи изготвянето и актуализирането на Националната стратегия за киберсигурност и пътната карта към нея;

= участва при изграждането и развитието на Националната координационно-организационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост;

= участва при създаването и развитието на Националния киберситуационен център, координира действията и комплексната реакция при заплаха от киберкриза и заплахи от хибриден характер;

= предлага на Съвета по киберсигурността:

а) нива за оценка на заплахата от кибератаки и киберинциденти и критерии за определянето им;

б) степени за определяне нивото на готовност за противодействие на кибератаки и киберинциденти – в зависимост от нивото на заплаха;

в) мерките, които да се предприемат при съответните степени на готовност;

= при необходимост, в състояние на повишена заплаха от кибер- или от хибриден характер, подпомага сформирането на екипи за анализ, реакция и възстановяване с участието на експерти от различни ведомства и организации;

= съдейства при планирането, подготовката и провеждането на учения в областта на киберсигурността;

= осигурява взаимодействие и подпомага дейността на секретаря на Съвета по сигурността към Министерския съвет.

1.10. Председателят на Държавна агенция „Електронно управление“

- провежда държавната политика в областта на мрежовата и информационната сигурност;
- изготвя и предлага за приемане от Министерския съвет Национална стратегия за мрежова и информационна сигурност в случаите, когато Националната стратегия за киберсигурност не съдържа информация за стратегическата рамка;
- издава методически указания и координира изпълнението на политиките за мрежова и информационна сигурност;
- удостоверява съответствието на внедряваните от административните органи информационни системи с изискванията за мрежова и информационна сигурност и упражнява контрол върху администрациите за спазване на тези изисквания;
- упражнява контрол за спазване на изискванията за мрежова и информационна сигурност на административните органи, с изключение на ведомствата и за мрежите на информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция „Национална сигурност“, Държавна агенция „Разузнаване“, Държавна агенция „Технически операции“, Служба „Военна информация“ и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи;
- осъществява проверки чрез оправомощени от него лица на информационната сигурност на определена информационна система или на предприетите от административния орган мерки и дава предписания за тяхното подобряване; в обхвата на проверките не попадат информационни системи на ведомствата и за мрежите на информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция „Национална

сигурност“, Държавна агенция „Разузнаване“, Държавна агенция „Технически операции“, Служба „Военна информация“ и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи;

- разработва методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с наредба;

- координира, организира и провежда международни и национални учения и тренировки в областта на мрежовата и информационната сигурност.

1.11. Министър на отбраната. Началник на отбраната

- Министърът на отбраната провежда държавната политика за защита и активно противодействие на кибератаки и хибридни въздействия върху системите за управление на отбраната и въоръжените сили. Министърът на отбраната организира подготовката за киберотбрана на системите за управление на страната при положение на война, военно положение и извънредно положение.

- Министърът на отбраната:

= организира изграждането и развиването на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили, включително на център за киберотбрана и тяхното ресурсно осигуряване;

= организира координацията и взаимодействието във връзка с изпълнението на поети ангажименти за колективна отбрана на споделеното киберпространство с Организацията на Северноатлантическия договор (НАТО) и Европейския съюз;

= съвместно с министъра на вътрешните работи и председателите на Държавна агенция „Национална сигурност“ и Държавна агенция „Електронно управление“:

а) изготвя допълнителни изисквания по отношение на планирането и осъществяването на мероприятията по подготовка на киберотбраната и киберустойчивостта на страната при обявяване на извънредно

положение, военно положение или положение на война и организира осъществяването на контрола за тяхното изпълнение;

б) организира изграждането, развиването и поддържането на потенциал за защита и активно противодействие, адекватно на съвременните предизвикателства и заплахи в киберпространството.

- Министърът на отбраната определя с наредба условията и реда за изграждане и поддържане на киберрезерв с цел повишаване на капацитета и способностите за киберотбрана във взаимодействие с научноизследователската и образователната общност и индустрията. Киберрезервът участва в съвместни обучения и тренировки и може да бъде включван при необходимост за решаване на практически задачи, свързани с киберотбраната.
- Началникът на отбраната:
  = организира поддържането на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили;
  = възлага интегрирането на задачите по киберотбрана като елемент от стратегическото планиране в плановете за изграждане на отбранителни способности и в плановете за операции на въоръжените сили;
  = организира и координира провеждането на международни или национални занятия, тренировки и учения в областта на киберотбраната.

1.12. Министър на вътрешните работи

- Министърът на вътрешните работи провежда държавната политика в областта на противодействието на киберпрестъпността.
- Органите на Министерството на вътрешните работи:
  = извършват оперативно-издирвателна дейност за противодействие на киберпрестъпността и произтичащите от нея заплахи за националната сигурност и за опазване на обществения ред;
  = поддържат и развиват способности за киберпревенция и защита, реакция, разследване и правоприлагане при компютърни престъпления;

= усъвършенстват организационната база и способностите на органите за разкриване и разследване на престъпни дейности в киберпространството и осъществяват взаимодействие с всички заинтересовани страни;

= осъществяват разследване при извършени компютърни престъпления, от които произтичат заплахи за националната сигурност и за опазване на обществения ред;

= извършват дейности по повишаване на информираността на обществото за съществуващи и нововъзникващи киберзаплахи и свързания с тях риск от престъпни деяния.

- В Главна дирекция „Борба с организираната престъпност“ на Министерството на вътрешните работи се изгражда:

= Център по киберпрестъпност, който осъществява дейности по разкриване, разследване и документиране на компютърни престъпления на национално ниво, и

= екип за реагиране при инциденти с компютърната сигурност за Министерството на вътрешните работи.

- В изпълнение на горепосочените дейностите Главна дирекция „Борба с организираната престъпност“ на Министерството на вътрешните работи:

= поддържа готовност за координирана, съвместна реакция с Националния екип за реагиране при инциденти с компютърната сигурност;

= подпомага разследващите органи чрез изготвяне на дигитални експертни справки на веществени доказателства;

= разполага с технически, финансови и човешки ресурси за гарантиране ефективното осъществяване на дейностите по оперативно издирване и за изграждането на центъра по киберпрестъпност.

- При уведомяване от Главна дирекция „Борба с организираната престъпност“ на Министерството на вътрешните работи предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни незабавно, когато това е технически възможно, да филтрират или преустановят зловредния

интернет трафик – източник на кибератака, към мрежи и информационни системи на субектите.

1.13. Държавна агенция „Национална сигурност“ – (ДАНС)

- Държавна агенция „Национална сигурност“ изпълнява политиката по защита от киберинциденти в комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност.

- В Държавна агенция „Национална сигурност“ се изгражда и поддържа Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност.

- Центърът изпълнява следните дейности:

= мониторинг и събиране на информация за събития и инциденти, свързани със сигурността на комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност;

= подаване на предупреждения за киберзаплахи и информация за киберинциденти към стратегическите обекти и дейности, които са от значение за националната сигурност;

= оказване на методическо съдействие в процеса на управление на киберинциденти;

= осигуряване на цялостен анализ на постъпващата информация и оценка на информационната защита на стратегическите обекти и дейности, които са от значение за националната сигурност.

= Центърът поддържа готовност за координирана съвместна реакция в рамките на Националната координационно-организационна мрежа за киберсигурност при настъпването на инциденти, свързани със сигурността на комуникационните и информационните системи на

стратегическите обекти и дейности, които са от значение за националната сигурност.

- Центърът изпълнява и задачи, свързани с функциите на Държавна агенция „Национална сигурност “.

- При уведомяване от Държавна агенция „Национална сигурност“ ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности са длъжни незабавно, когато това е технически възможно, да филтрират или преустановят зловредния интернет трафик – източник на кибератака.

1.14. Национални компетентни органи

- Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност за секторите и услугите, когато такива не са създадени със специален закон.

- Национален компетентен орган за всички административни органи, както и за лицата и организациите, е Държавна агенция „Електронно управление “.

- Националните компетентни органи:

= координират и контролират изпълнението на задачите, свързани с мрежовата и информационната сигурност на административните органи, операторите на съществени услуги и доставчиците на цифрови услуги съгласно този закон

= приемат, след съгласуване с Държавна агенция „Електронно управление “, насоки относно обстоятелствата, при които субектите са длъжни да уведомяват за инциденти.

= оценяват дали административните органи, операторите на съществени услуги и доставчиците на цифрови услуги изпълняват задълженията си по глава втора, както и въздействието на това изпълнение върху мрежовата и информационната сигурност и предприемат съответните мерки при неизпълнение

= съвместно с Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки по отношение на техническите области, които да се вземат предвид във връзка с използването на европейските или международните стандарти и спецификации от значение за мрежовата и информационната сигурност.

= със съдействието на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора.

- Националните компетентни органи гарантират, че екипите за реагиране при инциденти с компютърната сигурност получават уведомления за инциденти.

- Националните компетентни органи имат право да изискват от административните органи и от операторите на съществени услуги:

= информация, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност, резултати от одити на мрежовата и информационната сигурност, когато са извършени от друг квалифициран одитор, и доказателствата, на които те се основават

= доказателства за ефективно изпълнение на препоръките от одити на мрежовата и информационната им сигурност.

- В искането националните компетентни органи посочват целта му и уточняват каква информация или доказателства се изискват.

- След оценяването на информацията или на доказателствата съответният национален компетентен орган дава при необходимост задължителни указания за отстраняване на установените пропуски в изпълнението на изискванията.

- За целите на националните компетентни органи имат право да изискват от доставчиците на цифрови услуги да:

= предоставят информацията, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност

= отстранят всеки пропуск в изпълнението на изискванията.

- Когато получи доказателства, че даден доставчик на цифрови услуги не отговаря на изискванията, съответният национален компетентен орган предприема действия съгласно правомощията си. Тези доказателства могат да се предоставят от компетентен орган на друга държава – членка на Европейския съюз, в която доставчикът на цифрови услуги предоставя услугата.
- Националните компетентни органи имат право да изискват от екипите за реагиране при инциденти с компютърната сигурност информация.
- Националните компетентни органи оказват съдействие на Националното единно звено за контакт при изпълнение на функциите му.
- Националните компетентни органи си сътрудничат с органите за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни.
- Националните компетентни органи трябва да разполагат с технически, финансови и човешки ресурси, за да гарантират, че са в състояние да изпълняват ефективно възложените им задачи в съответствие с този закон.

1.15. Национално единно звено за контакт

- Към Държавна агенция „Електронно управление“ се създава Национално единно звено за контакт.
- Националното единно звено за контакт координира въпросите, свързани с мрежовата и информационната сигурност, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави – членки на Европейския съюз.
- Националното единно звено за контакт предоставя на всеки две години на Европейската комисия информация относно последователността на подходите за определянето на операторите на съществени услуги, която включва:

= националните мерки, чрез които са определени операторите на съществени услуги

= списък на съществените услуги

= броя на операторите на съществени услуги, определени за всеки сектор в и тяхното значение за този сектор.

= праговете, когато има такива, за определяне на минималното ниво на доставяните услуги спрямо броя ползватели, разчитащи на тях.

= значението на конкретния оператор на съществени услуги за поддържане на достатъчно ниво на услугата предвид наличието и на други възможности за предоставяне на тази услуга.

- Националното единно звено за контакт уведомява Европейската комисия за:

= обхвата на задачите на екипите за реагиране при инциденти с компютърната сигурност, както и за съществените елементи от тяхната процедура за предприемане на действия при инциденти, след тяхното създаване или при изменение на статута или процедурите им.

= приетата Национална стратегия за мрежова и информационна сигурност в тримесечен срок от приемането й.

- При трансграничен инцидент Националното единно звено за контакт уведомява националното единно звено за контакт на другата засегната държава – членка на Европейския съюз, когато е постъпило искане от Националния екип за реагиране при инциденти с компютърната сигурност.

- При случаи Националното единно звено за контакт запазва търговските интереси на оператора на съществените услуги или на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомленията им, в съответствие с българското законодателство и с правото на Европейския съюз.

- Националното единно звено за контакт представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления, естеството на инцидентите и действията, предприети за разрешаването им.

- Националното единно звено за контакт има право да изисква от националните компетентни органи информация, от Националния екип за реагиране при инциденти с компютърната сигурност.
- В случай на необходимост националните компетентни органи и Националното единно звено за контакт осъществяват сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни.

1.16. Секторни екипи за реагиране при инциденти с компютърната сигурност

- Административните органи, включително Държавна агенция „Електронно управление“, създават секторни екипи за реагиране при инциденти с компютърната сигурност. Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).
- Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания:

= да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки момент и да бъдат ясно посочени и добре известни на субектите и на партньорите.

= секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони.

= да осигуряват непрекъснатост на дейността си чрез:

а) подходяща система за управление и разпределяне на заявките;

б) достатъчен персонал, който да е постоянно на разположение;

в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение;

= изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с

указанията на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и с българското законодателство.

- Секторните екипи за реагиране при инциденти с компютърната сигурност разполагат с ресурси за ефективно изпълнение на задачите си, които включват най-малко следното:

= наблюдение на инциденти на национално равнище.

= подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните субекти.

= реакция при инциденти и оказване на методологическа помощ при разрешаване на инциденти – при поискване.

= осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация.

- Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди.

- С цел улесняване на сътрудничеството секторните екипи за реагиране при инциденти с компютърната сигурност насърчават възприемането и използването на общи практики за стандартизация за:

= процедури за предприемане на действия при инциденти и рискове.

= схеми за класификация на инциденти, рискове и информация.

- Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност, която се изгражда от секторните екипи и от Националния екип.

- Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон.

- Секторните екипи за реагиране при инциденти с компютърната сигурност изпращат веднъж на три месеца обобщена статистическа информация до Националния екип за реагиране при инциденти с компютърната сигурност относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност.

- Секторните екипи за реагиране при инциденти с компютърната сигурност, обхващащи стратегически обекти и дейности, които са от значение за националната сигурност:

= изграждат комуникационна свързаност с центъра, която се използва за подпомагане изпълнението на дейностите

= уведомяват незабавно центъра за настъпилите инциденти.

= В случаите последващи действия на субекти се координират с центъра и със съответния секторен екип за реагиране при инциденти с компютърната сигурност.

1.17. Национален екип за реагиране при инциденти с компютърна сигурност

- Към Държавна агенция „Електронно управление“ се създава Национален екип за реагиране при инциденти с компютърната сигурност, който отговаря на изискванията на секторните екипи.

- Националният екип за реагиране при инциденти с компютърната сигурност:

= действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво

= подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност

= участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност

= обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост.

= предоставя съвети и препоръки на органите на държавната власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност.

= оказва експертна подкрепа на административните органи и на други юридически лица при изграждане, внедряване и поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област.

= участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури.

= при възникване на инциденти в мрежовата и информационната сигурност дава препоръчителни указания на административните органи, на националните компетентни органи и на секторните екипи за реагиране при инциденти с компютърната сигурност.

= информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този закон, и в случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване.

= участва в международни мрежи за сътрудничество.

- Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, окажат съдействие на Националния екип за реагиране при инциденти с компютърната сигурност за отстраняване на установени от него киберинциденти в техните мрежи и/или услуги.

1.18. Сътрудничество и координация

- Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво.
- Държавна агенция „Електронно управление“ координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция „Национална сигурност“, Министерството на вътрешните работи и Министерството на отбраната.
- За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят със споразумение за взаимодействие между заинтересованите ведомства.
- За координиране на дейностите за реакция при кибератаки и мащабни инциденти председателят на Държавна агенция „Електронно управление“ може да създава междуведомствени оперативни групи с участието на ведомства, организации и институции, включително от частния сектор, имащи отношение към тези дейности.
- Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност – в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност.

Глава II – Мрежова и информационна сигурност[3]

2. Задължения на административните органи

по отношение на изискванията за сигурност и уведомяване за инциденти

- Административните органи осигуряват и отговарят за сигурността на използваните от тях мрежи и информационни системи.
- Административните органи предприемат:

= подходящи и пропорционални мерки, които трябва да осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск.

= подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на дейността им.

= мерките, определени с наредба.

- Административните органи уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност.
- Първоначално уведомяване се прави до два часа след констатирането на инцидента. Уведомленията се подават по образец съгласно наредба и съдържат информация, която дава възможност на секторния екип да определи евентуалното трансгранично въздействие на инцидента.
- В срок до 5 работни дни административният орган предоставя на секторния екип пълната информация за инцидента, определена с наредба.
- При наличие на обосновано предположение, че докладваният инцидент може да се класифицира като компютърно престъпление, секторният екип уведомява Главна дирекция „Борба с организираната престъпност“ на Министерството на вътрешните работи.
- Секторният екип запазва поверителността на информацията, съдържаща се в уведомленията.

[3] https://www.youtube.com/СДВР Столична Полиция Киберпрестъпност

- Задължения на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, по отношение на изискванията за сигурност и уведомяване за инциденти.

= Лицата и организациите осигуряват и отговарят за мрежовата и информационната си сигурност при предоставянето на административни услуги по електронен път.

= Лицата и организациите уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път.

= Секторният екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на лицата и организациите, както и поверителността на информацията, съдържаща се в уведомленията им.

- Задължения на операторите на съществени услуги по отношение на изискванията за сигурност и уведомяване за инциденти.

= Операторите на съществени услуги предприемат:

а) подходящи и пропорционални мерки, които трябва да осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск.

б) подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на предоставяните от тях съществени услуги;

= Операторите на съществени услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях съществени услуги.

= Когато оператор на съществени услуги разчита на доставчик на цифрови услуги, за да предоставя съществена услуга, операторът уведомява доставчика

на цифрови услуги за всяко значително увреждащо въздействие върху непрекъснатостта на съществената услуга, дължащо се на инцидент, засягащ доставчика на цифрови услуги.

= Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на оператора на съществени услуги, както и поверителността на информацията, съдържаща се в уведомлението му.

2.1. Предоставяне на информация[4]

- Съответният екип за реагиране при инциденти с компютърната сигурност при поискване предоставя на подалия уведомление за инцидент административен орган, лице или организация и оператор на съществени услуги съответната информация във връзка с последващите действия по уведомлението, включително информация, която би спомогнала за предприемането на ефективни действия при инцидента.
- След консултация със съответния субект, подал уведомлението, съответният екип за реагиране при инциденти с компютърната сигурност може да информира обществеността за отделни инциденти, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент.

2.2. Задължения на доставчиците на цифрови услуги

по отношение на изискванията за сигурност и уведомяване за инциденти

- Доставчиците на цифрови услуги предприемат:

= подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тях при предоставянето на услуги на територията на Република България;

= подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им

[4] Закон за киберсигурност

сигурност, върху предоставяните от тях услуги на територията на Република България, с цел осигуряване на непрекъснатост на тези услуги;

- Осигуряване на мерки и ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск, като са съобразени със:

= сигурността на системите и съоръженията;

= действията при инциденти;

= управление на непрекъснатостта на дейностите;

= наблюдение, одит и изпитване;

= спазване на международни стандарти.

- Доставчиците на цифрови услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях цифрови услуги.

- За определяне на въздействието на даден инцидент като съществено се вземат предвид:

= броят ползватели, засегнати от инцидента, и по-специално ползвателите, които разчитат на услугата за предоставяне на собствените си услуги;

= продължителността на инцидента;

= географският обхват по отношение на областта, засегната от инцидента;

= степента на нарушаване на функционирането на услугата;

= степента на въздействие върху стопанските и обществените дейности.

- Доставчиците на цифрови услуги подават уведомление само когато имат достъп до информацията, която е необходима, за да се оцени въздействието на инцидента като съществено.

- След консултация със засегнатия доставчик на цифрови услуги съответният секторен екип за реагиране при инциденти с компютърната сигурност и когато е приложимо, органите или екип за реагиране при инциденти с компютърната сигурност на други засегнати държави – членки на Европейския съюз, може да информират обществеността за отделни инциденти или да изискат от доставчика

на цифрови услуги да информира за това, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент или когато разкриването на инцидента е в интерес на обществеността поради други причини.

- Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомлението му.

2.3. Юрисдикция и териториалност

по отношение на доставчик на цифрови услуги

- Когато доставчик на цифрови услуги има седалище и адрес на управление или представител в Република България, но неговите мрежи и информационни системи са разположени в една или повече други държави – членки на Европейския съюз, съответният национален компетентен орган и компетентните органи на другите държави си сътрудничат и се подпомагат взаимно, ако е необходимо. Помощта и сътрудничеството може да включват обмен на информация между съответните компетентни органи и искания за предприемане на действия.

- Доставчик на цифрови услуги, който не е установен в държава – членка на Европейския съюз, но предлага в Европейския съюз услуги, определя свой представител в Европейския съюз. Представителят трябва да е установен в една от държавите – членки на Европейския съюз, в които се предлагат услугите. Когато представителят е със седалище и адрес на управление в Република България, се приема, че доставчикът на цифрови услуги е под юрисдикцията на Република България.

- Определянето на представител от доставчика на цифрови услуги не засяга съдебните производства, които биха могли да бъдат започнати срещу самия доставчик на цифрови услуги.

2.4. Уведомяване за инциденти

от субекти извън посочените административните органи, операторите на съществени услуги и доставчиците на цифрови услуги, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги.

- Субекти извън горепосочените може да уведомяват секторните екипи за реагиране при инциденти с компютърната сигурност за инциденти, които имат въздействие върху непрекъснатостта на предоставяните от тях услуги.
- При обработването на уведомленията секторните екипи за реагиране при инциденти с компютърната сигурност действат съгласно съответните разпоредби на тази глава, като уведомленията на горепосочените субектите се обработват с предимство пред уведомленията по извън горепосочените.
- Уведомленията се обработват само когато това не представлява несъразмерна или неоправдана тежест.

3. Административно наказателни разпоредби

3.1. Отговорност за нарушения, свързани с уведомяване за инциденти

- Административен орган, който не уведоми или уведоми след срока секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на неговата дейност, както и когато уведомлението не съдържа достатъчно информация, в случай че деянието не съставлява престъпление, се наказва с глоба от 1000 до 10 000 лв.
- При повторно нарушение наказанието е глоба от 2000 до 20 000 лв.
- На лице или организация, която не уведоми или уведоми след срока секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път, както и когато уведомлението не съдържа достатъчно информация в случай че деянието не съставлява престъпление, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

- При повторно нарушение глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв.

- Глобите и имуществените санкции се налагат и на оператор на съществени услуги, който не уведоми или уведоми след срока съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от него съществени услуги, както и когато уведомлението не съдържа достатъчно информация, в случай че деянието не съставлява престъпление.

- Глобите и имуществените санкции се налагат и на доставчик на цифрови услуги, който не уведоми или уведоми след срока съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има съществено въздействие върху непрекъснатостта на предоставяните от него цифрови услуги, както и когато уведомлението не съдържа достатъчно информация, в случай че деянието не съставлява престъпление.

3.2. Отговорност за не предоставяне на информация

или неизпълнение на указания.

- Административен орган, който не предостави информацията и доказателствата или не изпълни задължителни указания, се наказва с глоба от 1000 до 10 000 лв.

- При повторно нарушение наказанието е глоба от 2000 до 20 000 лв.

- Когато деянието е извършено от оператор на съществени услуги, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

- При повторно нарушение глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв.

- Глобите и имуществените санкции се налагат и на доставчик на цифрови услуги, който не предостави информацията или не отстрани пропуск.

3.3. Отговорност за други нарушения

- Длъжностно лице, което извърши или допусне извършването на друго нарушение по мрежова и информационна сигурност, се наказва с глоба от 1000 до 10 000 лв., освен ако деянието не съставлява престъпление.

- При повторно нарушение наказанието е глоба от 1500 до 15 000 лв.

- На лице, което не изпълни свое, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

3.4. Установяване на нарушенията

издаване, обжалване и изпълнение на наказателните постановления.

- Актовете за установяване на нарушения, извършени от административни органи, се съставят от длъжностни лица, определени от председателя на Държавна агенция „Електронно управление“.

- Актовете за установяване на нарушения, извършени от оператори на съществени услуги или от доставчици на цифрови услуги, се съставят от длъжностни лица, определени от ръководителите на административните органи.

- Актовете за установяване на нарушения се съставят от длъжностни лица, определени от министъра на вътрешните работи.

- Актовете за установяване на нарушения се съставят от длъжностни лица, определени от председателя на Държавна агенция „Национална сигурност“.

- Наказателните постановления се издават от:

= председателя на Държавна агенция „Електронно управление“ или от изрично оправомощени от него длъжностни лица;

= ръководителите на административните органи или от изрично оправомощени от тях длъжностни лица;

= министъра на вътрешните работи или от изрично оправомощени от него длъжностни лица;

= председателя на Държавна агенция „Национална сигурност“ или от изрично оправомощени от него длъжностни лица.

- Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на закона за административните нарушения и наказания.

Глава III – Киберзаплахи и киберпрестъпност[5]

4. Хронология

ЕС работи на различни фронтове за насърчаване на устойчивостта на киберпространството, борба с киберпрестъпността и укрепване на кибердипломацията и киберотбраната.[6]

-Отговор на ЕС на предизвикателствата, свързани с киберсигурността:

= Критичните сектори като транспорта, енергетиката, здравеопазването и финансите стават все по-зависими от цифровите технологии, за да осъществяват основната си дейност. Цифровизацията предоставя огромни възможности и предлага решения за много от предизвикателствата, пред които е изправена Европа, но не трябва да се пренебрегва и фактът, че по време на кризата с COVID-19 тя излага икономиката и обществото на киберзаплахи.

= Съветът приема заключения относно рамка за координиран отговор на ЕС на хибридни кампании - 23/05/2022

= Киберпространство: Съветът постига съгласие за укрепване на киберсигурността в ЕС и предотвратяване на кибератаки:

- 16/05/2022 Кибератаки: Съветът удължава режима на санкциите
- 13/05/2022 Укрепване на киберсигурността и устойчивостта в целия ЕС – споразумение относно Директивата за МИС 2
- 11/05/2022 Акт за оперативната устойчивост на цифровите технологии (DORA): постигнато е предварително споразумение

Броят и сложността на кибератаките и киберпрестъпността се увеличават в цяла Европа. Тази тенденция ще продължи да се засилва в бъдеще, тъй като до 2024 г. се очаква 22,3 милиарда устройства в световен мащаб да бъдат свързани с интернета на предметите.

[5] https://www.consilium.europa.eu/bg/policies/cybersecurity/

[6] https://trud.bg/Явор Колев 10.05.2019

4.1. Активизиране в областта на киберсигурността

с цел изграждане на отворено и сигурно киберпространство може да създаде по-голямо доверие сред гражданите в цифровите инструменти и услуги.

През октомври 2020 г. лидерите от ЕС призоваха за засилване на способността на ЕС:

- да се защитава от киберзаплахи
- да осигурява сигурна комуникационна среда, особено чрез квантово криптиране
- да гарантира достъп до данни за целите на съдебните и правоприлагащите органи

Извънредно заседание на Европейския съвет, 1–2 октомври 2020 г.

Цифрово бъдеще за Европа (обща информация)

Европа, устойчива на кибератаки

Стратегия на ЕС за киберсигурност

През декември 2020 г. Европейската комисия и Европейската служба за външна дейност (ЕСВД) представиха нова стратегия на ЕС за киберсигурност. Целта на тази стратегия е да се засили устойчивостта на Европа срещу киберзаплахи и да се гарантира, че всички граждани и предприятия могат да се възползват в пълна степен от надеждни услуги и цифрови инструменти. Новата стратегия съдържа конкретни предложения за въвеждане на регулаторни, инвестиционни и политически инструменти.

На 22 март 2021 г. Съветът прие заключения относно Стратегията за киберсигурност, в които подчерта, че киберсигурността е от съществено значение за изграждането на устойчива, екологична и цифрова Европа. Министрите от ЕС определиха като основна цел постигането на стратегическа автономност при същевременно запазване на отворената икономика. Това включва укрепване на способността да се вземат автономни решения в областта на киберсигурността с цел утвърждаване на водещите позиции на ЕС в сферата на цифровите технологии и повишаване на неговия стратегически капацитет.

Съветът приема заключения относно Стратегията на ЕС за киберсигурност (съобщение за медиите, 22 март 2021 г.)

4.2. Законодателни предложения на ЕС

за справяне с настоящите и бъдещите рискове онлайн и офлайн:

- актуализирана директива за по-добра защита на мрежите и информационните системи
- нова директива относно устойчивостта на критичните субекти

Стратегия на ЕС за киберсигурност (Европейска комисия)

Стратегия на ЕС за киберсигурност (Европейска служба за външна дейност)

4.3. Какво представлява киберсигурността

Киберсигурността включва дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на тези мрежи и системи и на други лица, засегнати от киберзаплахи.

Актът на ЕС за киберсигурността влезе в сила през юни 2019 г. и въведе:

- общоевропейска схема за сертифициране нов и по-засилен мандат за Агенцията на ЕС за киберсигурност
- Общоевропейска схема за сертифициране

Сертифицирането играе решаваща роля за гарантирането на високи стандарти за киберсигурност за ИКТ продукти, услуги и процеси. Фактът, че понастоящем различните държави от ЕС използват различни схеми за сертифициране на сигурността създава разпокъсаност на пазара и регулаторни пречки.

С Акта за киберсигурността ЕС въведе единна рамка за сертифициране в целия ЕС, която ще спомогне за:

- изграждане на доверие
- увеличаване на растежа на пазара на киберсигурността
- улесняване на търговията в целия ЕС

Рамката ще осигури цялостен набор от правила, технически изисквания, стандарти и процедури.

Схема на ЕС за сертифициране на киберсигурността (ЕК)

Пазар на ЕС в областта на киберсигурността

Европейските държави заемат 18 от първите 20 места в световния индекс за киберсигурност

Стойността на пазара на ЕС в областта на киберсигурността се оценява на над 130 милиарда евро и нараства със 17 % годишно.

ЕС разполага с над 60 000 дружества в областта на киберсигурността и над 660 центрове за експертни познания в областта на киберсигурността

4.4. Агенция на ЕС за киберсигурност

Новата Агенция на ЕС за киберсигурност се основава на структурите на своя предшественик — Агенцията на Европейския съюз за мрежова и информационна сигурност, но със засилена роля и постоянен мандат. Тя прие и същото съкращение (ENISA).

Агенцията подпомага държавите членки, институциите на ЕС и други заинтересовани страни в борбата с кибератаките.

Агенция на Европейския съюз за киберсигурност (https://www.consilium.europa.eu/)

4.5. Директива за мрежовите и информационните системи

Директивата за сигурността на мрежите и информационните системи (МИС) беше представена през 2016 г. като първата по рода си общоевропейска законодателна мярка за подобряване на сътрудничеството между държавите членки по изключително важния въпрос за киберсигурността. С тази директива бяха установени задължения по отношение на сигурността за операторите на основни услуги (в особено важни сектори като енергетиката, транспорта, здравеопазването и финансите), както и за доставчиците на цифрови услуги (онлайн места за търговия, търсачки и услуги „в облак“).

През декември 2020 г. Европейската комисия предложи преработена директива за МИС (МИС2), която да замени директивата от 2016 г. Новото предложение е в отговор на променящото се естество на заплахите и отчита цифровата трансформация, която беше ускорена от кризата с COVID-19.

4.6. Нов законодателен акт на Съвета и Европейският парламент

постигнаха предварително споразумение по новите мерки през май 2022 г:

- ще се осигури по-добро управление на риска и инцидентите и по-тясно сътрудничество
- ще се разшири обхватът на правилата
- Укрепване на киберсигурността и устойчивостта в целия ЕС – предварително споразумение между Съвета и Европейския парламент (съобщение за медиите, 13 май 2022 г.)

Предложение за преразгледана директива относно сигурността на мрежите и информационните системи (Европейска комисия)

4.7. Живот онлайн

как ЕС го прави по-лесен и по-безопасен за вас?

ЕС работи активно за подобряване на цифровата среда в полза на всички европейци. „Цифровият“ ни живот трябва да бъде безопасен, лесен и зачитащ основните свободи.

4.8. Борба на ЕС с киберпрестъпността

Киберпрестъпността приема различни форми и много от често срещаните престъпления се улесняват от киберпространството. Например престъпниците могат:

- да придобият контрол върху лични устройства, използващи зловреден софтуер
- да откраднат или компрометират лични данни и интелектуална собственост с цел извършване на онлайн измами
- да използват интернет и платформи на социалните медии за разпространение на незаконно съдържание
- да използват даркнет за продажба на незаконни стоки и хакерски услуги
- Някои форми на киберпрестъпност, като сексуалната експлоатация на деца онлайн, причиняват сериозни вреди на техните жертви.

В рамките на Европол беше създаден специализиран Европейски център за борба с киберпрестъпността, който да помага на държавите от ЕС да разследват престъпленията онлайн и да разбиват престъпните мрежи.

4.9. Европейски център за борба с киберпрестъпността (Европол)

Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT) е инициатива на държавите членки в областта на сигурността за идентифициране, приоритизиране и справяне със заплахите, породени от организираната международна престъпност. Противодействието на кибератаките е един от нейните приоритети.

Борба на ЕС с организираната престъпност (обща информация)

4.10. Действия срещу измамите с непарични платежни средства

Измамите и подправянето на непарични платежни средства представляват сериозна заплаха за сигурността на ЕС и осигуряват значителни приходи за организираната престъпност. Освен това този вид измами засягат доверието на потребителите в сигурността на цифровите технологии.

През април 2019г. ЕС прие нови правила за борба с измамите с непарични плащания. Държавите членки следва да транспонират новите правила през 2021г. ЕС установява по-строги правила за борба с измамите с непарични плащания (от 9 април 2019г.)

4.11. Подобряване на безопасността на децата в онлайн среда

През май 2022 г. Европейската комисия предложи ново законодателство за борба със сексуалното насилие над деца и сексуалната експлоатация на деца онлайн. Новите правила понастоящем се обсъждат в Съвета.

Междувременно ЕС прие временни правила, като дерогация от чл.5, параграф 1 и член 6, параграф 1 от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, за да се даде възможност на доставчиците на уеб базирани услуги за електронна поща и съобщения да продължат да разкриват сексуално насилие над деца онлайн.

През май 2021 г. преговарящите от Съвета и Европейския парламент постигнаха предварително споразумение за временните мерки, които позволяват на доставчиците на електронни съобщителни услуги, като уеб базирани услуги за електронна поща и изпращане на съобщения, да продължат да разкриват, премахват и сигнализират за онлайн материали, съдържащи сексуално насилие над деца, както и да прилагат технологии за предотвратяване на сприятеляването с деца със сексуална цел, докато бъде приета трайна законодателна уредба. Мерките влязоха в сила през август 2021 г. и срокът им на действие ще изтече през 2024 г.

4.12. Борба с насилието над деца онлайн

Сексуално насилие над деца (ЕК). Правосъдие и правоприлагане.

Правилата и политиките на ЕС са насочени и към други аспекти на борбата с киберпрестъпността и престъпността като цяло, свързани с правосъдието и правоприлагането, като например достъпа до електронни доказателства, криптирането и запазването на данни.

4.13. Достъп до електронни доказателства

Престъпниците използват цифровите технологии, за да извършват престъпления и да прикриват незаконни дейности. Поради това правоприлагащите и съдебните органи разчитат все повече на електронни доказателства, като например текстове, имейли или приложения за съобщения, за целите на своите наказателни разследвания и преследвания.

Ето защо ЕС работи по нови правила, които ще улеснят и ускорят трансграничния достъп до електронни доказателства.

По-добър достъп до електронни доказателства за борба с престъпността.

За да се улесни допълнително трансграничният достъп до електронни доказателства за целите на наказателното производство, ЕС:

- води преговори по споразумение със САЩ – страната, в която се намират повечето доставчици на услуги

- участва в преговорите по втория допълнителен протокол към Конвенцията от Будапеща

Съветът предоставя на Комисията мандат за водене на преговори по международни споразумения относно електронни доказателства по наказателно-правни въпроси (6 юни 2019 г.)

4.14. Криптиране

ЕС се стреми към активна дискусия с технологичния сектор, за да бъде постигнат правилният баланс между осигуряването на непрекъснатото използване на стабилни технологии за криптиране и гарантирането на правомощията на правоприлагащите и съдебните органи да работят при същите условия, както в офлайн пространството.

През декември 2020 г. Съветът прие резолюция относно криптирането, в която се подчертава необходимостта от сигурност както чрез криптиране, така и въпреки него.

Съветът приема резолюция относно криптирането (14.12.2020 г.)

За да се противодейства ефективно на престъпността в наши дни, е важно доставчиците на услуги да запазват определени данни, които могат да бъдат разкривани при определени строги условия за целите на борбата с престъпността. Запазването на данни обаче може да нарушава индивидуални основни права, по-специално правото на неприкосновеност на личния живот и защита на личните данни.

Съветът прие заключения относно запазването на данни от електронни комуникации за целите на борбата с престъпността. Съветът възложи на Комисията да събере допълнителна информация и да организира целеви консултации като част от всеобхватно проучване на възможните решения за запазването на данни, включително разглеждане на възможността за бъдеща законодателна инициатива.

Запазване на данни за целите на борбата с престъпността: Съветът приема заключения (6 декември 2019 г.)

4.15. Засилване на кибердипломацията

Европейският съюз и неговите държави членки силно насърчават изграждането на отворено, свободно, стабилно и сигурно киберпространство, в което правата на човека, основните свободи и принципите на правовата държава се зачитат напълно за целите на социалната стабилност, икономическия растеж, просперитета и целостта на свободните и демократични общества.

ЕС полага много усилия, за да се защити от киберзаплахи, идващи от трети държави, особено чрез съвместен дипломатически отговор, наречен „инструментариум за кибердипломация“. Този отговор включва дипломатическо сътрудничество и диалог, превантивни мерки срещу кибератаки и санкции.

Стратегията на ЕС за киберсигурност, приета от Европейската комисия и ЕСВД през декември 2020 г., укрепва дипломатическата реакция на ЕС на кибератаки.

4.16. Санкции срещу кибератаки

През 2019 г. Съветът създаде рамка, която позволява на ЕС да налага целенасочени санкции за възпиране и противодействие на кибератаки, представляващи външна заплаха за Съюза или за неговите държави членки.

По-специално рамката позволява на ЕС за първи път да налага санкции на лица или образувания, които са отговорни за извършването на кибератаки или опити за кибератаки, които предоставят финансова, техническа или материална помощ за извършването на такива атаки или които участват в тях по друг начин. Могат да се налагат санкции и на други лица или образувания, които са свързани с тях.

4.17. Ограничителните мерки включват

- забрана за пътуване на лица до ЕС
- замразяване на активи на лица и образувания

Първите по рода си санкции за кибератаки бяха наложени на 30.07.2020 г.

Кибератаки: Съветът вече може да налага санкции (17 май 2019 г.)

Санкции: как и кога ЕС приема ограничителни мерки (обща информация)

4.18. Сътрудничество в областта на киберотбраната

Киберпространството се счита за петата област на военни действия, съпоставима по важност за военните операции със сушата, морето, въздуха и космоса. Това е област, обхващаща всичко от информационните и телекомуникационните мрежи, инфраструктурата и данните, които те поддържат, до компютърните системи, процесорите и контролерите.

ЕС, заедно с Агенцията на ЕС за киберсигурност и Европол, сътрудничи в дейностите на Европейската агенция по отбрана (EDA) в областта на киберотбраната. EDA подкрепя държавите членки в изграждането на квалифицирана военна работна сила в областта на киберотбраната и гарантира наличието на проактивни и реактивни технологии за киберотбрана.

4.19. Стратегията на ЕС за киберсигурност

приета през декември 2020 г. от Комисията и ЕСВД, засилва:

- координацията в областта на киберотбраната
- сътрудничеството и изграждането на способности за киберотбрана
- Финансиране и научни изследвания

4.20. План за възстановяване

Киберсигурността е един от приоритетите на ЕС в отговор на пандемията от COVID-19, по време на която се наблюдава увеличаване на кибератаките. Планът включва допълнителни инвестиции в тази област.

План за възстановяване на Европа (обща информация)

„Хоризонт Европа“

От решаващо значение е да се намират новаторски решения, които могат да ни защитават срещу най-новите и най-усъвършенствани киберзаплахи. Поради тази причина киберсигурността е важна част от рамковите програми на ЕС за финансиране на научните изследвания и иновациите — „Хоризонт 2020 “ и нейния приемник „Хоризонт Европа“.

През май 2020 г. ЕС задели 49 милиона евро за засилване на иновациите в областта на киберсигурността и системите за неприкосновеност на личния живот. „Хоризонт Европа“ (ЕК) и „Цифрова Европа“.

В рамките на програмата „Цифрова Европа“ за периода 2021—2027 г. ЕС пое ангажимент да инвестира 1,6 милиарда евро в капацитет за киберсигурност и широко внедряване на инфраструктури и инструменти за киберсигурност в целия ЕС в полза на публичните администрации, предприятията и гражданите.
Програма „Цифрова Европа“ — неформално споразумение с Европейския парламент (14 декември 2020 г.)

Европа инвестира в цифрови технологии: програма „Цифрова Европа“
Център за експертни познания в областта на киберсигурността
През декември 2020 г. Съветът и Европейският парламент постигнаха неформално споразумение по предложението за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове, които да го подкрепят.
През април 2021 г. Съветът прие регламента за създаване на центъра и мрежата.

4.21. Експертен център в областта на киберсигурността

със седалище в Букурещ получава зелена светлина от Съвета (20 април 2021 г.)
Новият център има за цел:

- да подобри допълнително киберустойчивостта
- да допринася за внедряването на най-новите технологии за киберсигурност
- да подкрепя стартиращи предприятия и МСП в сектора на киберсигурността
- да усъвършенства научните изследвания и иновациите в областта на киберсигурността
- да допринася за преодоляване на недостига на умения в областта на киберсигурността

Букурещ беше избран от държавите — членки на ЕС, за седалище на новия център. Избор на седалище на Центъра на ЕС за експертни познания в областта на киберсигурността.

4.22. Сигурни свързани устройства на критичната инфраструктура

Свързаните устройства, включително машини, сензори и мрежи, съставляващи интернета на предметите, както и тяхната сигурност, ще играят ключова роля в по-нататъшното изграждане на цифровото бъдеще на Европа.

През декември 2020 г. Съветът прие заключения, в които се отчитат увеличеното използване на потребителски продукти и промишлени устройства, свързани с интернет, и произтичащите от това нови рискове за неприкосновеността на личния живот, сигурността на информацията и киберсигурността.

В заключенията се определят приоритети за разрешаване на този ключов въпрос и за повишаване на глобалната конкурентоспособност на сектора на интернета на предметите в ЕС чрез осигуряване на най-високите стандарти за устойчивост, безопасност и сигурност.

Киберсигурност на свързаните устройства — Съветът приема заключения (2 декември 2020 г.)

4.23. Защита на 5G мрежите

5G мрежите са от решаващо значение не само за цифровата комуникация, но и за критичните сектори като енергетиката, транспорта, банковото дело и здравеопазването. Следователно гарантирането на устойчивостта на 5G мрежите е от съществено значение за нашето общество.

Предвид на това, че се очаква през 2025 г. приходите от 5G мрежите в световен мащаб да достигнат 225 милиарда евро, те са ключов фактор за конкурентоспособността на Европа на световния пазар, а тяхната киберсигурност е от съществено значение за гарантиране на стратегическата автономност на Съюза.

През януари 2020 г. ЕС постигна съгласие по инструментариум за определяне на евентуален общ набор от мерки за смекчаване на основните рискове за киберсигурността на 5G мрежите и за предоставяне на насоки.

Сигурни 5G мрежи: въпроси и отговори относно инструментариума на ЕС Значение и рискове за сигурността на 5G технологията – Съветът приема заключения (3 декември 2019 г.)

5. Киберпрестъпност[7]

5.1. Заплаха от киберпрестъпления

нараства с всеки изминал ден. Какво ни дебне в необятното пространство на интернет. Адекватни мерки ли е предприел българският бизнес срещу онлайн измамите. Можем ли да се защитим и как да не станем жертва на хакери. За престъпленията в интернет пространството и как да се предпазим от тях:

- Интернет престъпленията вече придобиват колосални размери. Щетите са за милиарди в целия свят, а схемите на киберпрестъпниците може да се формулират, както следва:

- Киберпрестъпленията са едни от най-динамично развиващите се и иновативни престъпления, поради техните необичайни начини и методи за извършване. В днешното информационно общество заплахата от киберпрестъпления нараства с всеки изминал ден. Ето защо правоприлагащите органи и организации в световен аспект полагат много усилия и влагат значителни ресурси, за да гарантират своята киберсигурност. Изключително разпространени към днешна дата са интернет измамите, фишингът, spear фишингът, кражбата на лични данни в интернет, ползването на злонамерен софтуер. Напоследък зачестяват измамите, извършвани посредством онлайн платформи за търговия с платежни инструменти и/или бинарни опции, криптовалута и редица други. Фишингът е непрекъсната заплаха, а рискът е още по-голям в социални медии като Facebook, Twitter и Google+. Хакерите могат да създадат клонинг на един сайт и да го представят за истински. Целта е потребителите да въведат лична информация.

[7] https://www.consilium.europa.eu/bg/policies/cybersecurity/

Така хакерите придобиват лична информация - пароли, потребителски имена, кодове за сигурност, както и номера на кредитни карти и евентуално нанасят щети на потребител или фирма. Щетите, причинени от фишингът, варират от отказ на достъп до електронна поща, до значителни финансови загуби. Съществуващите защитни механизми могат да бъдат от полза. Чрез тях може да бъде намален рискът от посегателства върху личното киберпространство, както и да се ограничат щетите от евентуални киберпрестъпления.

Като пряко въздействие върху българския бизнес и интернет потребителите в страната имат най-вече атаките с криптолокър. Към фишинг имейл е прикачен зловреден код, който криптира всички важни потребителски данни, като се иска откуп в дигитална валута Биткойн. Жертви на подобни киберпрестъпления са родни компании от всякакъв калибър. Изключение не правят и правителствени и неправителствени организации, министерства, училища и т.н. Важен момент при тези атаки е тяхното високо ниво на латентност/скритост. Бизнесът в повечето случаи не желае да докладва на компетентните органи, че е жертва на киберпрестъпление, под страх от загуба на репутация, клиенти и партньори. В тази връзка българските компании в момента са неподготвени за широк кръг от кибератаки. Важен компонент от тази ситуация е липсата на достатъчна информираност у висшия мениджърски състав за съвременните киберзаплахи и необходимостта от детайлен риск анализ, инвестиция в компетентен IT ресурс и обучение на персонала на всички нива, по въпросите на киберсигурността. Не са редки случаите, в които представители на IT отделите на български компании от всякакъв мащаб допускат наивни грешки, довеждащи до загуби за хиляди и стотици хиляди лева. Често се срещаме с неправилно конфигурирани информационни ресурси, не обновени(update) операционни системи и приложения, липса на надеждни антивирусни продукти. Или служители, отговорни за разплащанията, си предоставят паролата за служебната поща след фишинг мейл, не са деактивирани профили или не са сменени пароли след напускане на конкретен служител и т.н.

Почти всяка седмица в отдел „Киберпрестъпност“ при ГДБОП-МВР се явява представител на пострадала българска фирма от компрометирана служебна комуникация. Хакери придобиват достъп до комуникация с чуждестранен контрагент и в подходящ момент променят банковите детайли, където да се преведат парите. По тази схема имаме български компании ощетени средно с 20-30 хиляди евро на случай. Най-голямата подобна щета, която разследваме, е за един милион лева. Както всички знаем - няма сто процентова сигурност и защита, но при желание и воля от ръководния състав на фирмата се постигат завидни резултати.

Всички отговорни мениджъри - осъзнават предизвикателствата на съвременния киберсвят, инвестират в компетентен IT персонал и обучавайте всичките си служители.

5.2. Мерки необходими за предпазване от киберпрестъпността

Нещата, за които трябва да внимават българските мениджъри по сигурността са прекалено много. Атаките наистина се усъвършенстват и зачестяват. Бъдещата киберкартина не изглежда никак розова. Защитена среда се гради и постига с качествен и обучен персонал. Това естествено е свързано най-вече с възнаграждението и допълнителните условия на труд. В България на IT отделите се гледа най-често като на спомагателна дейност, в която няма нужда да се инвестира или да се привличат нови и кадърни хора. Техниката е настроена, служителите работят монотонно и само някой „капризен“ принтер веднъж месечно създава проблеми. Огромна част от компании, обаче не подозират, че в мрежата им от месеци са се загнездили хакери, който четат кореспонденцията на мениджърския състав и търпеливо планират своя удар. А той може да се избегне, ако в IT отдела са налични служители, които следят и анализират логовете на мейл сървъра, събитията в домейна, мрежата и на отделни крайни компютри. Много компании предпочитат да загубят няколко десетки хиляди евро еднократно, отколкото да инвестират в хора. Но по-важен е обученият, компетентен и качествено мотивиран персонал. Неговото наличие е гаранция за

надежден работен процес, бърза и адекватна реакция. Наскоро стана ясно, че България е била логистичен център за киберизмами за т. нар. бинарни опции. Бинарните опции са улеснен начин да се залага на ценови разлики на глобални пазари, т.е. най-често дава възможност инвеститор да подкрепи поскъпването или поевтиняването на даден актив или валута в рамките на определен времеви период. Инвеститорите реално залагат при инвестиционен брокер, че даден актив или валута ще поскъпне или поевтинее. Всички лицензирани инвестиционни посредници са посочени в електронната страница на Комисията за финансов надзор. Следва да се проверява винаги легитимността и квалификацията на инвестиционния посредник. Според Закона за пазарите на финансови инструменти инвестиционния посредник изпълнява услуги за сметка на клиента въз основа на писмен договор с него. Инвестиционният посредник е длъжен да предоставя информация на клиента си по начин, който му позволява да разбере естеството и рисковете на инвестиционната услуга, както и на предлагания финансов инструмент. Инвестиционният посредник не може да съхранява при себе си паричните средства на своите клиенти. Измамите се извършват посредством платформи за търговия с „финансови инструменти“ или „бинарни опции“, като на „инвеститорите“ са обещавани големи печалби. Престъпната дейност се осъществява по следния начин: първо се провежда кампания в рекламиране на онлайн платформа за търговия с „финансови инструменти“. След рекламата на платформата, чрез кол центрове, ситуирани в България се набират клиенти (инвеститори), които биват въвеждани в заблуждение да инвестират в търговия с финансови инструменти. Чрез създадените акаунти на клиенти на горепосочените платформи, „инвеститорите“ след превод на определени суми, започват да виждат как вложените от тях суми започват да се „покачват“. Извършителите на измамата увещават клиентите да извършат допълнителни инвестиции, за да може печалбата да се увеличи. Процесът на инвестиране продължава до момента, докато не се изразходят всички възможности на клиентите, след което извършителите на престъплението обявяват, че всички

инвестирани от тях средства са загубени по различни причини, вследствие на което комуникацията се преустановява. Разпространението или продажбата на бинарни опции на инвеститори на дребно се забранява напълно на територията на ЕС.

5.3. Най-често срещани жертви на измамните схеми в интернет

Интернет, мобилните телефони и компютърните технологии свързват хората и бизнеса. От друга страна обаче, те предоставят безброй много възможности на киберпрестъпниците да експлоатират слабостите - бъгове в сайта ви, използване на неподходяща парола, незащитеност на личните ви данни. 2/3 от потребителите на Интернет по целия свят стават жертви на киберпрестъпления и понякога, цената която плащат е твърде висока. Най-много пострадали има в Китай, където 83% от сърфиращите в мрежата стават жертви на тежки компютърни вируси, кражби на самоличност, измами с кредитни карти и други престъпления. На второ и трето място са Бразилия и Индия, където 76% от потребителите на Интернет биват измамени. За да се предпазите от онлайн престъпления, можете да следвате няколко прости правила: Използвайте антивирусна програма или софтуер, ако някое съобщение във вашата входяща поща или прикачен файл в него ви изглежда съмнително, по-добре не го отваряйте. Използвайте винаги различни потребителски имена и пароли за отделните сайтове. Не използвайте онлайн банкиране или сайтове, свързани с финансите ви, през публични и несигурни Wi-Fi връзки. Пазарувайте онлайн само през проверени и познати сайтове.

Използвайте отделен имейл акаунт за важните неща и втори акаунт за социални медии и онлайн пазаруване. Никога не изпращайте данни за достъп и пароли по имейл.

5.4. Измама 419, история, действие, ефект, последствия, загуби

При този тип СПАМ измами получавате e-mail-и от различни африкански държави, в които се твърди, че сте избран от някой човек, за да посредничите в голям трансфер на пари, при който можете да получите огромна част от сумата.

Съществуват много форми на този тип измами, наречени накратко 419 или Нигерийско Писмо. Всеки ден биват измамени редица потребители.

- История на Измама 419

Първия вариант на подобен тип измама бил приложен през далечната 1588, когато хора получавали писма, за които се твърдяло, че са изпратени от испански затворник, държан в крепост. Въпросният затворник обещавал да подели своето богатството, ако му изпратите пари, с които до успее да подкупи надзирателите на замъка.

Измамата 419 е навлязла през ранните 90 години, когато няколко безработни нигерийски студенти я прилагат върху мнозина бизнесмени, заинтересовани в петролния сектор. След многократния им успех, престъпни групи започват да прилагат системата върху по-голям брой хора. Ранния вариант на 419 бил изпращан чрез писмо, факс или телекс. По-късно интернет технологията позволява изпращането на подобен тип писма до милиони потребители дневно.

- Действие и ефективност на Измамата 419

За да достигат до значителен брой потребители, измамниците използват програми, които сканират електронната мрежа за е-мейл адреси, на които по-късно автоматично изпращат въпросните писма. Приблизителните стойности са около два отговора на хиляда изпратени писма. Съдържанието на мейлите обикновено се състои от кратка история включваща страна от третия свят, голяма сума пари (обикновено няколко милиона долара), бивш диктатор, диаманти, африкански банки и т.н. Обикновено организацията е на изключително високо ниво, включващо работещи и автентични телефонни номера, факсове, адреси, в някои редки случаи дори и връзки с посолства. Всеки, който се заеме с проверка на фактите обикновено открива, че всичко е реално. След като измамниците установят контакт с някой човек, му изпращат документи, които трябва да попълни. Въпросните документи са с много точно подправени печати, пощенски марки, холограми и др. Първото ниво след това е да изпратите най-различни

такси по "трансфера". Таксите обикновено са в неголям размер, и значителен брой хора се усещат за бъдещия неуспех и прекратяват интереса си, други пък стигат дотам, че губят суми в размери от стотици хиляди долара.

Съществуват хора излъгвани до такава степен, че са пътували сами до въпросните държави за да вземат своя "дял", някои от които убити или отвлечени срещу откуп.

- Последствия и загуби от Измама 419

Съществуват множество случаи, при които жертвите на подобен тип измами са пострадали дори физически. Поради невъзможността от преодоляването на големи парични загуби, някои хора са стигали до самоубийство. Други потърпевши, мислейки, че могат да поемат контрола върху ситуацията в свои ръце, са пътували лично до страните, от които били извършени измамите, за да разнищят случая с местните власти, надявайки се да си върнат изгубените пари. През 1995 година, американски гражданин, жертва на "измама 419" бил убит в Нигерия. Известно време след това, в столицата на Чехия- Прага, потърпевш от същата измама застрелва и убива работещия в нигерийското посолство Майкъл Лекара Уайд. По същото време гръцки гражданин бил убит в Южна Африка след замесване в измама 419. Това е малка част от криминалната хроника свързана с подобен тип измами, най-големи загуби обаче, претърпяват нигерийските бизнесмени. Колкото и наивно да звучи системата, по която се извършва измамата, в периода до 1997 година са били отчетени загуби от над сто милиона долара. Днес сумата възлиза на милиарди.

5.5. Профил на киберпрестъпниците

Киберпрестъпленията са едни от най-динамично развиващите се и иновативни престъпления в съвременното модерно общество поради техните необичайни начини и методи за извършване. Профилът на киберпрестъпника е многолик и сложен за дефиниция. Интернет предлага много възможности, които престъпниците използват, за да въведат в заблуждение жертвите си, да генерират големи печалби, да укрият средства, да стигнат до вашите лични данни, да

изнудват, да окажат психологически натиск и да манипулират дете и да се възползват от неговата психо-физическа незрялост.

5.6. Децата като най-незащитените в мрежата

Как престъпниците ги примамват и как малчуганите да се предпазват?

Най-голямата опасност в интернет е контактът с педофил. В интернет педофилите започват контакт с набелязаната си жертва най-често през някоя социална мрежа като фейсбук, защото тези сайтове се ползват от много деца и тийнейджъри. След като влязат в контакт с детето или тийнейджъра, те се представят за връстник. След започване на разговор, те често предлагат комуникацията да се пренесе в Скайп - това е така, защото Скайп е по-защитена програма за комуникация от фейсбук. Скоро след началото на разговора те преминават към сексуални теми, като понякога дори изпращат порнографски снимки или видео, за да убедят детето, че тези неща са напълно нормални. После правят опит да подмамят детето да си направи снимка или видео по бельо или гол/а. В случай че получат снимка или видео от детето, те започват изнудване, като заплашват, че ще разпространят получените снимки или видео, ако детето откаже да изпрати още. В редки случаи изнудването цели и да принуди детето да се яви на реална среща с цел сексуална злоупотреба с него. С детето трябва да се говори от ранна възраст за тази опасност. Децата все по-рано започват да ползват социалните мрежи и не винаги могат да усетят опасността. На заподозрения извършител на такъв тормоз не трябва да се казва, че родител може да се намеси в ситуацията или че ще бъде блокиран. За да може да се проведе разследване и такъв човек да бъде заловен, той не трябва да разбира, че е заподозрян. Контактът с него трябва да се прекрати под привидно благовиден предлог, без да се издава, че намеренията му са станали ясни. Добре е да се снима (скрийншот) или да се запази на файл пълният разговор на детето с извършителя като доказателство. След това веднага подайте сигнал на Горещата линия за борба с незаконно съдържание и поведение или на отдел „Киберпрестъпност“ в ГДБОП на www.cybercrime.bg.

5.7. Опасения по време на избори и очаквани кибератаки

Към настоящия момент в отдел „Киберпрестъпност“ няма постъпила информация за планирани или подготвяни кибератаки. В случай на необходимост служителите на отдела са готови да реагират бързо и своевременно съобразно предоставените им от закона правомощия.

През 2015 г. по време на местните избори бяха атакувани сайтовете на ЦИК, МВР и няколко други институции.

През 2015 г. по време на кметските избори, които бяха комбинирани с референдум, срещу България бе извършена мощна кибератака. Президентската институция, Министерският съвет, сайтът на ЦИК, бяха атакувани по такъв начин, че бяха блокирани. С много голяма степен на вероятност зад тази хакерска атака се предполага, че стои руска група, свързана с руското военно разузнаване, но към момента няма опасност за подобни атаки.

ЗАКЛЮЧЕНИЕ

Изследват се увеличаващите се предизвикателства при създаването на ефективни политики по сигурността с оглед постоянно усложняваща се информационна среда- от една страна и растяща взаимосвързаност и от друга – върху възможностите за решаването им. Всичко това е представено през призмата на значимостта на личните данни, като ключов елемент за политиките по информационна и киберсигурност, които са подложени на задълбочен преглед на настоящото изследване.

Амбицията е не просто да се разкрие важността на технологичния аспект от киберпространството върху опериращите към момента системи и политики, ангажирани с опазването на националната сигурност, а представлява опит за поглеждане отвъд традиционните модели на обвързаност между управление на процесите в социума, насочени към гарантиране на целостта и сигурността на държавата и същевременно защитавайки личното пространство и неприкосновеността на нейните граждани.

Основание за подобни твърдения се търсят в множество резултати от съществуващи научни изследвания за влиянието на информационното пространство върху съзнанието, мотивацията и поведенческата психология на хората, които в последващ план имат реално отражение във физическата реалност.

В тази нова среда политиките за национална сигурност вече не могат да функционират ефективно, базирайки се на принципите за гарантиране на безопасността на страната, бизнеса и гражданите, обслужвали индустриалната епоха..

Основен аргумент за това твърдение е, че в прехода от пост-индустриално към информационно общество се променя структурата на самата реалност в следствие еволюцията на информационното пространство, което постепенно се превръща в своеобразен конструктор (дефинитивен) на реалността. Спешната необходимост от приоритизирането на този феномен за политиките по

национална сигурност се явява логическо следствие от нарастващата технологична зависимост на процесите в социума през последните десетилетия.

Предизвикателствата тук са свързани с факта, че в тази технологично обусловена среда мрежовите функции на отделните социални единици и групи вече са достигнали нивото, при което лесно могат да катализират „ефект на пеперудата“ и реално да се причинят както значими поражения, така и огромен положителен ефект върху компактни маси от населението на планетата. Това изисква комплексно изследване на проблематиката, свързана с опазването на личните данни в новата информационна среда, като през анализа на този специфичен елемент от политиките за сигурността се разкрива ключовото им влияние на индивидуално-групово, организационно, държавно и национално ниво.

През последното десетилетие ставаме свидетели на все по-бързите темпове на развитие на света, където технологиите заемат огромно място.

Пандемията, която промени изцяло живота ни, като че ли прокара път за новите информационни и комуникационни технологии и хората станаха зависими от тях.

Вече започваме да заемаме местата си в отвореното и свободно киберпространство и започваме едно ново приобщаване на политическо, икономическо и социално ниво.

За да остане обаче това пространство социална, икономическа, военна и т.н. се стреми към дигитализиране.

Технологиите от ново поколение са инструмент за постигане на тези пели. Ставаме свидетели на гигантски технологични творения - дронове, роботи, суперкомпютри и др.

Дори вече познатите ни средства за война могат да бъдат заместени от едно устройство, което да нанесе невиждани по размер щети.

И тук отново идва мястото на сигурността и това как тя може да бъде гарантирана, но този път в едно друго пространство, а именно киберпространството.

Основни киберзаплахи в ЕС и в частност в България, както и дали самата киберпрестъпност е заплаха за България.

Целта при дефиниране на киберпрестъпност е да се покаже в каква степен България е способна да се справя с такива проблеми от ново поколение.

Киберпрестъпността е определена като престъпление, при което компютър или компютърни мрежи могат да бъдат обект на престъпление или инструмент за извършване на такова.

Компютърно престъпление или киберпрестъпление се отнася до всеки тип престъпление, който включва компютър и компютърна мрежа.

Области на криминологията, които се занимават с компютърните престъпления и компютърната престъпност, са компютърната криминология и киберкриминологията.

Компютърът може да е използван в извършването на престъпление или да е цел на престъплението.

Това се отнася и до криминалната експлоатация на интернет.
Киберпрестъпленията са дефинирани като „правонарушения, които са извършени срещу индивиди или групи от индивиди с криминален мотив с цел умишлена вреда върху репутацията на жертвата или причиняване на физическа или морална щета на жертвата директно или индиректно, използвайки модерни телекомуникационни мрежи като интернет (чат, имейли, форуми и групи) и мобилни телефони (SMS/MMS)“.

Такива престъпления могат да застрашават също така националната сигурност или финансов просперитет.

Компютърни престъпления, на борбата с които е обръщано особено високо внимание са: грууминг, детска порнография, кражби на информация по кредитни карти.

Други теми в тази област са вируси, спам, онлайн тормоз, онлайн активности, свързани с трафик на наркотици и други.

Киберпрестъпността може да засегне невиждан брой жертви и то с минимални усилия.

Самата подготовка на престъплението е много по-икономична и малка в сравнение с престъпление от друг вид.

Предмет и Дефиниране на понятията „киберпрестъпление" и „киберпрестъпност"

Голяма част от изследванията и публикациите в областта на киберпрестъпността започват с опити за дефиниране на този социален феномен.

Киберпрестъпността са отъждествява с всяко действие (деяние), при което като инструмент:

- цели или място на извършване се явяват компютърните системи или мрежи.

Като пример за търсене на международно признато определение за киберпрестъпността може да се посочи Международната конвенция за подобряване на защитата срещу киберпрестъпността и тероризма, в която киберпрестъпността се определя като неправомерни действия срещу компютърните системи и мрежите в киберпространството.

ИЗВОД

Киберсигурността урежда дейностите по организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността, и предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност.

Въвежда се Закон за киберсигурност според изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.). С УКАЗ № 257 на Президент на Републиката: Румен Радев. На основание чл. 98, т. 4 от Конституцията на Република България се обнародва в „Държавен вестник“ Законът за киберсигурност, приет от 44-то Народно събрание на 31 октомври 2018 г. Издаден в София на 7 ноември 2018 г. Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., и Наредба в сила от 26.07.2019 г. Приета с ПМС № 186 от 19.07.2019 г. Обн. ДВ. бр.59 от 26 Юли 2019г., изм. ДВ. бр.36 от 13 Май 2022г., изм. ДВ. бр.47 от 24 Юни 2022г.

Закона за киберсигурност предвижда мерки по прилагане на Регламент за изпълнение (ЕС) 2018/151 на Комисията от 30 януари 2018 г. за определяне на правила за прилагане на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета по отношение на допълнителното уточняване на елементите, които трябва да се вземат предвид от доставчиците на цифрови услуги при управлението на рисковете за сигурността на мрежите и информационните системи, както и на показателите за определяне на това дали даден инцидент има съществено въздействие (ОВ, L 26/48 от 31.01.2018 г.).

Списък на използваната литература

https://trud.bg/Явор Колев 10.05.2019

https://www.youtube.com/СДВР Столична Полиция Киберпрестъпност(2117)

https://www.consilium.europa.eu/bg/policies/cybersecurity/

https://prezi.com/h4cvu9moid5e/presentation/

Закон за киберсигурност