ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА
ENTI SHTETËROR I REVIZIONIT
STATE AUDIT OFFICE

КОНЕЧЕН ИЗВЕШТАЈ
ЗА ИЗВРШЕНА ИТ РЕВИЗИЈА
КАКО РЕВИЗИЈА НА УСПЕШНОСТ

„ЕФЕКТИВНОСТ НА ПРЕЗЕМЕНИТЕ МЕРКИ НА НАДЛЕЖНИТЕ ОРГАНИ ЗА ЗАШТИТА НА КРИТИЧНИТЕ ИНФОРМАЦИСКИ СИСТЕМИ“

08 2023 03 11

9 ИНДУСТРИЈА, ИНОВАЦИЈА И ИНФРАСТРУКТУРА

Скопје, април 2024 година

С О Д Р Ж И Н А

Список на кратенки

АЕК	Агенција за електронски комуникации
ВИС	Важни информациски системи
Влада	Влада на Република Северна Македонија
ЕНЕР	Електронски национален регистар на прописи на Република Северна Македонија
ЕСЈН	Електронски систем за јавни набавки: https://e-nabavki.gov.mk/
ЕУ	Европска Унија
ИКТ	Информациско комуникациска технологија
КИИ	Критична информациска инфраструктура
КИС	Критични информациски системи
МИОА	Министерство за информатичко општество и администрација
МКД-ЦИРТ	Национален центар за одговор на компјутерски инциденти
МФ	Министерство за финансии
NIS/NIS2/НИС/НИС2	The Network and Information Security Directive (NIS) – Директива за мрежна и информациска безбедност на ЕУ
НАТО	Организација на Северноатлантскиот договор
SLA	Service-level agreement - Договорот на ниво на услуга што се очекува од договорниот орган, како и правните лекови или казни доколку не се постигнат договорените нивоа на услуги
Собрание	Собрание на Република Северна Македонија
Совет	Национален совет за сајбер безбедност
ФЗОРСМ	Фонд за здравствено осигурување на Република Северна Македонија
CSIRT	Computer Security Incident Response Team - Тим за одговор на инциденти врз компјутерската безбедност
CERT	Computer Emergency Response Team - Тим за одговор на компјутерски вонредни ситуации
CIRT	Computer Incident Response Team - Тим за одговор на компјутерски инциденти

Поимник

ИТ ревизија	Ревизија на информациски системи
Безбедност на мрежни и информациски системи	Способност на мрежните и информациските системи, да се спротивстават, со одредено ниво на доверба, на секое дејство кое ја загрозува достапноста, автентичноста, интегритетот или доверливоста на складираните, пренесените или обработените податоци или на поврзаните услуги што ги нудат или се достапни преку тие мрежни и информациски системи
DDoS напад	Дистрибуиран напад на одбивање на услуга е сајбер криминал во кој напаѓачот го преплавува серверот со интернет сообраќај за да ги спречи корисниците да пристапат до поврзаните онлајн услуги и сајтови
Компјутерски безбедносен инцидент	Компјутерски безбедносен инцидент е секој реален или сомнителен несакан настан во врска со безбедноста на компјутерските системи или компјутерските мрежи, односно чинот на прекршување на експлицитни или имплицитни безбедносни политики.
Log file	log датотека е компјутерски генерирана датотека со податоци која содржи информации за шемите на користење, активностите и операциите
ИП/IP адреса	Адреса на Интернет протокол (IP) е единствениот идентификациски број доделен на секој уред поврзан на интернет
Malware, Малвер	Злонамерен софтвер, се однесува на секој нападен софтвер развиен од сајбер криминалци (често наречени хакери) за кражба на податоци и оштетување или уништување на компјутери и компјутерски системи. Примери за вообичаен малициозен софтвер вклучуваат вируси, црви, тројански вируси, шпионски софтвер, adware и откупни софтвери (ransomware)
Оператори на критична инфраструктура	Оператори на суштински услуги и оператори на важни услуги
Сајбер безбедност	Систем на активности и мерки потребни за заштита на мрежните и информациските системи, корисниците на таквите системи и другите лица погодени од закани преку компјутерски мрежи
Спам	Безбедносен инцидент кој води до компромитирана веб-локација на веб-сервер со неовластено поставена рекламна содржина
Сајбер закана	Секоја потенцијална околност, настан или активност што може да оштети, наруши или на друг начин негативно да

	влијае врз мрежата и информациските системи, корисниците на таквите системи и други лица
Тим за одговор на компјутерски безбедносни инциденти	Посебна организациска единица надлежна за преземање на соодветни постапки и мерки за поддршка на откривање, анализа на инцидент и ограничување на неговото влијание, како и одговор на инцидент кој би можел да настане во рамки на конкретниот сектор (CSIRT)
Фишинг	Безбедносен инцидент кој води до лажна интернет страница на компромитирана веб-локација чија цел е кражба на лични или осетливи податоци
Firewall	Заштитен ѕид е бариера помеѓу две мрежи кои идентификува и блокира сајбер закани додека низ него дозволува соодветен сообраќај
Хакирање	Недозволен влез во туѓ систем и уништување или крадење информации од страна на компјутерски корисник
Штетен/малициозен домен	Небезбедни домени се надворешни врски до веб-локации што може да содржат фишинг, малициозен софтвер или несакан софтвер, регистрирани од напаѓачите кои се прикриени и остануваат активни за краток временски период за да се избегне откривање

Број:
Дата:

РЕЗИМЕ

Извршивме ревизија на успешност – ревизија на информациски системи на тема „Ефективност на преземените мерки на надлежните органи за заштита на критичните информациски системи“ со цел да дадеме одговор на прашањето **„Дали преземените мерки од надлежните органи обезбедуваат ефикасна и целосна заштита на критичните информациски системи?“**
Ревизијата на успешност е извршена согласно Годишната програма за работа на Државниот завод за ревизија за 2023 година.

Со ревизијата на успешност опфативме период од 2020 до 2022 година, при што беше опфатен период пред и период по завршување на ревизијата, до денот на изготвување на овој извештај.

За да одговориме на главното ревизорско прашање, ги определивме следните специфични прашања:

- Дали правната регулатива обезбедува соодветни предуслови за заштита на критичните информациски системи?
- Дали се доволни финансиските, техничките и административните капацитети за заштита на критичните информациски системи?
- Дали има координација помеѓу органите и институциите во справувањето со безбедносните инциденти?

Со спроведената ревизија и применетата ревизорска методологија и прибраните ревизорски докази, стекнавме разумно уверување дека институциите и органите не обезбедуваат ефикасна и целосна заштита на критичните информациски системи.

Имено, заклучокот го донесовме врз основа на докази за отсуство на законска регулатива од областа на безбедноста на информациските системи, не извршеното усогласување на националното законодавство со европските директиви, отсуството на стратешки документи како сет на мерки и активности како и нефункционирање на Советот не обезбедува соодветни предуслови на заштита на критичните информациски системи.

Минималните безбедносни мерки и стандардите за заштита на информациските системи, регулативата за дефинирани критериуми и креирањето на регистер со

оператори на критични информациски системи се неопходни активности за заштита на информациските системи. Финансиските средства предвидени за информациска безбедност како и вложување во вработените од оваа област, треба да се разберат и прифатат како превентивни мерки од штета во однос на трошокот направен по безбедносен инцидент.

Воспоставениот начин на пријава и одговор при компјутерски безбедносен инцидент, состојбите со тимови за одговор на компјутерски безбедносни инциденти кои не се формирани, не осигурува навремен и соодветен одговор на инцидент, како и оневозможува навремено исклучување од интернет мрежата на инфицираните и малициозни уреди кои се приклучени преку интернет операторите, со што се продолжува нивната штетна активност.

Ревизорските активности беа насочени кон утврдени ризици во две области при што се констатирани следните состојби:

ИТ управување

- отсуство на законска регулатива од областа на безбедноста на информациските системи;
- усогласувањето на националното законодавство со европските директиви НИС од 2016 година и надградената НИС2 регулатива од 2023 година, што е рамка на ЕУ за воспоставување на минимални мерки за сајбер безбедност во критичната ИКТ инфраструктура на земјите членки не е извршено;
- подготвен е предлог закон за безбедност на мрежи и информациски системи во 2019 година кој до денот на известување од ревизијата не е донесен, а подготвен е нов предлог закон во 2023 година кој се наоѓа во собраниска процедура;
- Национална ИКТ стратегија која е усвоена е со важност до 2017 година додека последната Националната стратегија за сајбер безбедност е со важност до 2022 година. И покрај тоа што се подготвени, Националната ИКТ стратегија и Националната стратегија за сајбер безбедност се уште се наоѓаат во меѓу институционално усогласување;
- Национален совет за сајбер безбедност формиран е во 2019 година заради координација и следење на спроведените активности согласно Националната стратегија за сајбер безбедност на Република Македонија 2018-2022. Од неговото формирање до периодот на известување од ревизијата Советот одржал еден состанок, при што на ревизијата не и се презентирани годишни извештаи за работата доставени до Владата, предложени мерки за подобрување на имплементацијата на Стратегијата и Акцискиот план, мерки за поголема ефикасност за управување со сајбер кризи како и стратешки насоки и препораки поврзани со сегментот на сајбер безбедност;
- регулатива за дефинирани критериуми и креирање на регистер со оператори на критична инфраструктура (ВИС и КИИ) како и дефинирање на минимални

безбедносни мерки и стандарди за заштита на нивните информациски системи не се донесени.

ИТ операции

- пријавата на компјутерски безбедносен инцидент од страна на институциите до МКД-ЦИРТ не е пропишана;
- начинот на оневозможување пристап до интернет мрежата на инфицирани и малициозни уреди кои се приклучени преку интернет операторите, а кои се извор на малициозни софтвери не е регулиран;
- лица за информациска безбедност во институциите не се назначени како и доволен број на вработени со кој се минимизира ризикот од навремена детекција на закани по информацискатa безбедност на прифатливо ниво како и преземање на мерки за заштита од истите;
- отсуство на континуирана стручна обука за најновите закани по информацискатa безбедност;
- недоволно формирани тимови за одговор на компјутерски безбедносни инциденти;
- не се врши анализа на ризици со предлог мерки според приоритет на ризиците за нивно намалување, ублажување, пренесување или минимизирање на прифатливо ниво, со точна временска рамка за спроведување на истите;
- не се спроведува континуирана анализа, со цел согледување на реалната состојба и дефинирање мерки и препораки за подигнување на нивото на безбедност, извршување на редовни ревизии за детектирање на грешки и ранливости на безбедноста, развој и периодично тестирање на планови на информацискатa безбедност во институциите.

Препораките дадени во овој извештај се однесуваат на активностите кои Владата преку ресорните министерства, како и другите државни институции и органи треба да ги преземат со цел отстранување на причините од утврдените неправилности, утврдените состојби или потенцијалните ризици прикажани во овој извештај, како и активностите кои треба да придонесат за надминување на утврдените слабости и обезбедат подобрување на безбедноста на информациските системи на субјектите кои имаат критична инфраструктура, особено во делот на достапноста, интегритетот и доверливоста на информациите кои ги обработуваат.

Нагласуваме дека во текот на целиот процес на вршење на ревизијата, ревизорскиот тим на Државниот завод за ревизија имаше постојана стручна и професионална соработка и комуникација од назначеното лице за комуникација со ревизорскиот тим и одговорните лица кај сите институции вклучени во низата на активности кои беа предмет на ревизија и кои изразија и покажаа позитивен однос кон ревизијата.

Од страна на одговорните лица на Владата, МИОА и АЕК не се добиени забелешки на Нацрт извештајот на Овластениот државен ревизор.

1. ВОВЕД

1.1. Основ и причини за извршување на ревизијата

Во последните години, на глобално ниво, забележан е раст на нивото и сериозноста на злонамерните сајбер активности, така што овие безбедносни закани треба да се третираат како интегрален дел од националната и меѓународната безбедност.
Зависноста од новите технологии и потребата од поголема достапност на услугите во сајбер просторот е причина корисниците и институциите да ја зголемат свесноста за значењето на интегритетот, достапноста и доверливоста на податоците.
Постојаните промени што се случуваат во информацискатa безбедност, наведуваат на размислување и подготовка за подобра заштита од заканите. Еден од клучните чекори за тоа е навремено откривање на потенцијалните закани и соодветен одговор на истите. При зачувувањето на информацискатa безбедност, важно е дефинирање на регулативата, стратешките документи, ресурсите, соодветните улоги на учесниците како и заедничката одговорност на повеќето чинители.

Имајќи го во предвид горенаведеното, во Годишната програма за работа на Државниот завод за ревизија за 2023 година планирана е и извршена ИТ ревизија како ревизија на успешност на тема „Ефективност на преземените мерки на надлежните органи за заштита на критичните информациски системи“.

1.2. Предмет на ревизија

Заштитата на критичните информациски системи наметнува потреба за идентификување на сектори и институции кои обезбедуваат суштински и важни услуги како и заштита на нивните комуникациски мрежи и информациски системи. Исто така неопходно е обезбедување на заедничко високо ниво на безбедност и заштита, превенција од сајбер безбедносни инциденти или кризи, како и развој на брза и ефективна оперативна меѓусебна соработка за заштита на мрежи и информациски системи. Значајно е да има сигурност при користење и достапност на комуникациски мрежи, високо ниво на интегритет, достапност и доверливост на податоците создадени од државните органи, утврдување на критичните информациски системи и дефинирање на соодветни улоги на учесниците.
Со таа намена во состав на АЕК формирана е посебна организациона единица - Национален центар за одговор на компјутерски инциденти МКД-ЦИРТ, како национален CSIRT на Република Северна Македонија, кој претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

Националниот центар за одговор на компјутерски инциденти ја има следната мисија:

- да координира и да помага на органите и институциите од јавниот сектор во имплементацијата на проактивни услуги за намалување на ризикот од

компјутерски безбедносни инциденти, како и при справувањето со инцидентите кога истите ќе настанат;
- да спроведува активности за едуцирање и подигање на свесноста кај граѓаните за негативните ефекти на сајбер-заканите и компјутерскиот криминал и
- навремено да обезбедува совети за сите негови конституенти.

1.3. Законска регулатива

Заштитата на критичните информациски системи е уредена со следните нормативни акти:
- Закон за електронските комуникации;
- Закон за енергетика;
- Национална стратегија за сајбер безбедност на Република Македонија 2018 – 2022 со акциски план за истата;
- НИС директива (ЕУ) 2016/1148 донесена од Европскиот парламент која се однесува на високо заедничко ниво на сајбер безбедност во ЕУ;
- НИС2 надградена директива (ЕУ) 2022/2555 донесена од Европскиот парламент која се однесува на високо заедничко ниво на сајбер безбедност во ЕУ и со која се заменува претходно донесената директива;
- Предлог-мерки за подобрување на безбедноста на информациските системи во институциите од јавниот сектор од Владата од 131-та седница одржана на 21.02.2023 година, во делот на Агенда за дигитална трансформација;
- Правила за сајбер-безбедност.

1.4. Институционална рамка

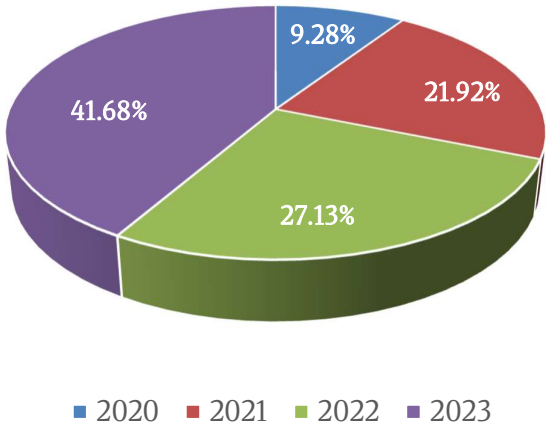
Владата преку министерствата и други државни институции и органи е директен носител на мерките и политиките за заштита на критичните информациски системи. Владата има донесено Одлука за формирање на Национален совет за сајбер безбедност[1] заради координација и следење на спроведените активности согласно Националната стратегија за сајбер безбедност на Република Македонија 2018-2022, како и за дефинирање на нови стратешки насоки и препораки поврзани со сегментот на сајбер безбедност.

1.5. Финансирање на дејноста

Вкупната вредност на склучените договори од областа на информацискатa безбедност на ИКТ системите на сите државни институции кои истите ги имаат објавено на ЕСЈН се за период 01.01.2020 до 15.12.2023 година објавени во системот на ЕСЈН е 376.961 илјада денари и истата е претставена на следниот графикон:

[1] Одлука бр. 45-7326/1 од 02.10.2019 година

Графикон број 1 – Процентуална распределба на вредноста на склучените договори од областа на информацискатa безбедност на ниво на државни институции по години



2. ЦЕЛИ, ОПФАТ И МЕТОДОЛОГИЈА НА РЕВИЗИЈАТА

2.1. Цели на ревизијата

Целта на ИТ ревизијата како ревизија на успешност е да даде оценка на преземените мерки од надлежните органи за обезбедување ефикасна и целосна заштита на критичните информациски системи.

Специфичните цели на ИТ ревизијата како ревизија на успешност, кои се поврзани со поединечните предметни области на ревизијата, се однесуваат на оценување на:

- правната регулатива која треба да обезбеди соодветни предуслови за заштита на критичните информациски системи;
- донесените потребни нормативни и стратешки акти за заштита и безбедност на информациските системи со утврдени и разграничени надлежности на инволвираните институции;
- дефинираните критериуми за идентификување на секторите со листа на критични информациски системи;
- надзорот, координацијата, спроведувањето и предлагањето на мерки и активности на заштита на критичните информациски системи – КИС;
- финансиските, техничките и административните капацитети за заштита на критичните информациски системи;
- координацијата помеѓу органите и институциите во справувањето со безбедносните инциденти;
- проактивните услуги за намалување на ризикот од безбедносни инциденти од страна на МКД-ЦИРТ;
- анализи и преземени мерки за намалување на ризиците од компјутерски безбедносни инциденти;
- оперативни тимови и обезбедени услуги за справување со компјутерски безбедносни инциденти.

Препораките дадени во овој извештај, ќе имаат додадена вредност во насока на: донесување на стратешка и правна рамка, подобрување на мерките и активностите на заштита на критичните информациски системи, што ќе влијае на позитивен начин на подобрувањето на процесите за заштита и намалување на ризиците од безбедносни инциденти.

2.2. Ревизорски прашања

Ревизијата на успешност е активност која ја спроведовме со цел да дадеме оценка за и да одговориме на главното ревизорско прашање:

„Дали преземените мерки од надлежните органи обезбедуваат ефикасна и целосна заштита на критичните информациски системи? “

Специфични прашања по утврдени области се:

- Дали правната регулатива обезбедува соодветни предуслови за заштита на критичните информациски системи?

- Дали се доволни финансиските, техничките и административните капацитети за заштита на критичните информациски системи?
- Дали има координација помеѓу органите и институциите во справувањето со безбедносните инциденти?

2.3. Опфат на ревизијата

Со ревизијата на информациските системи како ревизија на успешност, опфативме период од 2020 до 2022 година, а одредени прашања и настани се опфатени претходно и последователно до денот на известување за ревизијата.

Согласно утврдените ризици по добиените прелиминарни информации, а врз основа на избран примерок, извршивме увид на лице место во Владата, АЕК и МИОА.
Останатите субјекти ги опфативме со прашалници и увид во бараната документација.
Со цел да добиеме поширок податоци и информации поврзани со темата на ревизијата, изработен и доставен е прашалник до 18 институции во јавниот сектор (Прилог број 2).
Ревизорските активности кои ревизорскиот тим ги спроведе во субјектите опфатени со ревизијата беа насочени кон повеќе области и под области:

- ИТ управување
  - Правна регулатива за заштита на критичните информациски системи и
  - Финансиски, технички и административни капацитети за заштита на критичните информациски системи.
- ИТ операции
  - Координација помеѓу органите и институциите во справување со безбедносни инциденти.

2.4. Критериуми за ревизија

За оценка на ефективноста на преземените мерки на надлежните органи за заштита на критичните информациски системи се користени критериумите и показателите за оценка прикажани во Прилог број 1 кон ревизорскиот извештај.

2.5. Методологија на ревизијата

2.5.1. ИТ ревизијата како ревизија на успешност е извршена во согласност со стандардите на ISSAI за ревизија на успешност, Кодексот на етика на Државниот завод за ревизија и Упатството за ревизија на информациски системи на INTOSAI - GUID 5100.

2.5.2. Кај оваа ревизија на успешност избравме и применивме комбиниран пристап од пристапот ориентиран кон системите, пристапот ориентиран кон проблемите и пристапот ориентиран кон резултатите. Ревизијата беше насочена кон проверка, анализа и испитување на донесените законски и стратешки документи, акциски планови и ЕУ директиви од оваа област и анализа на системите кои се користат за безбедноста на информациските системи како и методите кои се преземаат за рано откривање и превенирање на инциденти, причините за проблемите кои се јавуваат и дали поставените цели се исполнети.

2.5.3. Со цел добивање на релевантни и доволни ревизорски докази кои водат кон ревизорските наоди, заклучоци и препораки, ги користевме методологијата и техниките на ревизија на успешност:

- проучување на законска и друга регулатива, стратешки и плански документи од областа предмет на ревизија,
- разговори/интервјуа со лица релевантни за темата на ревизијата,
- прашалници до релевантните субјекти,
- проверка на документација,
- анализа на податоци и информации,
- увид на лице место и
- интернет истражување.

2.5.4. Ревизијата на успешност е извршена во периодот од 03.04.2023 до 29.12.2023 година од тим на Државниот завод за ревизија.

2.5.5. Резултатите од спроведената ревизија на успешност беа презентирани на завршен состанок со претставници на субјектот предмет на ревизија и претставници од институциите кои беа вклучени во истражувањето на ден 13.02.2024 година преку он-лине ZOOM платформата.

3. РЕВИЗОРСКИ НАОДИ

3.1. ИТ Управување

Информацискатa безбедност е значајна за заштита на критичната инфраструктура бидејќи сајбер нападите можат да предизвикаат сериозни оштетувања на инфраструктурата и нејзините функции, како што се:

- загрозување на доверливоста, интегритетот и достапноста на податоците и информациите;
- нарушување на работењето и контролата на физичките средства и процеси;
- загрозување на безбедноста и благосостојбата на јавноста и животната средина;
- нарушување на довербата и сигурноста во инфраструктурата и нејзините услуги;
- настанување на финансиски загуби и штети на угледот на институциите - сопственици на инфраструктурата како и операторите.

Сериозните оштетувања на ИКТ системот кај субјект од критична инфраструктура може да доведат до прекин на давањето на услугите кои се од суштинско значење за државата и граѓаните, без притоа да може точно да се дефинира периодот на опоравување и враќање во состојба на нормално функционирање.

Информацискатa безбедност е од суштинско значење за да се обезбеди отпорност и континуитет на критичната инфраструктура и услугите што тие ги обезбедуваат на општеството. Таа бара целокупен пристап кој опфаќа технички, политички, човечки и аспекти на однесувањето, како и соработка и координација помеѓу различни засегнати страни, како што се владата, индустријата и академската заедница. Сајбер нападите врз критичната инфраструктура може да имаат различни мотиви, како што се измама, шпионажа, саботажа, изнуда, тероризам или војување.

Информацискатa безбедност на критичната инфраструктура се соочува со многу предизвици, како што се:

- комплексноста и меѓузависноста на критичните инфраструктурни системи, кои создаваат повеќекратни вектори на напад и каскадни ефекти;
- затекнатите и застарени технологии кои често се користат во критичната инфраструктура, на кои им недостасуваат соодветни безбедносни карактеристики и ажурирања;
- недостигот од квалификувани професионалци за сајбер безбедност и недостатокот на свест и обука кај вработените и корисниците на критичната инфраструктура;
- правните и регулаторните празнини и недоследности што ја попречуваат координацијата и споделувањето информации меѓу различните засегнати страни.

За информацискатa безбедност потребен е проактивен и колаборативен пристап, особено:

- развивање и имплементирање на стандарди и најдобри практики за критичните инфраструктурни сектори;
- спроведување редовни проценки и ревизии за да се идентификуваат и ублажат ранливостите и ризиците;
- подобрување на свеста и едукација кај операторите и корисниците;
- воспоставување и одржување на ефективни планови и способности за одговор и обновување по безбедносни инциденти;
- поттикнување на споделување информации и соработка меѓу владата, индустријата и академијата за заканите и решенијата.

3.1.1. Правна регулатива за заштита на критичните информациски системи

3.1.1.1. Законска и друга регулатива

Закон за електронските комуникации

Со измените на Законот за електронските комуникации[2] од 2014 година, во состав на Агенцијата за електронски комуникации е формирана посебна организациона единица - **Национален центар за одговор на компјутерски инциденти МКД-ЦИРТ**, како национален CSIRT на Република Северна Македонија, кој претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

НИС директива

НИС Директивата (ЕУ) 2016/1148 на Европскиот парламент и на Советот на ЕУ од 6 јули 2016 година содржи мерки за висок општ степен на безбедност на мрежни и информациски системи кои државите членки на ЕУ треба да ги усогласат во своите законодавства.

Во Европскиот парламент на 16 јануари 2023 година, усвоена е новата НИС2[3] директива која се однесува на високо заедничко ниво на сајбер безбедност во ЕУ. Земјите-членки имаат рок заклучно со 17 октомври 2024 година, да извршат промени во националните законодавства за усогласување со директивата. Со донесувањето на новата НИС2 директива, НИС директивата од 2016 година е ставена вон сила.

[2] Службен весник на Република Македонија број 188/2014
[3] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Најважни мерки на директивата НИС2

Директивата НИС2 е нова регулатива на ЕУ која има за цел да ја подобри сајбер безбедноста на суштинските и важни субјекти во различни сектори. Според директивата НИС2, институциите мора да преземат мерки за решавање во следните области:

- управување со ризик: институциите мора да имплементираат политики и процедури за да ги идентификуваат, проценат и ублажат сајбер ризиците и да обезбедат безбедност на нивните информациски системи и мрежи;
- корпоративна одговорност: институциите мора да доделат улоги и одговорности за сајбер безбедноста на нивното раководство и вработените и да се погрижат тие да се обучени и свесни за сајбер заканите и најдобрите практики;
- обврски за известување: институциите мора да пријават значајни сајбер инциденти до релевантните органи и засегнати страни во одредени рокови и да соработуваат со нив во истрагата и решавањето на инцидентите;
- деловен континуитет: институциите мора да подготват и тестираат планови за да обезбедат континуитет на нивните услуги и операции во случај на голем сајбер инцидент и да ги вратат своите нормални функции што е можно поскоро.

Покрај овие области, директивата НИС2 исто така бара од институциите да имплементираат 10 минимални безбедносни мерки за справување со специфични форми на сајбер закани, како што се криптирање/шифрирање, автентикација, резервна копија, управување со безбедносни надградби/закрпи и како безбедност на синџирот на снабдување (услуги од трети страни).

Институциите кои нема да се усогласат со директивата НИС2 во земјите членки на ЕУ, се соочуваат со финансиски казни врз основа на нивниот вкупен промет, како и правни или репутациски последици.

Директивата НИС2 се применува на два вида субјекти: суштински и важни субјекти. Суштински субјекти се оние кои обезбедуваат услуги кои се од витално значење за општеството и економијата, како што се **енергијата, транспортот, банкарството, финансиските пазари, здравството, водата, дигиталната инфраструктура, вселената, ИКТ операторите и јавната администрација** .

Важни субјекти се оние кои обезбедуваат услуги кои имаат значително влијание врз општеството и економијата, како што се поштенски услуги, управување со отпад, хемикалии, храна, производство, дигитални услуги и истражување.

Директивата НИС2 бара од земјите-членки да назначат национални надлежни органи и единствени точки за контакт за сајбер безбедноста и да воспостават национални стратегии за сајбер-безбедност и планови за одговор на инциденти. Од земјите-членки, исто така се бара да соработуваат и да разменуваат информации меѓу себе и со институциите, телата и агенциите на ЕУ, како што се Агенцијата за

сајбер безбедност на Европската унија (ENISA) и Тимот за одговор при компјутерски инциденти при итни случаи за институциите, телата и агенциите на ЕУ (ЦЕРТ-ЕУ).

Директивата НИС2 воведува нов систем на безбедносен надзор и спроведување, врз основа на профилот на ризик на субјектите. Националните надлежни органи се одговорни за следење и ревизија на усогласеноста на субјектите со директивата НИС2 и за наметнување санкции во случај на неусогласеност. Санкциите може да варираат во зависност од сериозноста, времетраењето и повторувањето на прекршувањето и може да вклучуваат административни казни, наредби за прекин на активноста или повлекување на овластувањето за давање услуга.

Закон за безбедност на мрежи и информациски системи

Отсуството на правна регулатива во државата во областа на безбедност на мрежи и информациски системи, потребата од усогласување со НИС директивата како и утврдената активност во Националната стратегија за сајбер безбедност на Република Македонија (2018-2022), наметна потреба од изготвување на Закон за безбедност на мрежи и информациски системи. Истиот од страна на МИОА е подготвен како предлог закон[4] и поставен на ЕНЕР[5] во месец октомври 2019 година. Ревизијата утврди дека предлог законот до денот на известување од ревизијата е се уште поставен на ЕНЕР со отворен статус. Со предлог законот дефинирани се институции задолжени за секој од секторите кои имаат ИКТ системи со критична инфраструктура, како и преземање на мерки, надзор и тимови за одговор по инциденти и заштита на информацискатa безбедност.

Закон за безбедност на мрежни и информациски системи и дигитална трансформација

Во месец јули 2023 година формирана е работна група за подготовка на нов Предлог на Закон за дигитализација и безбедност на мрежи и информациски системи. Во Предлог на законот треба да биде транспонирана Директивата на ЕУ 2016/1148 на мерки за високо заедничко ниво на безбедност на мрежни и информациски системи, а во исто време да биде земена во предвид НИС2 директивата.

Предлог законот за безбедност на мрежни и информациски системи и дигитална трансформација објавен е на ЕНЕР во септември 2023 година и по поминатa јавна расправа истиот е разгледан на седница на Влада[6].

Со изготвениот предлог закон утврдено е обезбедување високо ниво на кибер безбедност со цел заштита и понатамошен развој на општеството, градење и развој на информациско-комуникациска (ИКТ) инфраструктура, односно поефикасна и

[4] https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471
[5] https://ener.gov.mk/Default.aspx
[6] https://vlada.mk/node/35385

поефективна дигитална трансформација на јавниот сектор. Една од клучните цели на овој закон е дигитална трансформација на јавниот сектор, што ќе се однесува на органите на државната управа (освен на органите на државната управа од областа на безбедноста и одбраната) на Република Северна Македонија. Дигиталната трансформација ќе се однесува и на други институции од јавниот сектор по нивно барање, а во согласност со овој закон и со Планот за дигитална трансформација на јавниот сектор.

За примена на предложениот закон предвидено е формирање на Агенција за безбедност на мрежни и информациски системи и дигитална трансформација. Во истиот се дефинирани операторите на суштински и важни услуги како средни или големи претпријатија кои обезбедуваат услуги во секторите: енергетика, транспорт, банкарство, финансиски пазар, здравство, снабдување и дистрибуција на вода за пиење, отпадни води, дигитална инфраструктура, управување со ИКТ-услуги (B2B), вселена, дигитални услуги, поштенски и курирски услуги, управување со отпад, изработка, производство и дистрибуција на хемикалии, производство, преработка и дистрибуција на храна, производство, истражување.

Регистарот на оператори на суштински и важни услуги утврдено е да го води Агенција за безбедност на мрежни и информациски системи и дигитална трансформација и истиот редовно да се ажурира.

Предлог законот е доставен до Собранието за разгледување и усвојување. До периодот на известување од ревизијата, предлог законот не е разгледан и усвоен од Собранието.

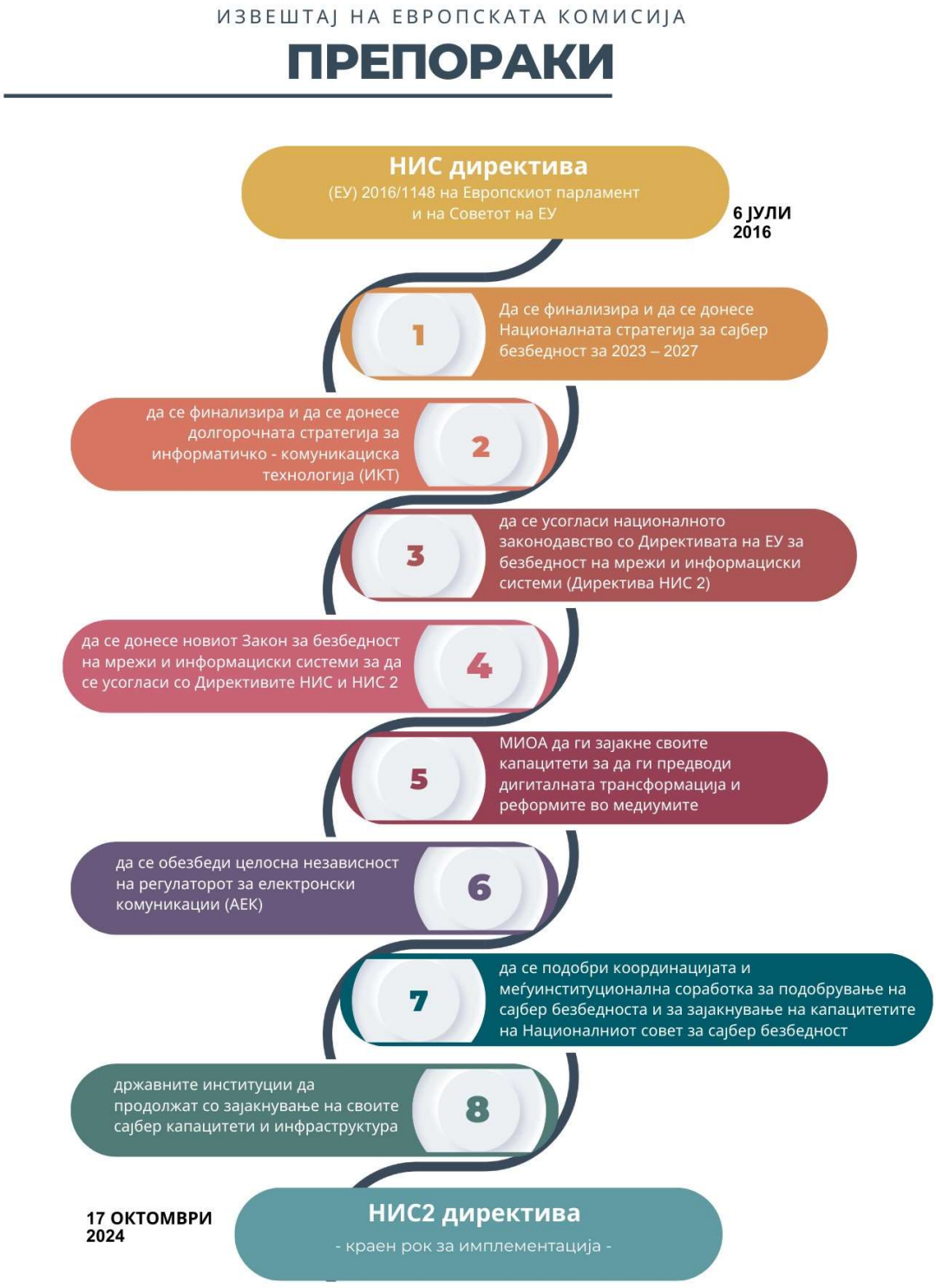
Согласно овој предлог закон ќе се формира Агенција за безбедност на мрежни и информациски системи и дигитална трансформација која ќе биде одговорна за информацискатa безбедност, но во првата година предвидени се финансиски средства само за Комисијата на агенцијата која ќе раководи со истата. Развојот и оперативното функционирање на Агенција за безбедност на мрежни и информациски системи и дигитална трансформација ќе опфати период од најмалку неколку години. Со тоа рокот за имплементирање на НИС2 директивата, до октомври 2024 година, нема да биде исполнет, и ризикот од закани по информацискатa безбедност во државата и понатаму ќе биде висок.

Извештај на Европската комисија

Во извештајот на Европската комисија за Северна Македонија за 2023 година, во поглавје 10: Дигитална трансформација и медиуми, земјата е оценета како умерено подготвена во областа на дигиталната трансформација и медиумите.

Препораките од минатата година во делот во информацискатa безбедност, остануваат исти и се прикажани на слика број 2.

Слика број 2


ИЗВЕШТАЈ НА ЕВРОПСКАТА КОМИСИЈА
ПРЕПОРАКИ
НИС директива
(ЕУ) 2016/1148 на Европскиот парламент и на Советот на ЕУ
6 ЈУЛИ 2016
1
Да се финализира и да се донесе Националната стратегија за сајбер безбедност за 2023 – 2027
2
да се финализира и да се донесе долгорочната стратегија за информатичко - комуникациска технологија (ИКТ)
3
да се усогласи националното законодавство со Директивата на ЕУ за безбедност на мрежи и информациски системи (Директива НИС 2)
4
да се донесе новиот Закон за безбедност на мрежи и информациски системи за да се усогласи со Директивите НИС и НИС 2
5
МИОА да ги зајакне своите капацитети за да ги предводи дигиталната трансформација и реформите во медиумите
6
да се обезбеди целосна независност на регулаторот за електронски комуникации (АЕК)
7
да се подобри координацијата и меѓуинституционална соработка за подобрување на сајбер безбедноста и за зајакнување на капацитетите на Националниот совет за сајбер безбедност
8
државните институции да продолжат со зајакнување на своите сајбер капацитети и инфраструктура
17 ОКТОМВРИ 2024
НИС2 директива
- краен рок за имплементација -

Понатаму во препораките, во однос на Националната стратегија за сајбер безбедност 2018-2022 и покрај тоа што е наведено дека органите спроведуваат активности што се дел од стратегијата, има потреба од подобра координација и меѓу институционална соработка. Националниот регулатор ја промовирал сајбер безбедноста преку својот Национален центар за одговор на компјутерски инциденти. Притоа биле пријавени инциденти поврзани со сајбер безбедноста во 145 субјекти, какви што се државни институции, банкарство, здравство, енергетика, транспорт и комуникациски организации.

Ваквата состојбата во отсуство на законска регулатива од областа на безбедноста на информациските системи може да предизвика долгорочни несакани последици по информацискатa безбедност на ИКТ системите во институциите и да го доведе во прашање високото заедничко ниво на безбедност и заштита на мрежни и информациски системи и дигитална трансформација на јавниот сектор. Истото ќе доведе и до запирање на инвестиции, маргинализирање и одложување на имплементацијата на мерките за подобра заштита на информациските системи.
Исто така, не е извршено усогласување на националното законодавство со европските директиви НИС од 2016 година и надградената НИС2 регулатива од 2023 година која ги дефинира минималните мерки за сајбер безбедност во критичната ИКТ инфраструктура на земјите членки на ЕУ и истото претставува ризик од користење и пристап до заедничките информациски системи на ЕУ.
Како земја на пристапниот пат кон ЕУ, треба да се посветиме на усогласување на домашното законодавство со законодавството на ЕУ.

Ревизијата сака да истакне дека во делот на законската регулатива направени се измени на Законот за енергетика во 2022 година при што Регулаторната комисија за енергетика и водни услуги, добива нова надлежност во полето на сајбер безбедноста во енергетскиот сектор, со кој се уредува обезбедување на мрежите и на информациските системи на операторите и производителите на електрична енергија кои управуваат со моќност над 200 MW. Операторите треба да преземаат мерки и активности за откривање закани и спречување сајбер напади и инциденти и да воспостават механизми за справување со заканите и последиците од нападите и инцидентите како и за обновување на мрежите и системите до состојба во која се наоѓале пред сајбер нападот или инцидентот.
Одредбите на законот се однесуваат и на компании во државна сопственост од дејноста како што се акционерските друштва „Електрани на Северна Македонија“ и „МЕПСО - Оператор на електропреносен систем на Северна Македонија“, вклучително и компаниите регистрирани од овие друштва.

Наведените субјекти особено се должни да:
- назначат службеник за сајбер безбедност;
- се сертифицираат според меѓународни стандарди за безбедност на мрежите, информатичка безбедност и сајбер безбедност;
- донесат методологија за проценка на ризици од сајбер напади и инциденти и оперативни планови за превенција и реакција на сајбер напади и инциденти;

- размената информации за сајбер закани и инциденти со Регулаторната комисија за енергетика, а по потреба и меѓусебно и со други оператори и
- донесат и да применуваат програма за обука за вработените во врска со сајбер безбедност.

Имајќи ја предвид сериозноста и потребата од сајбер-одбраната, како компатибилен дел од целокупната сајбер безбедност, новата регулатива за сајбер безбедност се воспоставува како стандард за енергетски компании од електроенергетскиот сектор. Со цел да се обезбеди сигурност во снабдувањето со електрична енергија и да се намалат ризиците од нарушување на континуирано снабдување со електрична енергија, Регулаторната комисија за енергетика и водни услуги на 08.06.2023 донесе Правила за сајбер-безбедност[7]. Со правилата за сајбер-безбедност во секторот за електрична енергија, се уредуваат стандардите за сајбер-безбедност во секторот за електрична енергија, мерките и активностите за воспоставување на сајбер безбедносна култура и се очекува да се подигне свесноста за заканите кај сите чинители во секторот за електрична енергија. Правилата се со одложено важење од шест месеци и почнуваат да важат од јануари 2024 година.
Една од пропишаните законски обврски е и сертифицирање на операторите согласно меѓународни стандарди, како што е стандардот „ISO/IEC 27001:2022 - Безбедност на информации, сајбер безбедност и заштита на приватноста“ во однос на посебниот дел за сајбер безбедност.

3.1.1.2. Стратешки документи

Национална стратегија за сајбер безбедност на Република Македонија 2018 - 2022 година

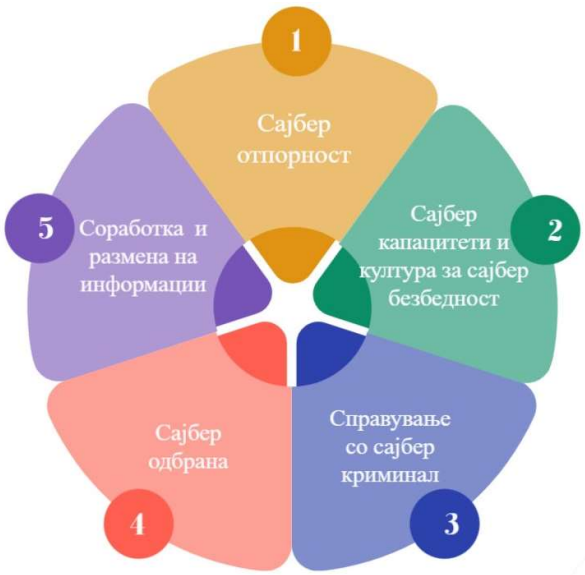
Во јули 2018 година од страна на Владата донесена е „Национална стратегија за сајбер безбедност на Република Македонија 2018 - 2022 година”[8]. Истата претставува стратешки документ кој треба да служи како патоказ за развој на сигурно, безбедно, доверливо и отпорно дигитално опкружување, поддржано од квалитетни капацитети, кои се базираат на доверба и соработка во полето на сајбер безбедноста.
За имплементација на стратегијата, во ноември 2018 година од страна на Владата донесен е Акциски план за стратегијата[9] кој содржи цели, активности и рокови за нивно спроведување. Приоритетни активности во Акцискиот план се следните:

[7] Регулаторна комисија за енергетика и водни услуги на Република Северна Македонија (erc.org.mk)
[8] https://www.mioa.gov.mk/?q=mk/node/1813
[9] https://www.mioa.gov.mk/?q=mk/node/1813

- формирање на Национален Совет за сајбер безбедност;
- формирање на тело со оперативни капацитети за сајбер безбедност како новоформиран самостоен орган (агенција, дирекција) или како новоформирана организациска единица, односно орган во рамки на постоечки орган;
- изработка на студија за идентификација на КИИ и ВИС.

Во рамките на стратегијата утврдени се пет цели прикажани на следнава слика:

Слика број 3 – Утврдени цели на Националната стратегија за сајбер безбедност на Република Македонија 2018 - 2022 година



Од предвидените активности во рамки на Цел 1, донесена е **Национална таксономија за сајбер инциденти** [10]**.** По предлог на АЕК, истата е донесена од страна на Владата во 2020 година. Националната таксономија за сајбер инциденти претставува категоризиран стандард и кореспондира со референтната таксономија за сајбер-инциденти на ENISA[11] и со истата се изедначуваат критериумите при класификација на настаните во ИКТ системите. Со Националната таксономија сите институции од владиниот, јавниот и приватниот сектор, како и операторите на критична информациска инфраструктура во државата, кои разменуваат информации за настани поврзани со компјутерска безбедност, ќе имаат еднакво разбирање за случувањата и контекстот на настанот за кој се разменуваат информации.

[10] 79-та седница на Владата на РСМ, точка 16, арх.бр. 44-5898/1 од 05.08.2020 година

[11] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport

Исто така со Цел 1 предвидена е активност за идентификација и заштита на КИИ и ВИС, со која треба да се дефинира листа на КИИ и ВИС врз основа на Студија за дефинирање и идентификација а која ќе биде усогласена со НИС директивата, но истата не е реализирана заради недонесена законска рамка.

Нова нацрт Национална стратегија за сајбер безбедност 2023-2027 е подготвена и објавена на ЕНЕР на 20.12.2023 година и е на меѓуинституционално разгледување и усогласување, пред истата да биде доставена до Влада.

Национална ИКТ стратегија

Националната ИКТ стратегија има за цел да постави јасен патоказ за подобра дигитализација на општеството, со што директно влијае врз квалитетот на животот на граѓаните. Преку стратегијата се наметнува максимална дигитализација на работните процеси кај правните лица (институции и бизниси), давајќи можност за употреба на иновативни решенија со кои се елиминира употребата на хартијата.
Последната усвоена ИКТ стратегија е за периодот 2016-2017 година.

Нацрт Националната стратегија за ИКТ 2020 – 2025 е изработена според условите на проектот финансиран од ЕУ „Изработка на долгорочна Национална стратегија за ИКТ 2020 - 2025“[12] склучен според сервисниот договор ФВЦ СИЕА 2018 (FWC SIEA 2018). Истата е изработена во нацрт фаза на 05.10.2020 година.

Од страна на МИОА извршена е промена на годините предвидени за имплементација на стратегијата на 2021-2025, наместо 2020-2025, од причина што пандемијата предизвикана од корона-вирусот го отежна спроведувањето на планираните активности и предизвика одложување на навременото усвојување на Стратегијата од страна на Владата. Оваа нацрт верзија е објавена на ЕНЕР порталот на 10.06.2021 година како нацрт верзија „Националната ИКТ стратегија 2021 – 2025 верзија1.1“[13]. Заедно со стратегијата изработен е и Акциски план за Националната ИКТ стратегија[14].

Дополнително изготвена е нова нацрт Национална ИКТ стратегија 2023-2030 која е објавена на ЕНЕР на 22.12.2023 година и истата е на меѓуинституционално разгледување и усвојување пред нејзиното доставување до Влада.

Стратегијата претставува документ во кој се детализирани повеќекратните фактори кои влијаат на инвестирањето на институцијата во информацискатa безбедност при што треба да се опфатат сите аспекти на управување со технологијата, вклучително и управувањето со трошоците, човечкиот капитал, хардверот и софтверот, добавувачите и ризикот.

[12] Договор бр. 201/408197
[13] https://ener.gov.mk/Default.aspx?item=newdocumentdetails&detalisId=23
[14] https://ener.gov.mk/Default.aspx?item=newdocumentdetails&detalisId=27

Последната Национална ИКТ стратегија е со важност до 2017 година додека последната Национална стратегија за сајбер безбедност е со важност до 2022 година. И покрај тоа што се подготвени, Нацрт Националната ИКТ стратегија и Нацрт Националната стратегија за сајбер безбедност се уште се наоѓаат во постапка на меѓуинституционално усогласување. Отсуството на стратешки документи како сет на активности и мерки, не обезбедува безбедна, отпорна и доверлива дигитална средина која влијае државата да биде безбедно место за он-лине делување и работа со напредни човечки и технички капацитети.

Со Заклучок[15] на Влада усвоен е Патоказ за дигитална трансформација (2024-2026-2028-2030) со кој се задолжуваат органите на државната управа, а им се препорачува на институциите кои немаат статус на органи на државна управа, да ги усогласат стратешките документи и планови со Патоказот за дигитална трансформација (2024-2026-2028-2030).

Во Патоказот за дигитална трансформација, во делот на Пристапи кон процесот за дигитална трансформација - Насоки за оптимални резултати од дигитализацијата, точка 9 упатува на интегрирање на мерките за сајбер безбедност како стандарди во инфраструктурата и обработката на податоците во насока на заштита и отпорност на системите од сајбер напади и гаранција на интегритет на податоците.

3.1.1.3. Национален совет за сајбер безбедност

Со Одлука[16] на Влада формиран е Национален совет за сајбер безбедност за координација и следење на спроведените активности согласно „Националната стратегија за сајбер безбедност на Република Македонија 2018-2022“ и Акцискиот план на Националната стратегија за сајбер безбедност на Република Македонија 2018-2022, како и дефинирање на нови стратешки насоки и препораки поврзани со сегментот на сајбер безбедност.

Советот го сочинуваат тројца членови и заменици на членовите на Советот, а тоа се министрите за информатичко општество и администрација, одбрана и внатрешни работи како и нивните заменици.

Согласно Одлуката предвидено е советот да се состанува најмалку еднаш месечно, а по потреба и почесто и за својата работа да доставува годишен извештај до Владата најдоцна до 31 март во тековната година за претходната година. Начинот на работа на Советот како и начинот на соработка и размена на информации со други државни органи, институции и засегнати страни од областа на сајбер безбедноста е уреден со Деловник за работа[17] донесен на првата седница на Советот на која е избран и

[15] Бр. 41-807/2 од 16 јануари 2024 година.
[16] Број 45-7326/1 од 2 октомври 2019 година.
[17] Број 08/1-240/1 од 10.01.2020 година.

секретар на Советот[18] и меѓуресорска работна група[19] за стручно-оперативна поддршка.

Ревизијата утврди дека Советот од неговото формирање до периодот на известување од ревизијата се состанал само еднаш. На ревизијата не и беа презентирани:

- годишни извештаи за работата на Советот доставени до Владата заради нејзино информирање;
- конкретни мерки предложени за подобрување на имплементацијата на Стратегијата и Акцискиот план;
- соодветни мерки за поголема ефикасност за управување со сајбер кризи итн.

со кои документи и активности би се потврдиле дејствијата и ангажманот на Советот во периодот за кој е вршена ревизијата.

Нефункционалноста на Советот ја доведува во прашање ефективноста, ефикасноста и релевантноста во справувањето со современите и идните предизвици за сајбер безбедноста, улогата и способноста да функционира за време на сајбер-криза.

3.1.2. Финансиски, технички и административни капацитети за заштита на критичните информациски системи

3.1.2.1. Институционални капацитети за заштита на критични информациски системи

Градењето и одржувањето на институционалните капацитети ќе придонесе за сеопфатен и ефективен пристап за заштита на критичните информациски системи од заканите кои постојано се развиваат. Редовните ажурирања, обуките и адаптацијата на новите технологии и закани се клучни за обезбедување на тековната безбедност на овие системи.

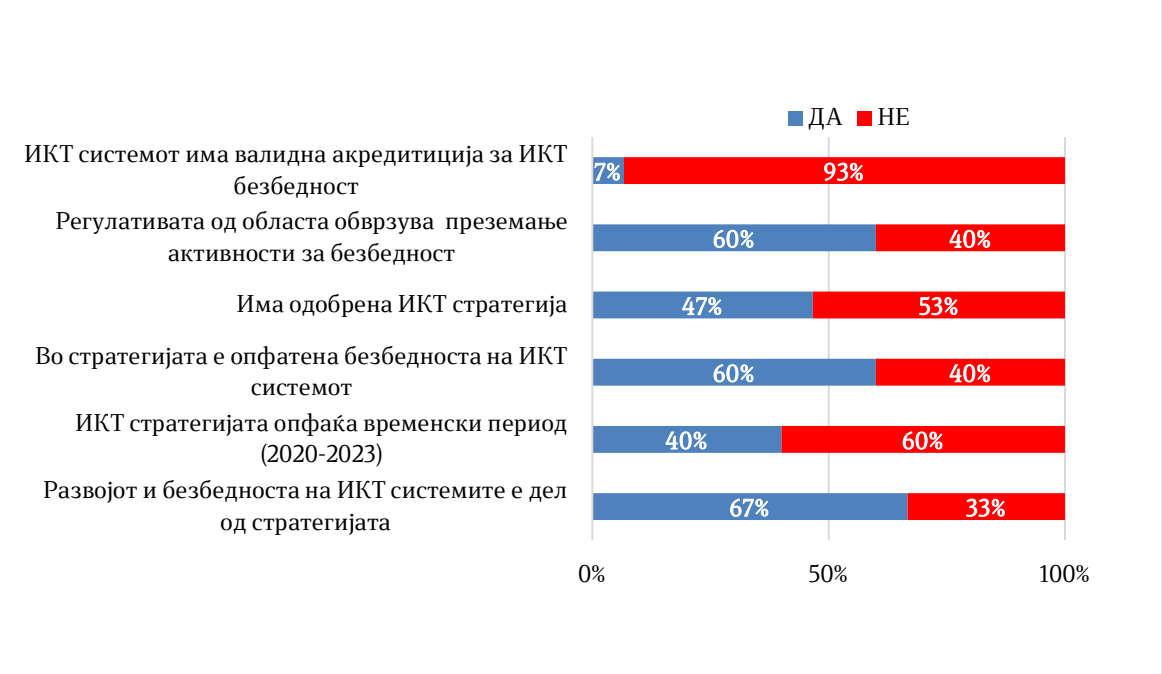
Институциите за поефикасно справување со информацискатa безбедност во своите стратешки документи треба да дефинираат цели, приоритети, активности, ресурси и одговорности за заштита на ИКТ системите и податоците кои ги обработуваат. Тоа ќе доведе до конзистентни, доволни и навремени активности во примената на информациските политики, процедури и контроли. Истото може да се направи како посебен план за информациска безбедност или да бидат дел од постојните ИКТ стратегии.

По извршената анализа на добиените одговори на доставените прашалници кај институциите опфатени со примерокот, состојбата со ИТ управување во делот на

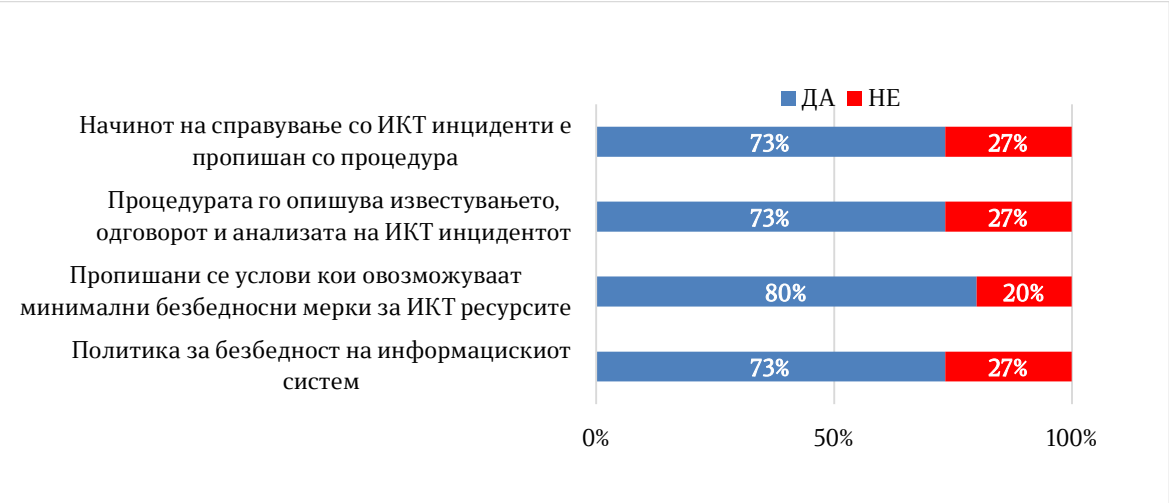
[18] Решение број 08/1-240/2 од 10.01.2020 година.
[19] Решение број 08/1-240/3 од 10.01.2020 година.

стратешки документи како и мерки и стандарди за информациска безбедност, се презентирани на графикон број 4 и 5.

Графикон број 4 - Стратешки документи за информациска безбедност



Графикон број 5 - Пропишани мерки и стандарди за информациска безбедност



Анализата покажа дека кај 53% од институциите кои го одговориле прашалникот не е одобрена ИКТ стратегијата додека 40% воопшто ја немаат опфатено информациската безбедност во стратешките документи. Само една институција

поседува сертификат за информациска безбедност. Пропишаните документи за постапување и одговор по ИКТ инциденти отсуствуваат кај 27% од институциите.

Преземањето на соодветни мерки за информациска безбедност на ИКТ системите во голема мерка зависи од целосноста во евиденцијата со сите ИКТ ресурси како и состојбата во која истите се наоѓаат.

Евиденцијата на ИКТ средствата е неопходна во информацискатa безбедност заради потребата од нивна анализа и утврдување на ризичните места по безбедноста на оваа опрема. Тоа е предуслов за планирање на мерки за нивно надминување.

Користењето на уреди за кои повеќе не се произведуваат резервни делови, апликативен софтвер кој повеќе не е поддржан од производителот, востановените безбедносни слабости во софтверите и неможноста за нивна надградба со понови верзии за надминување на тие слабости се примери за ранливости на информацискатa безбедност на ИКТ системите.

Со анализата од добиените одговори на прашалниците, утврдивме дека 20% од институциите немаат целосна евиденција за состојбата на ИКТ средствата при што истото е прикажано на графикон број 6.

Графикон број 6 - Евиденција на ИКТ ресурси

Погоре утврдените состојби покажуваат недоволни институционални капацитети и носат ризици од:

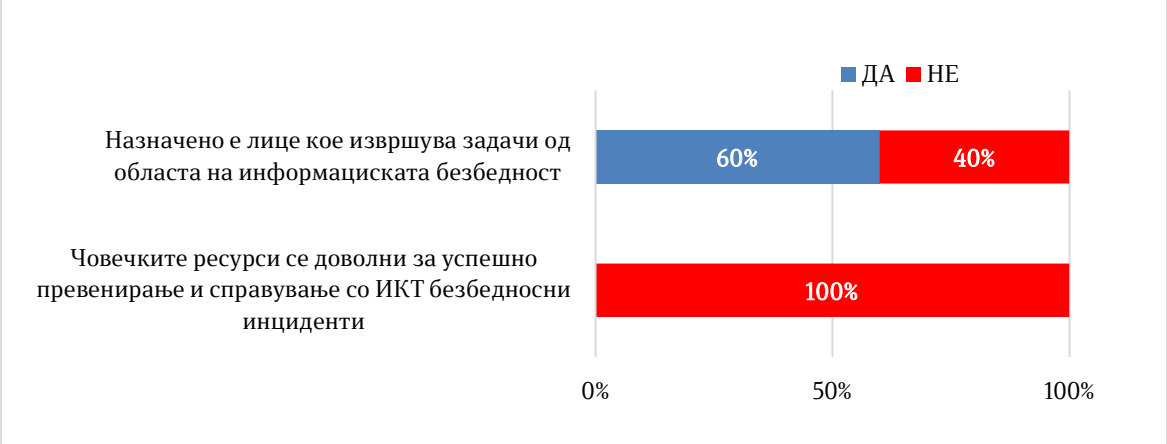
- зголемена ранливост на сајбер закани;
- неефективно управување со инциденти;
- ограничена подготвеност за сајбер-безбедносни инциденти;
- несоодветна распределба на ресурси;
- регулаторни ризици и ризици за усогласеност;
- недостаток на координација и комуникација;
- ослабена култура на информациска безбедност;
- зголемена веројатност за непропустливо нарушување на оперативниот ризик за координација на податоци;
- тешкотии во демонстрирање на зрелост за сајбер-безбедност.

3.1.2.2. Кадровска екипираност за заштита на критични информациски системи

Човечките ресурси со соодветни квалификации, знаења и вештини имаат најголемо значење во информацискатa безбедност. Со зголемувањето на бројот на информациските инциденти, побарувачката за квалификувани професионалци кои можат да ги заштитат ИКТ системите од се пософистицираните сајбер закани значително е во пораст, што го прави процесот на нивно ангажирање, а во исто време и задржување и мотивирање на постоечкиот кадар, особено предизвикувачки и со зголемена побарувачка од овој кадар.

Од одговорите на прашалниците доставени до институциите за состојбата со човечките ресурси, ревизијата утврди дека кај сите институции нема доволно човечки ресурси за превенирање и справување со ИКТ безбедносни инциденти додека кај 40% од институциите не е назначено лице одговорно за информациска безбедност[20], со цел навремено пријавување на инциденти и размена на информации за инциденти, ранливост, закани и ризици поврзани со безбедноста на информациските системи до Националниот центар за одговор на компјутерски инциденти MKD-CIRT. Ваквите состојби се прикажани на графиконот број 7.

Графикон број 7 - Човечки ресурси за информациска безбедност



Потребата од експерти за информациска безбедност во една институција се од клучно значење за заштита на ИКТ ресурсите, одржување на безбедна компјутерска средина, воспоставување на цврста одбрана против многубројните еволуирачки сајбер закани и одржување на доверливоста, интегритетот и достапноста на ИКТ ресурсите на институцијата.

Заради се поголемиот број на ИТ безбедносни инциденти во светот, профилот на ИТ експерти за информациска безбедност во моментов се меѓу најбараните и

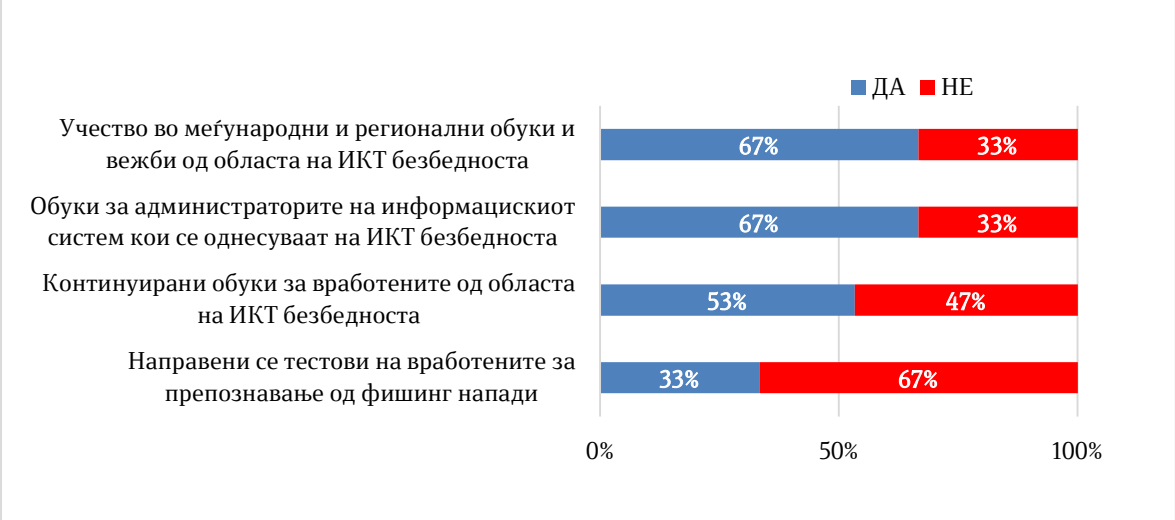
[20] Утврдено со заклучок на Влада на 131-ва седница од 21.02.2023

најдефицитарните од сите во ИТ секторот, особено со фактот дека членови на овие тимови можат да бидат само високо стручни ИТ професионалци кои континуирано се надградуваат со нови обуки.

Во постојната регулатива, исто така не е уредено кои лица можат да извршуваат работни задачи од областа на информацискатa безбедност, вклучително и за лицата кои се ангажирани за оваа намена преку трети страни т.е. надворешни компании и експерти од областа.

Од извршената анализа на одговорите на прашалниците, утврдивме дека во институциите потребни се дополнителни обуки за подигање на свесноста на вработените за ИКТ безбедност како и тестирање за проверка на свесноста меѓу другото и за препознавање на фишинг напади. Истото е прикажано на графикон број 8.

Графикон број 8 - Обуки за информациска безбедност



Дополнително ревизијата изврши увид во податоците во ЕСЈН системот, во делот на склучени договори за набавки кои се однесуваат на обуки и утврди дека за периодот 2020-2023 година има вкупно 9 склучени договори за потребите на МКД-ЦИРТ, додека од останатите субјекти не се евидентирани посебни набавки за обуки.

Со Заклучок на Влада[21] се врши задолжување на сите органи на државна управа, а им се укажува на институциите кои не се органи на државна управа, сите вработени задолжително да се регистрираат и да завршат една од следните он-лине обуки:

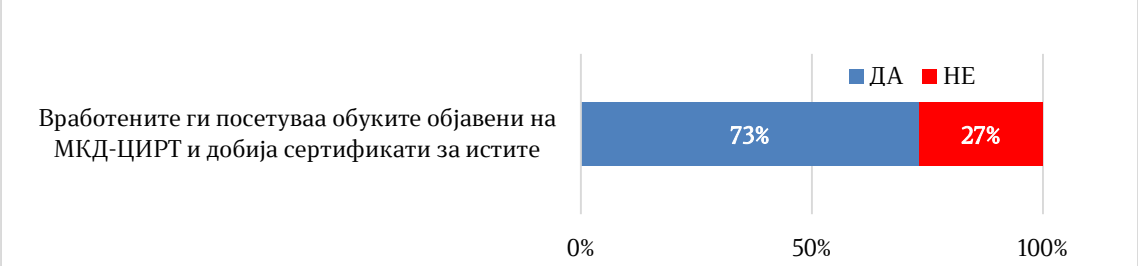
- основна обука за сајбер безбедност за вработени во јавната администрација и вработени во приватниот сектор или
- основна обука за сајбер безбедност за менаџерски и раководен персонал во јавен и приватен сектор

[21] Заклучок на Влада на 131-ва седница од 21.02.2023

кои се достапни на веб-локацијата: https://lms.mkd-cirt.mk/, во рок од 90 дена.

Посетеноста на он-лине обуките за информациска безбедност објавени на МКД-ЦИРТ а утврдена од дадените одговори на прашалниците е прикажана на графиконот број 9.

Графикон број 9 - Посетени он-лине обуки за информациска безбедност



Процентот на посетеност од 73% на обуките од страна на вработените во институциите кои одговорија на прашалникот, не претставува реална слика за состојбите на вработените во јавната администрација бидејќи според податоците на МКД-ЦИРТ заклучно со декември 2023 година, повеќе од 19.500 лица ги посетиле обуките што во однос на расположливите достапни податоци од 129.374 лица вработени во јавната администрација[22], има за ефект недоволно подигнување на јавната свест за информациска безбедност и превенција од безбедносни инциденти.

Обуките се најдобриот начин за едукација и подигнување на свеста на вработените за ризиците што треба да ги избегнуваат и активностите што треба да ги преземаат при препознавање на сомнителни ситуации за можни информациски безбедносни инциденти.

3.1.2.3. **Финансиски ресурси за заштита на критичните информациски системи**

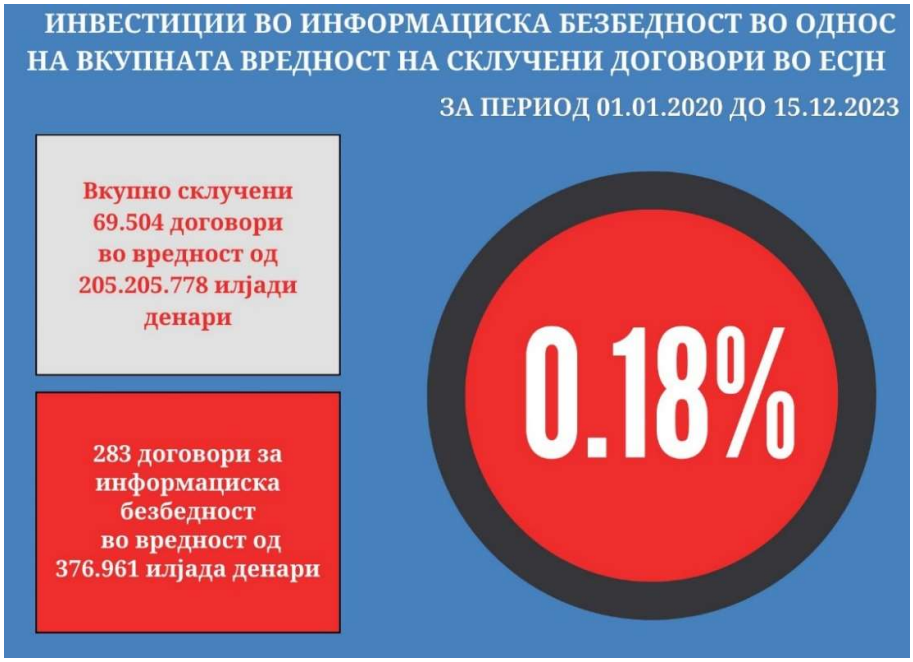
Регистар на операторите на критична инфраструктура – КИИ и ВИС не е утврдена поради отсуство на законски пропишана регулатива. Ваквата состојба оневозможува утврдување на инвестициите од областа на информациската безбедност и вкупна вредност на истите. Од тие причини ревизијата направи анализа на вредноста на склучените договори објавени во ЕСЈН на сите државни субјекти чиј предмет на набавка е од областа на информациската безбедност.

Во анализата не се вклучени инвестициите од оваа област кои се спроведуваат преку меѓународни проекти и грантови од институциите.

Ревизијата ги анализираше податоците на склучени договори од системот на ЕСЈН, за периодот 01.01.2020 до 15.12.2023 година, при што потврдивме вкупно 69.504 склучени договори во вкупна вредност од 205.205.778 илјади денари, од кои за 67.913 склучени договори во вкупна вредност од 189.378.401 илјада денари евидентиран е

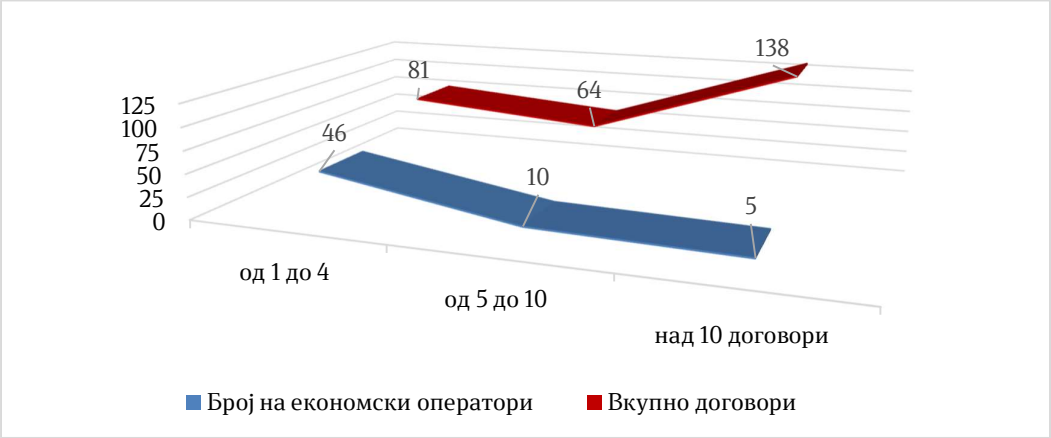
[22] Извештај од регистарот на вработените во јавниот сектор

запис со број на јавна набавка, додека кај 1.591 склучен договор со вкупна вредност од 15.827.377 илјади денари евидентиран е запис без број на јавна набавка. Притоа за набавки поврзани со областа на информацискатa безбедност склучени се 283 договори со 61 економски оператор во вкупна вредност од 376.961 илјада денари, што претставува 0,18% од вкупната вредност на склучени договори, прикажано на слика број 10 :



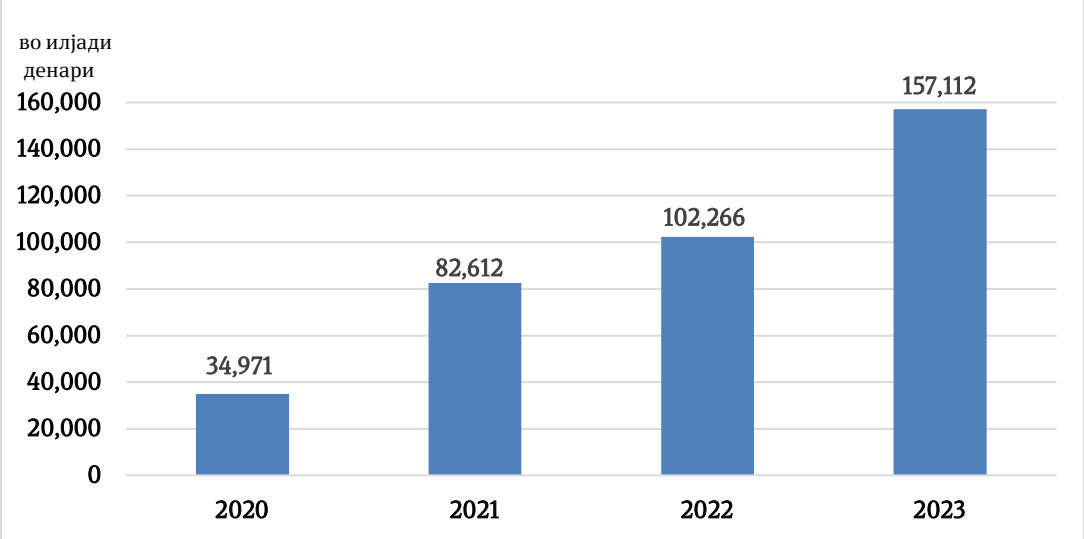
Анализата на склучените договори со економските оператори покажува дека 5 економски оператори од вкупно 61 имаат склучено повеќе од 10 договори од областа на информацискатa безбедност и истата е дадена на графикон број 11.

Графикон број 11 - Број на склучени договори



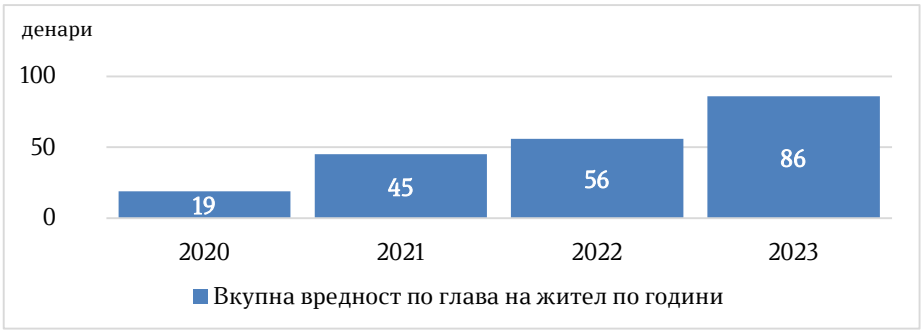
Анализа на вкупната вредност на склучени договори од областа на информацискатa безбедност објавени во системот на ЕСЈН, по години е прикажана на графикон број 12.

Графикон број 12 - Вкупна вредност на склучени договори од областа на информацискатa безбедност објавени во системот на ЕСЈН



Со споредба на податоците од пописот на населението во 2021 година и вкупната вредност на склучени договори според системот на ЕСЈН за информациска безбедност на годишно ниво, на графиконот број 13 се прикажани годишни инвестиции по глава на жител, изразени во денари:

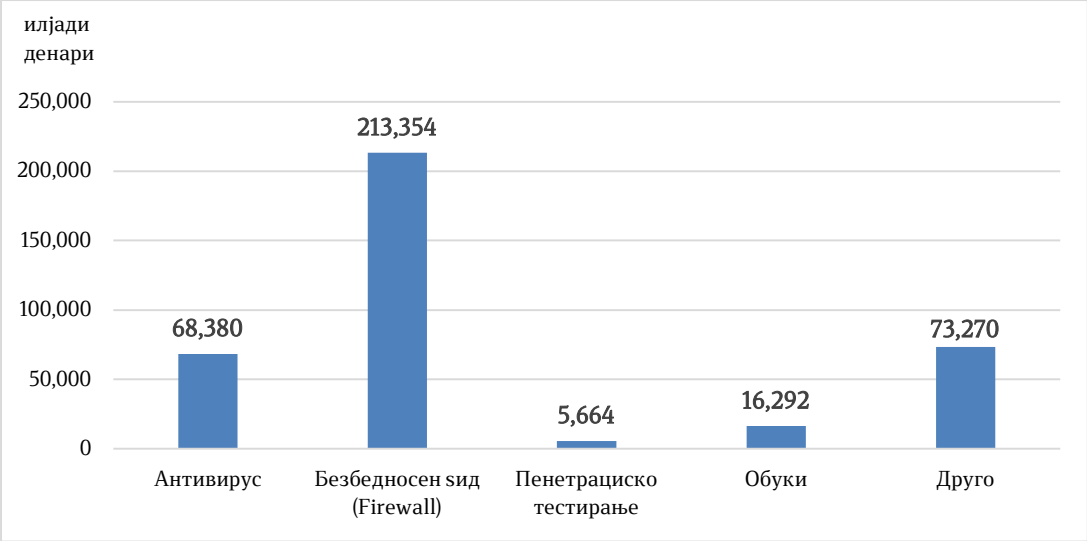
Графикон број 13 - Вкупна вредност на склучени договори за информациска безбедност по глава на жител



Пресметките покажуваат дека за информациска безбедност во 2022 година се инвестирани 56 денари по глава на жител, а во 2023 година 86 денари или 1,4 EUR годишно по глава на жител. Имајќи го во предвид значењето на информацискатa безбедност, бројот на ИКТ системи и штетите што можат да настанат, недоволното инвестирање во областа претставуваат ризик да не се преземат сите потребни мерки и активности за справување со информацискатa безбедност и намалување на ранливоста на ИКТ системите.

Анализата на склучените договори по предмет на набавки од областа на информацискатa безбедност е претставена на графикон број 14.

Графикон број 14 - Вкупна вредност на склучени договори за период 01.01.2020 - 15.12.2023



Согласно склучените договори, инвестициите во сите државни институции за набавка на безбедносна заштита - антивирус се помалку од 300 илјади евра годишно, а за безбедносен ѕид (Firewall) се околу 850 илјади евра годишно.

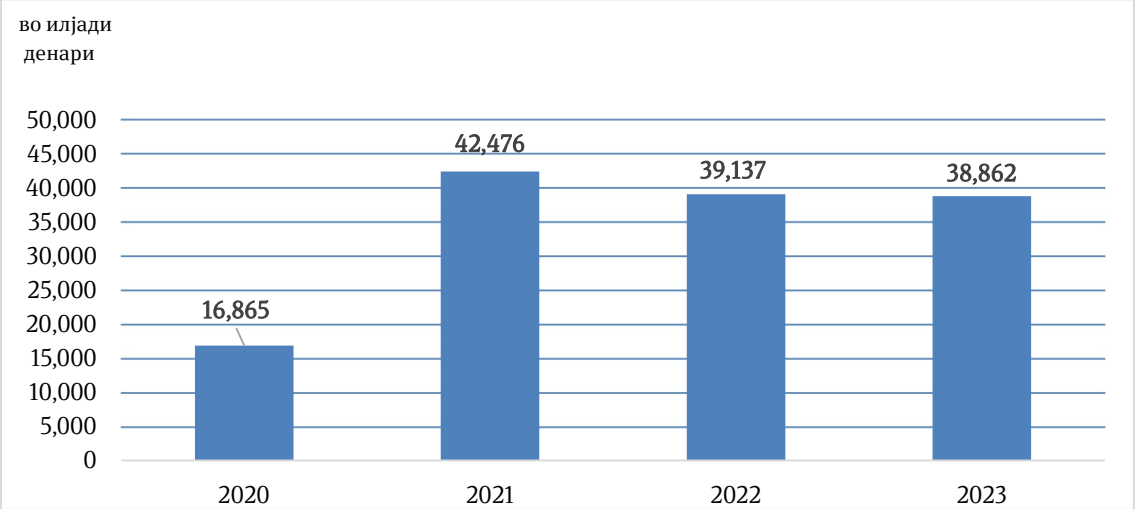
Во делот на други набавки голема ставка претставува договорот на еден договорен орган кој има потпишано договор за ЦИРТ во вредност од околу 28 милиони денари во 2023 година.

Со анализа на податоци добиени од системот на ЕСЈН, за набавки за пенетрациско тестирање во периодот опфатен со ревизија, склучени се вкупно 10 договори за проверка на безбедноста на ИКТ системите. Овие договори се склучени од само 6 институции од сите јавни институции кои се во системот на ЕСЈН.

Со ваквиот тип проверки на информациска безбедноста се врши тестирање и одредување на состојбата и слабостите на ИКТ системите на институциите, без која не може да се утврди степенот на безбедност на ИКТ системите.

Исто така, направивме анализа на вредноста на склучените договори на јавните набавки на АЕК, во делот на набавки за потребите на МКД-ЦИРТ, што е прикажано на графикон број 15.

Графикон број 15 - Вкупна вредност на склучени договори од АЕК за МКД ЦИРТ објавени во системот на ЕСЈН



АЕК за потребите на МКД-ЦИРТ, во периодот од 01.01.2020 до 15.12.2023 година има вкупно 25 склучени договори за набавки во вкупна вредност од 137.339 илјади денари, од кои девет договори се за обуки, меѓународни вежби или конференции.

Ваквите утврдени состојби на недоволно инвестирање претставуваат ризик да не се преземат сите потребни мерки и активности за справување со информацискатa безбедност и намалување на ранливоста на ИКТ системите, а имајќи го во предвид значењето на информацискатa безбедност на ИКТ системи и штетите што можат да настанат кај истите.

Воедно состојбите со тестирање за информацискатa безбедност и обуките покажуваат на недоволно преземени активности за информациска безбедност од страна на институциите за прецизно одредување на ризиците и мерките за нивно намалување и превентивно зголемување на знаењето кај вработените за заштита и справување на ризиците поврзани со информациска безбедност.

3.2. ИТ Операции

3.2.1. Координација помеѓу органите и институциите во справување со безбедносни инциденти

Употребата на информатичко комуникациската технологија и информациските системи и развојот на електронските услуги го зголемува ризикот од безбедносни инциденти и злоупотреби, што ги прави овие закани едни од посериозните врз националната безбедност. Во последните години сајбер заканите се меѓу најзначајните безбедносни закани, што е основна причина истите да се третираат како интегрален дел од националната и меѓународната безбедност. Зголемената потреба од електронски услуги во интернет просторот значи дека нефункционалните ИКТ системи и сериозните безбедносни напади можат да имаат значително негативно влијание врз функционирањето на јавниот и приватниот сектор, како и на целото општеството. Неопходноста од новите технологии и потребата од поголема достапност на услугите во интернет просторот е причина повеќе корисниците и институциите да ја зголемат свесноста за значењето на интегритетот, достапноста и доверливоста на податоците. Македонските комуникациски мрежи се дел од глобалните комуникациски мрежи, што подразбира дека сајбер безбедносните инциденти на друго место можат да влијаат врз македонскиот сајбер простор и услуги, и обратно.
Справувањето со инцидент вклучува три функции: пријавување на инцидентот, анализа на инцидентот и одговор на инцидентот. Функцијата за пријавување на инцидентот му овозможува на CSIRT да служи како централна точка за контакт за пријавување на локалните проблеми. Ова овозможува сите извештаи и активности за инцидентите да бидат собрани на едно место каде што информациите може да бидат разгледани и поврзани во рамки на матичната институција. Ова претставува еден дел од функцијата за анализа на инцидентот. Другиот дел од оваа функција претставува преземање на подлабоко разгледување на извештајот за инцидентот со цел да се утврди обемот, приоритетот и заканата заедно со истражување за можните одговори и ублажувања. Функциите за одговор на инцидентот може да бидат во различни форми. CSIRT може да испрати препораки како да се направи опоравување и спречување на понатамошни инциденти, па потоа системските и мрежните администратори да ги извршат тие задачи сами или CSIRT може сам да ги изврши задачите врз погодениот систем. Одговорот може да вклучува и размена на информации и научени лекции со други соодветни тимови и институции. Овие функции за справување со инциденти се реактивни услуги кои CSIRT може да ги понуди.

Сајбер отпорноста обезбедува доверливост, интегритет и достапност преку идентификација, заштита и воспоставување на претходна состојба од сајбер инциденти. Јавниот и приватниот сектор мора да имаат навремени и точни информации и предлози за подобрување на сајбер безбедноста и да бидат во

можност меѓусебно да соработуваат во случај на сајбер инциденти. Потребно е да се идентификуваат сите релевантни капацитети за сајбер безбедност кај сите засегнати страни и преку дефинирање на конкретни надлежности и активности да се стават во функција на подобрување на сајбер безбедноста и во функција на справување со сајбер инциденти. Целта е да се обезбеди заштита на најважниот дел од инфраструктурата во државата, користење на соодветни решенија за одбрана на државните интереси од страна на надлежните институции и подготвеност за сериозни (комплексни) сајбер инциденти.

3.2.1.1. Активности на МКД-ЦИРТ за намалување на ризиците од безбедносни инциденти

Со Законот за електронските комуникации во состав на АЕК се формира Национален центар за одговор на компјутерски инциденти MKD-CIRT, како Национален CSIRT на Република Северна Македонија, кој претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

МКД-ЦИРТ во Правилникот за систематизација на работните места во АЕК е систематизиран како сектор со две одделенија:

- Одделение за одговор на компјутерски инциденти и
- Одделение за процена на ризици по информациска безбедност.

За својата работа МКД-ЦИРТ секоја година подготвува годишна програма и годишен извештај за работата кои се доставуваат од АЕК и се усвојуваат од Владата.

Владата на 131-та седница одржана на 21.02.2023 година, во делот Агенда за дигитална трансформација усвојува информација со предлог-мерки за подобрување на безбедноста на информациските системи во институциите од јавниот сектор, каде се задолжуваат сите органи на државна управа, а им се укажува на институциите кои не се органи на државна управа да направат план за реализација и да ги предвидат финансиските импликации на мерките на Националниот центар за одговор на компјутерски инциденти MKD-CIRT, достапни на веб-локација: https://aek.mk/en/soopstenie/, во рок од 90 дена односно до 21.05.2023 година. Мерките ги предвидуваат следниве активности:

Услугите коишто се во надлежност на МКД-ЦИРТ за конституентите, граѓаните, јавниот и приватниот сектор се поделени во неколку групи: реактивни, проактивни и услуги за управување со квалитетот на безбедноста.

Реактивните услуги вклучуваат известувања од страна на конституент по настанат инцидент или други настани во врска со закани и напади како на пример:

компромитиран уред, штетен софтвер/малвер, ранливост или друг тип на слични инциденти. По пријава на инцидент МКД-ЦИРТ постапува со мерки кои имаат за цел спречување на ширење на инцидентот, намалување на штетата, опоравување од настанатиот инцидент и споделување на искуството во насока на идна превенција.

Проактивните услуги имаат за цел детекција и превенција на нападите пред истите да се случат. Во оваа категорија на услуги, информациите и знаењето со кои располага тимот на МКД-ЦИРТ се дистрибуира до конституентите и соработниците со цел тие да ги заштитат своите средства и да не станат цел на напади.

Услугите за управување со квалитетот на безбедноста имаат за цел промена и подобрување на постојни и етаблирани услуги кои се независни од управување со инциденти и најчесто ги реализираат други оддели кај конституентите (организациони единици за ИТ, ревизија и сл.) Информациите и знаењето со кое располага тимот на МКД-ЦИРТ ќе помага во подобрување на безбедносните аспекти кај услугите кои ги реализираат конституентите. Цел е да се идентификуваат ризиците, заканите и слабостите на информациските системи кај конституентите.

МКД-ЦИРТ во своето работење обезбедува услуги за: известувања и предупредувања, далечински одговор на инцидент, одговор на ранливост, основна свест, едукација и обука, координација на одговор на инцидент, напредна свест, едукација и обука, координација на одговор на ранливост, анализа на закани и ранливости. Поради недостаток на ресурси пред се човечки, спроведувањето на напредните услуги: одговор на инцидент на лице место, форензичка анализа и безбедносна проценка и ревизија, со секоја годишна програма се одложуваат за наредни години.

Со увид во актот за систематизација до 2023 година утврдивме дека од пет систематизирани работни места, пополнето било само едно до 2022 година т.е. две работни места во 2022 година. Со новиот акт за систематизација од 2023 година[23], утврдивме дека МКД-ЦИРТ од предвидени 11 систематизирани работни места, пополнети се само 3 што претставува само 27% пополнетост на предвидените работни места што покажува на недоволно човечки ресурси за извршување на предвидените работни задачи.

МКД-ЦИРТ со цел да ги реализира своите активности, во периодот предмет на ревизија, има спроведено повеќе јавни набавки на услуги и склучено договори со трети страни за нивно обезбедување како што се:

- Услуга - Систем за управување со сајбер ризици, закани и ранливости на национално ниво, со цел „континуирано да врши мониторинг за ризици, да добива информации за компјутерски закани и инциденти (по автоматски пат или

[23] https://aek.mk/wp-content/uploads/aek_private/Pravilnik%20za%20sistematizacija%201102-13-10.pdf

од трети страни) и постојано да располага со показатели за малициозен сообраќај што доаѓа или излегува од државата“. Овој систем е од највисок приоритет бидејќи е основа за точна информација за актуелните закани, ризици и нивото на загрозеност на државата од сајбер-напади и треба да овозможи моментален и актуелен увид, мерење, следење и истражување на ризици во врска со компјутерската безбедност на национално ниво, на ниво на критични сектори во државата и на ниво на организации кои се оператори на критична информациска инфраструктура во државата. Услугата е овозможена за вкупно 50 институции.

- Услуга - Систем за управување со компјутерски инциденти и сајбер безбедносни настани и информации, со цел управување со компјутерски инциденти и сајбер безбедносни настани и информации за потребите на МКД-ЦИРТ, обезбедено е одржување и надградба на постојни софтверски апликации кои се дел од овој систем, имплементација на нови софтверски решенија базирани на отворен изворен код, како и поддршка за управување и одговор по инцидент. Услугата е овозможена за вкупно 20 институции, при што за секоја овозможен е увид во состојбата од нивниот систем.
- Услуга - Систем за сајбер-безбедносен надзор над мрежните инфраструктури, со цел да овозможи централизиран надзор и информирање за сајбер закани, напади, инциденти и ранливости од дистрибуирани компјутерски мрежни инфраструктури односно интегрирано решение за сајбер-безбедносен надзор, анализа и заштита на мрежен IP сообраќај за потребите на АЕК и други оддалечени институции и локации. Притоа овозможено е следење на сообраќајот во реално време и можност за детекција и приоретизирање на различни типови на закани, напади и настани од безбедносен карактер. Услугата е овозможена за вкупно 20 институции.
- Услуга за надворешна сајбер-безбедносна проверка (скенирање на веб-сајтови), која овозможува секоја организација самостојно да врши проверки, а истовремено Националниот центар за одговор на компјутерски инциденти MKD-CIRT да има кумулативен и детален увид во секој извештај по завршено скенирање/проверка. Вкупно 110 веб сајтови страни се скенираат од вкупно 74 институции.
- Услуги за едукативни видеа, он-лине квизови и конференции за сајбер безбедност за зголемување на отпорноста на сајбер напади за јавниот, владиниот и приватниот сектор како и на операторите на критични информациски системи. Притоа изработени се анализи на злонамерни содржини како и едукативни видеа за сајбер безбедност. Организирани се и вежби, конференции, натпревари и обуки во кои ИТ експерти вработени кај конституентите се стекнаа со меѓународно признати сертификати. Изработени се и он-лине обуки за сајбер безбедност за јавна администрација и за раководство кај менаџерски и раководен персонал во јавен и приватен сектор со можност за сертифицирање по истите, за кои информации се дадени во точка 3.1.2.2.

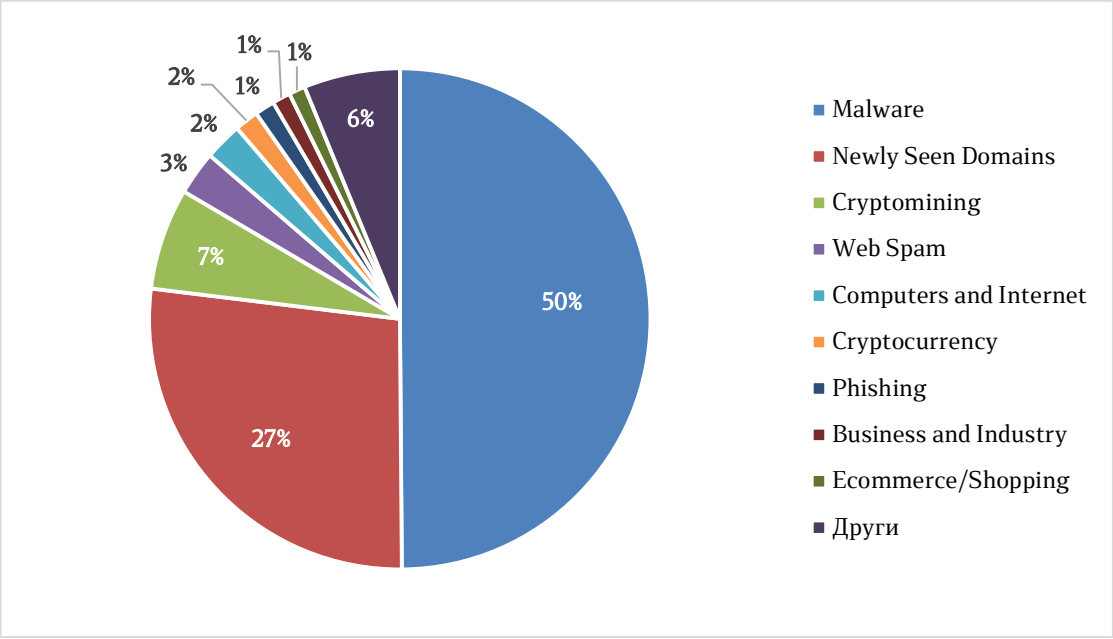
Во рамките на МКД-ЦИРТ системот има виртуелни серверски имплементации на кои функционираат:

- Апликација за пријава на инциденти;
- Апликација за рано предупредување веб закани;
- Систем за управување со корисници – CRM

МКД-ЦИРТ на својата веб страна https://mkd-cirt.mk/antibotnet/maliciozni-domeni/ има објавено ажурирана листа на идентификувани малициозни, потенцијално малициозни и непознати домени со категорија т.е. причина за идентификацијата, собрани преку Системот за сајбер-безбедносен надзор на мрежна инфраструктура на МКД-ЦИРТ. Притоа препорачано е да се блокираат наведените домени во системот за заштита на компјутерската мрежа и ИКТ системите на институциите.

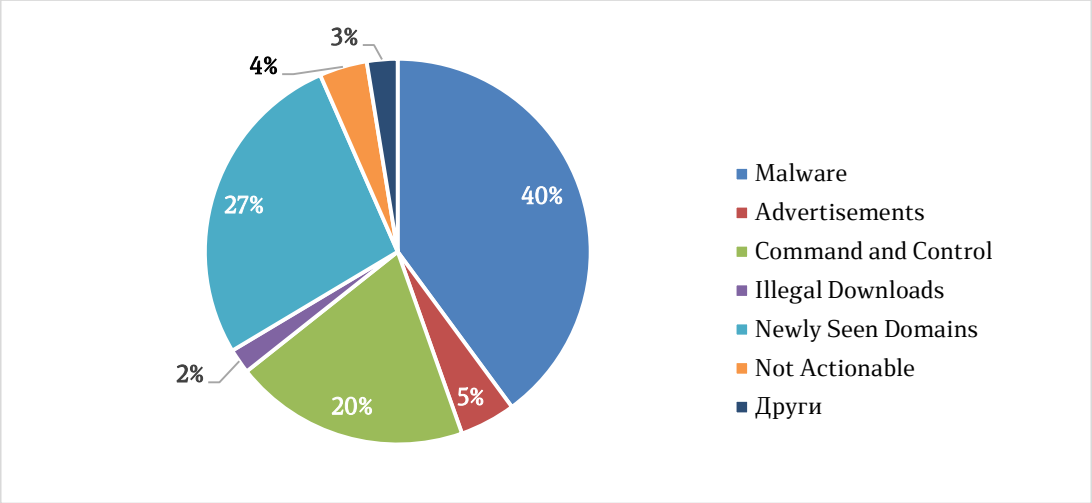
Извршивме анализа на листа со вкупно 854 штетни домени при што учеството на истите се претставени на графиконот број 16 по категории.

Графикон број 16 - Дефинирани видови на штетни домени по категории



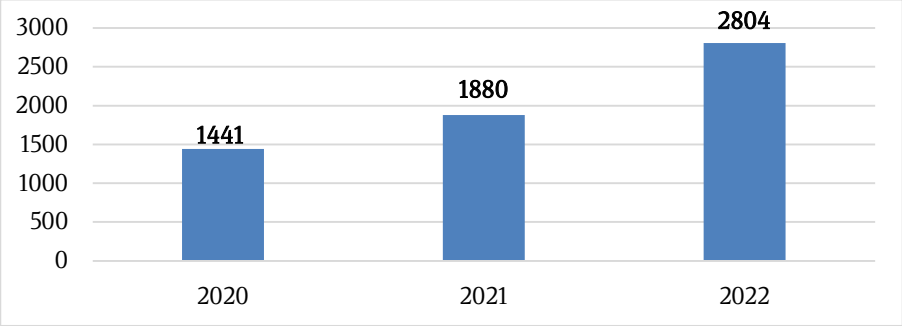
Најзастапениот малициозен домен - малвер со вкупно 426 подтипови е прикажан по подтипови на графиконот број 17.

Графикон број 17 - Подтипови на детектиран малвер во проценти



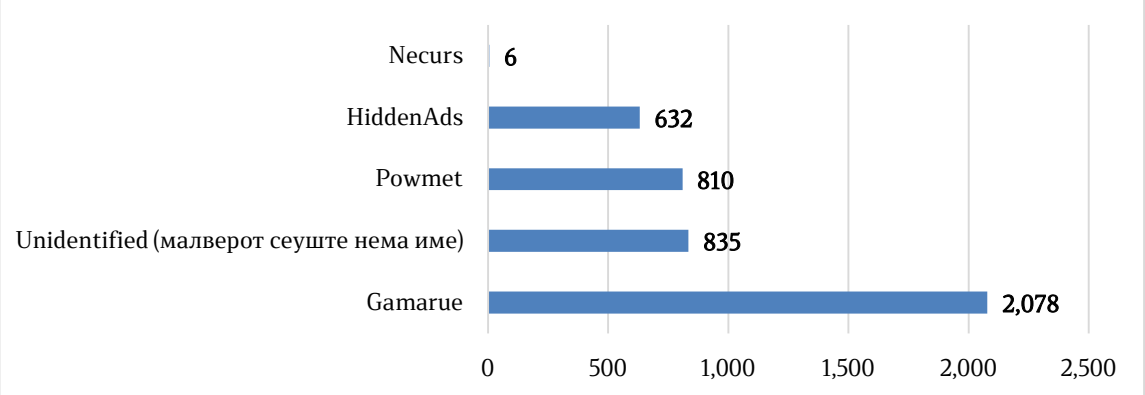
Бројот на инциденти по информацискатa безбедност кои се пријавени во МКД-ЦИРТ за период 2020 -2022 се дадени на следниов графикон број 18.

Графикон број 18 - Број на пријавени инциденти во MKD-CIRT



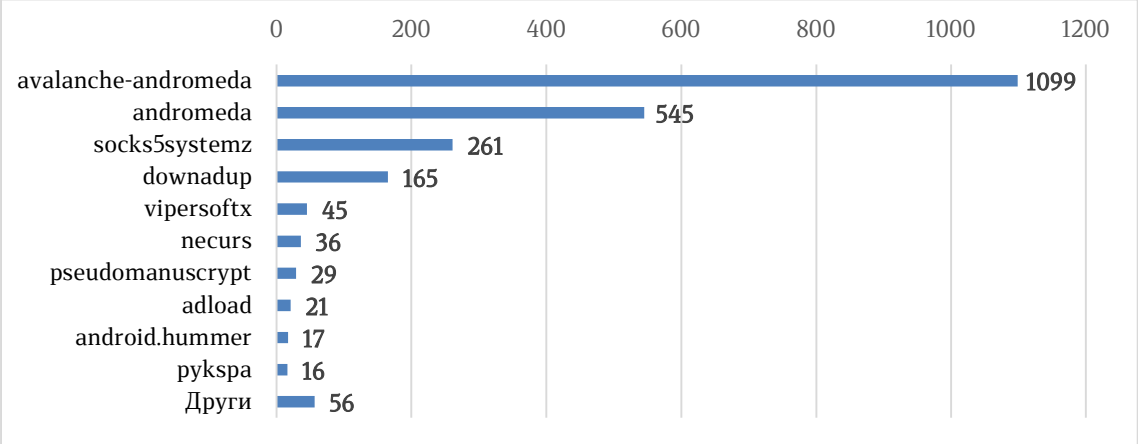
Од информациите презентирани во годишните извештаи на МКД-ЦИРТ, најзастапени типови на малвер во државата се прикажани на графикон број 19.

Графикон број 19 - Број на застапени типови на малвер



Според податоците на Фондацијата за известување за безбедност на интернет и истрага за злонамерни активности Shadowserver[24], во прилог е графикон број 20 на македонски јавни ИП адреси кои во еден или повеќе наврати се извор на штетни активности од типот малвер.

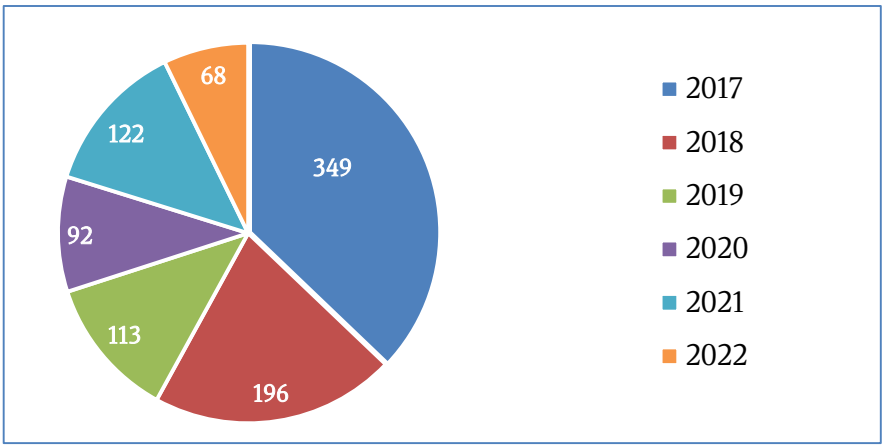
Графикон број 20 - Тип на закани од единствени ИП адреси за територија на државата



МКД-ЦИРТ периодично ги известува операторите кои обезбедуваат услуга за широкопојасен интернет, да ги информираат крајните корисници да го отстранат од нивните уреди од идентификуваниот малициозен софтвер, како и заштита на безбедноста и интегритетот на мрежата на операторите кои обезбедуваат услуга за интернет.

Според анализите[25] на МКД-ЦИРТ дадена е статистика на хакирани јавни веб страни во државата, прикажано на графикон број 21.

Графикон број 21 - Број на хакирани јавни веб-страници



[24] https://dashboard.shadowserver.org/statistics/combined/map/?map_type=top&day=2024-01-28&source=sinkhole&source=sinkhole6&tag=all&geo=all&data_set=count&scale=log

[25] https://mkd-cirt.mk/wp-content/uploads/2022/08/Statistika-2021-Copy.pdf

Поради отсуството на законска обврска за исклучување од интернет мрежата на инфицирани и малициозни уреди кои се приклучени преку интернет операторите, истите не постапуваат по доставените известувања од МКД-ЦИРТ за постоење на инфицирани уреди во нивните мрежи. Кон ова придонесува и склучениот договор на корисниците на малициозните уреди со интернет операторите, со што се овозможува нивната штетна активност.

Во отсуство на правна регулатива во државата за задолжително пријавување на инциденти како и обврска за задолжително постапување по препораките од МКД-ЦИРТ, не е возможно утврдување на точниот број на ИКТ безбедносни инциденти на ниво на држава, процентот на пораст на инцидентите, типовите на инциденти како и штетите предизвикани од нив. Исто така, нема можност за соодветно планирање, анализирање и преземање мерки за превенција односно навремено спречување на ескалација на истите.

3.2.1.2. Мерки и активности за намалување на ризиците од компјутерски безбедносни инциденти

Со доставениот прашалник до институциите, во делот на мерки и активности за намалување на ризиците од компјутерски безбедносни инциденти, ги опфативме следниве области:

Проценка на ризици за ИКТ безбедност

Почетна активност во информацискатa безбедност претставува проценка на опасностите и слабостите која се прави преку анализа на ризици. Постојат институции кои неажурно ги водат утврдените ризици, а постојат и институции кои воопшто немаат регистар за ИКТ безбедносни ризици. Прегледот е даден на графикон број 22.

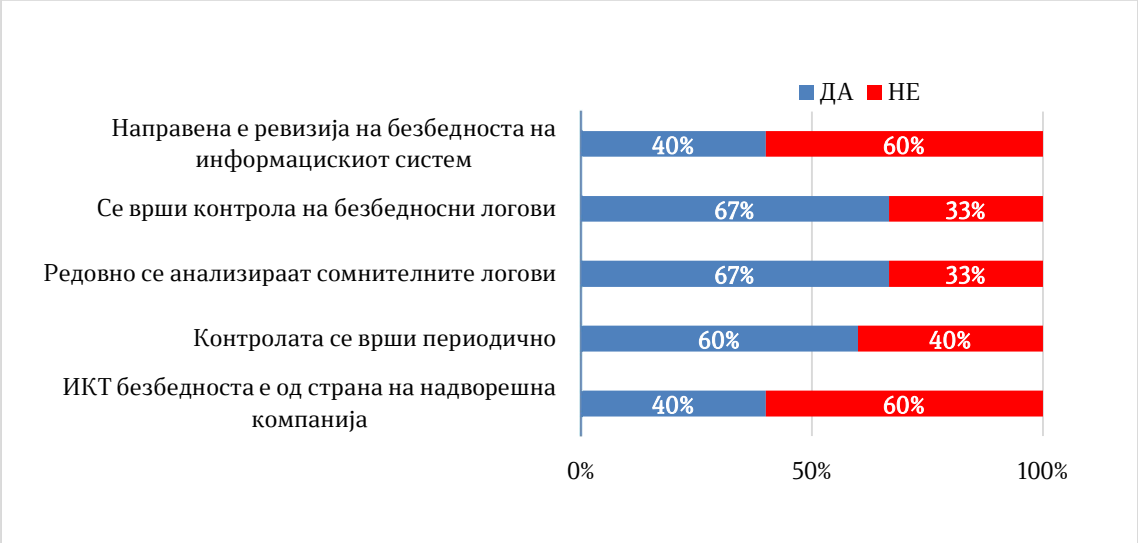
Графикон број 22 - Дефинирани ризици за информациска безбедност

Најголем дел од институциите вршат рангирање на ризиците меѓутоа нивното надминување или намалување (до прифатливо ниво) зависи од нивните годишни буџети за информациска безбедност, при што истиот најчесто е недоволен. Покрај финансиските средства, на ваквата состојба влијае и недостатокот на ИТ човечки ресурси.

Континуирана анализа на состојбата со информациска безбедност

Континуираната анализа на состојбата со информациска безбедност кај дел од институциите отсуствува, односно постојат институции кои воопшто не ги анализираат листите со сомнителни настани во нивните ИКТ системи. Анализата е прикажана на графиконот број 23.

Графикон број 23 - Контроли за состојбата на информацискатa безбедност



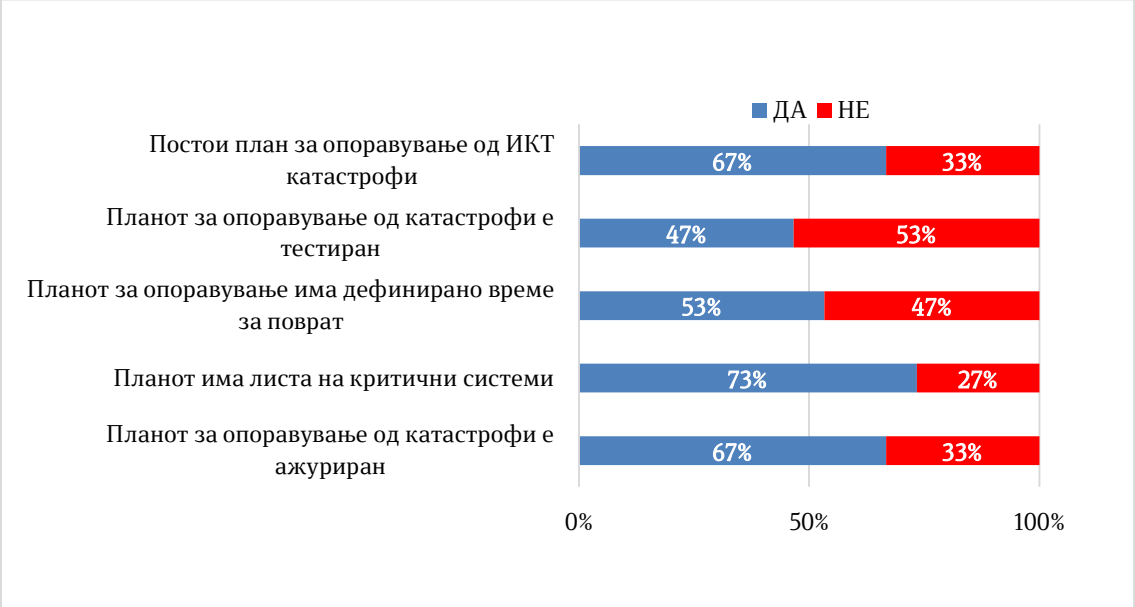
Институциите и покрај тоа што немаат доволно вработени за ИКТ безбедност, немаат ни договори со надворешни компании за преземање на соодветни мерки за ИКТ безбедност. Исто така анализата покажа дека 60% од институциите опфатени со прашалник, немаат направено контрола на безбедноста на нивниот информациски систем.

Од извршената анализа на склучените договори по јавните набавки објавени во ЕСЈН, утврдивме дека има само 10 склучени договори од 6 државни институции за услуги за тестирање на информацискатa безбедноста на нивните ИКТ системи во период од 01.01.2020 до 15.12.2023 година во вкупна вредност од 5.664 илјади денари. Без тестирање на безбедноста на своите ИКТ системи, институциите не се во можност да подготват и имплементираат мерки кои навистина ќе ги отстранат или намалат ризиците во информацискатa безбедност на нивните ИКТ системи што влијае врз степенот на нивната ранливост.

Воспоставување на континуитет по ИКТ катастрофа

Во делот на потребни документи за ефикасна безбедносна заштита, според добиените одговори на институциите, ревизијата утврди дека некои од институциите немаат подготвено план за опоравување од ИКТ катастрофи, додека 53% од институциите кои што имаат подготвено план, истиот воопшто не го тестираа односно не го ажурираа. Ваквата состојба е прикажана на графиконот број 24.

Графикон број 24 - План за опоравување од ИКТ катастрофи

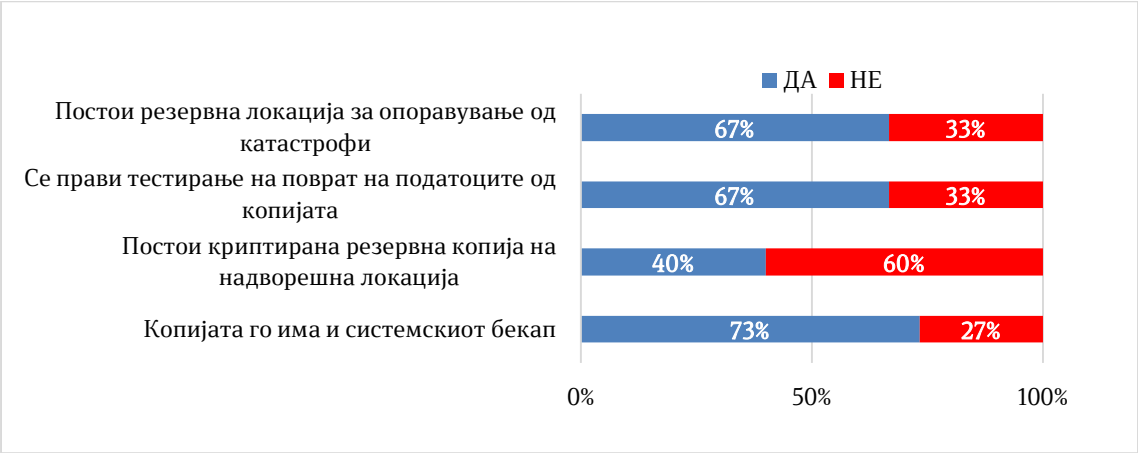


Резервна копија на податоци

Резервната копија на податоци претставува заштита на податоците односно можност за повратот по губење или уништување на оригиналните податоци во ИКТ системите. Бројот на напади со криптирање на податоците во системите е во постојан пораст, при што се бришат сигурносните копии, со кое се оневозможува лесен повратот на функционалноста на ИКТ системите. Поради тоа, од особена важност е ажурна и исправна надворешна резервна копија, која нема да биде директно поврзана со системот, но од друга страна ќе биде доверлив извор за повратот при ИКТ катастрофа.

На графиконот број 25 прикажано е дека 60% од институциите до кои беа доставени прашалници немаат криптирана копија на податоците на надворешна локација.

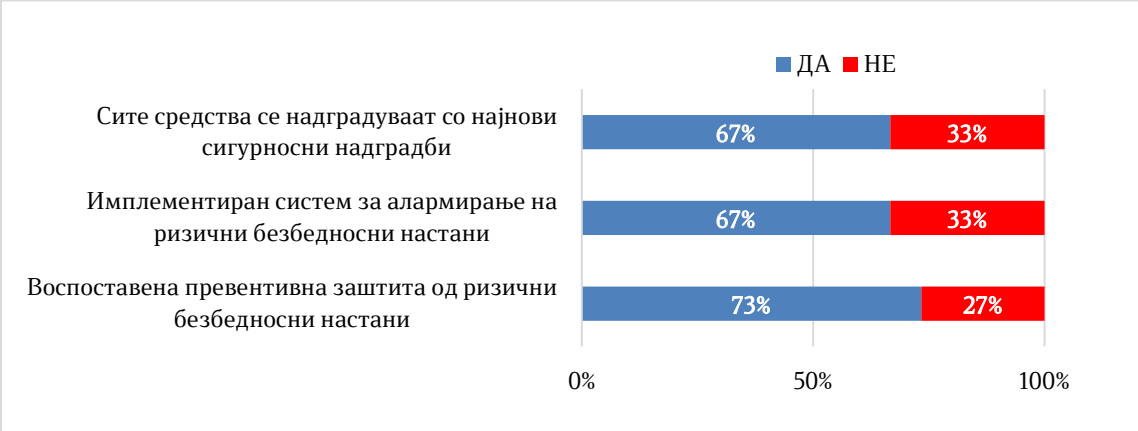
Графикон број 25 - Резервна безбедносна копија на податоците



Мерки за превентивна заштита

Постојат три видови на мерки за безбедносна заштита на ИКТ системите: превентивни, детективни и корективни. Спроведувањето на превентивните мерки може да придонесе до поголеми заштеди од трошоците што треба да се одвојат во случај на спроведување на корективни мерки. Навременото инвестирање во системи за надгледување и контрола на ИКТ системите, како и на мрежниот сообраќај, може да превенира штети од поголеми размери. Кај 33% од институциите нема имплементирано систем за алармирање на ризични безбедносни закани и истото е прикажано на графикон број 26.

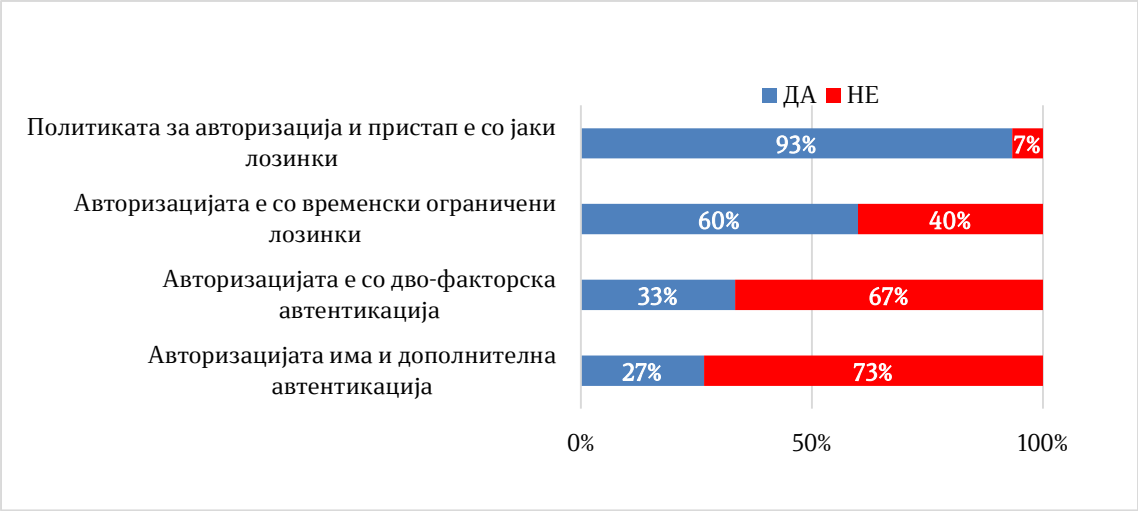
Графикон број 26 - Превентивна заштита и сигурносни надградби



Заштита на пристап до ИКТ ресурсите

Од анализата на одговорите на доставениот прашалник, иако поголемиот број институции имаат политика за пристап со јаки лозинки, утврдивме дека 67% од институциите немаат воведено двофакторска автентикација за корисниците што претставува една од минималните безбедносни мерки на информацискатa безбедност. Воведувањето на двофакторска автентикација при далечинско поврзување на ИКТ системите го минимизира ризикот од неавторизиран упад, прикажано на графикон број 27.

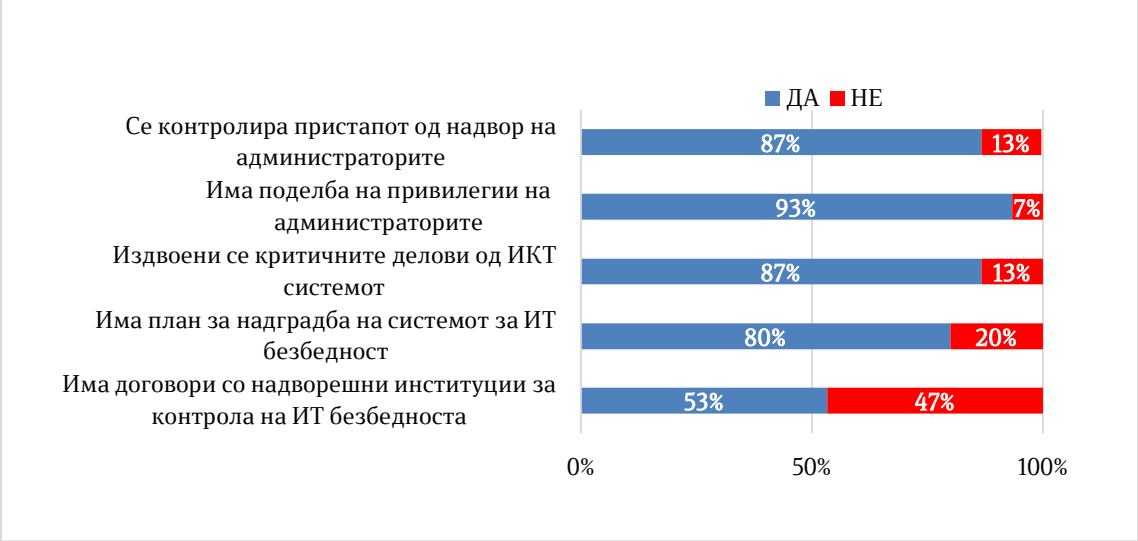
Графикон број 27 - Авторизација за пристап до ИКТ ресурсите



Администраторски привилегии до ИКТ ресурсите

Поделбата на должности на различни нивоа за администраторските корисници и посебната заштита е од исклучителна важност за информацискатa безбедност на ИКТ системот. Отсуството на ваквата заштита може да предизвика поголеми штети од страна на неавторизиран корисник. Еден од најчестите неавторизирани упади во системите, што има тенденција на пораст во последните години, е од страна на администраторски корисник на трети страни со кои институцијата соработува. Поради тоа, ефикасната контрола како и барањето гаранција за сигурност на ИКТ системот на институции кои имаат договори за ниво на услуги (SLA) услуги со други институции е меѓу примарните услови за надминување или ублажување на овој ризик што е претставено на графиконот број 28.

Графикон број 28 - Администраторски пристап до ИКТ ресурсите



Предлог мерки за подобрување на безбедноста на информациските системи

Владата на 131-вата седница[26] одржана на 21.02.2023 година, донесе Информација со предлог-мерки за подобрување на безбедноста на информациските системи во институциите од јавниот сектор, каде се препорачува на институциите да преземат минимални безбедносни мерки наведени во соопштението објавено од МКД-ЦИРТ на 13.09.2022 година: https://aek.mk/soopstenie/.

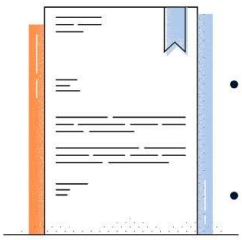
[26] https://vlada.mk/file/79023/download?token=ZvZx5t_w

ПРЕДЛОГ МЕРКИ ЗА ПОДОБРУВАЊЕ НА БЕЗБЕДНОСТА НА ИНФОРМАЦИСКИТЕ СИСТЕМИ ВО ИНСТИТУЦИИТЕ ОД ЈАВНИОТ СЕКТОР

Заклучоци од 131-та седница на Владата на Република Северна Македонија, одржана на 21 февруари 2023 година

Се задолжуваат сите органи на државна управа, а им се укажува на институциите кои не се органи на државна управа;

- да определат лице одговорно за информациска безбедност во нивните организации за навремено пријавување на инциденти и размена на информации за инциденти со MKD-CIRT, во рок од 15 дена.
- да достават до MKD-CIRT, Образец за регистрација на конституенти и Образец - Барање за регистрација на користење на бесплатна услуга за надворешна сајбер безбедносна проверка на веб-апликации, во рок од 30 дена.



- сите вработени да завршат Основна обука за сајбер безбедност за вработени во јавната администрација и вработени во приватниот сектор или за менаџерски и раководен персонал, во рок од 90 дена.
- да воспостават и понатаму за службена комуникација да користат исклучиво службени е-маил адреси на службен домен, во рок од 90 дена.
- да направат план за реализација и да ги предвидат финансиските импликации на мерките на MKD-CIRT, во рок од 90 дена.

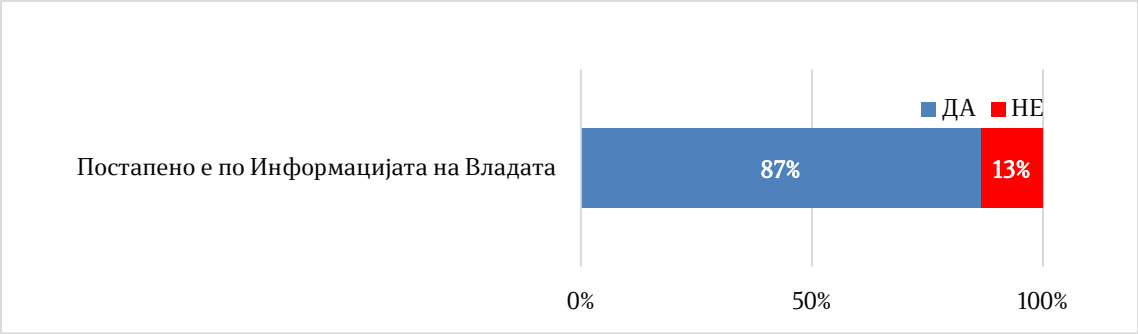
Се препорачува на Националниот центар за одговор на компјутерски инциденти MKD-CIRT при Агенцијата за електронски комуникации,

- да достави до Владата извештај за спроведена бесплатна надворешна сајбер-безбедносна проверка на веб-апликации на пријавените институции, во рок од 60 дена.

Поради зачестените сајбер-напади во државата и регионот, се препорачува организациите од јавниот, владиниот и приватниот сектор да извршат безбедносна процена на своите ИКТ системи и услуги и да имплементираат и применуваат превентивни мерки и процедури за заштита од сајбер напади и инциденти. Како високо-приоритетни активности се препорачува навремено ажурирање на системски и апликациски софтвер и хардвер, проверка на пристапот, промена на лозинки, воведување на најава со повеќе фактори, ажуриран и активен антивирусен софтвер на сите уреди, запишување на секоја активност во дневници, тестирање на бекап и валидација за исправен бекап, план за одговор на инциденти, спроведување на надворешно безбедносно скенирање, едукација на вработените, безбедност на соработници и трети лица/страни, пријава на инциденти и сомнителни активности, идентификувано лице за пријавување на сомнителни активности.

Со анализа на добиените одговори од прашалникот, во делот на преземени мерки за подобрување на безбедноста на информациските системи, кои произлегуваат од заклучок на Влада на 131-ва седница, утврдивме дека 13% од институциите не презеле мерки за подобрување на информацискатa безбедност согласно дадените предлог мерки, а кое е прикажано на графикон број 29.

Графикон број 29 - Предлог мерки за подобрување на безбедноста на информациските системи



Предлог мерките од страна на АЕК (МКД-ЦИРТ) до Владата доставени се во септември 2022 година, но истите се усвоени со заклучок на седница 5 месеци подоцна. Непосредно пред усвојувањето на мерките за подобрување на безбедноста на информациските системи, настанат е сериозен безбедносен инцидент на ИКТ системот на ФЗОРСМ[27] за што е известено во извршената ревизија согласно годишната програма за 2023 година за работа на Државниот завод за ревизија.

На 174-тата седница на Владата од 25.07.2023 година, разгледана е информацијата за постапувањата на институциите по Предлог мерките за подобрување на безбедноста на информациските системи од 131-вата седница, при што известувања за мерките се добиени од 33 институции. Исто така не е утврден начинот на следење на реализацијата на активностите утврдени во заклучокот на Владата од 131-вата седница, како и начинот на контрола на степенот на нивната имплементација.

Институциите кои ќе ги применат овие мерки во значителна мерка ќе ги намалат ризиците од неавторизиран упад во нивните ИКТ системи и ќе ја зголемат заштитата на нивниот ИКТ систем.

Состојбите со проценката на ризици, воспоставување на континуитет по ИКТ катастрофи, правење резервна безбедносна копија на податоците, спроведување на мерки за превентивна заштита, заштита на пристапот до системите како и управувањето со администраторските привилегии влијае врз градење на отпорноста кај јавните институции кои се почесто се цел на сајбер напади заради оневозможување на системите кои даваат услуги кон граѓаните, изнуди, кражби на податоци и има директни, видливи и сериозни последици врз нивниот живот.

[27] Извештај за извршена ревизија на финансиски извештаи и ревизија на усогласеност за 2022 година на ФЗОРСМ

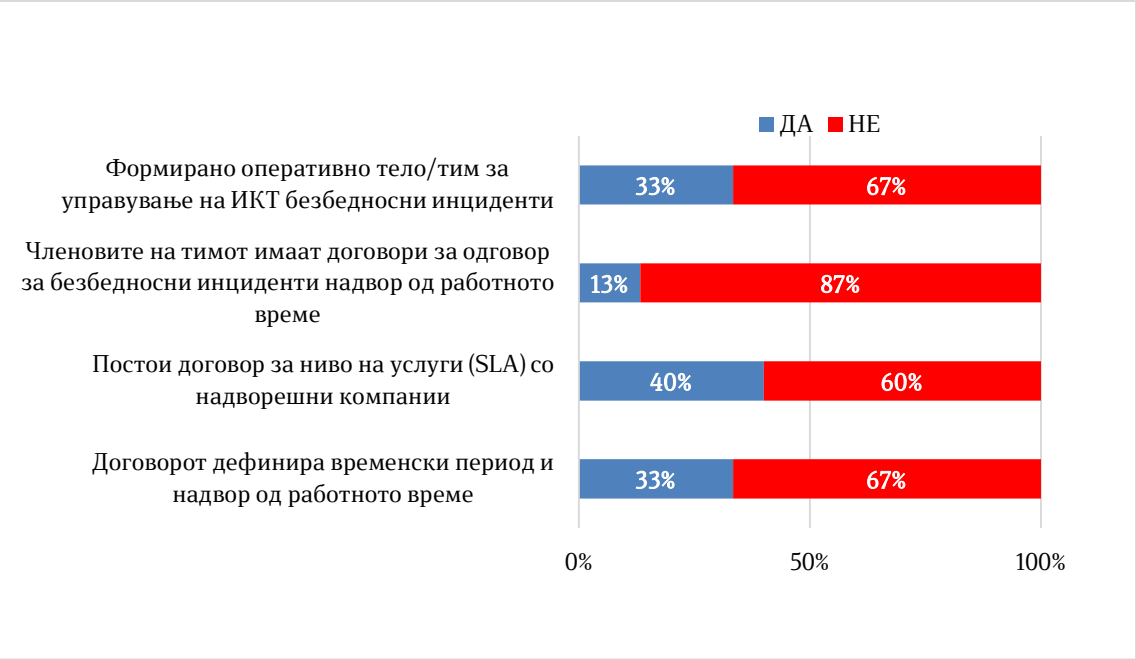
3.2.1.3.Оперативни тимови за справување на компјутерски безбедносни инциденти

Безбедносните закани на ИКТ системите се реалност при што секој вмрежен систем може потенцијално да биде компромитиран и за многу кратко време може да предизвика застој, кражба на податоци, репликација на вируси, црви и тројанци преку интернет. Игнорирањето на информацискатa безбедност може да ја чини институцијата време, напор, продуктивност или може да има значајно финансиско влијание како и загуба на угледот.
Една од основните форми на дејствување со цел превенирање, но и справување со ваков тип на проблеми е воспоставувањето на CSIRT, кои се одговорни за примање, разгледување на извештаи за инциденти, како и одговор на истите и извршување на реактивни, проактивни и безбедносни услуги за управување со квалитет.
Дури и институции со високо развиени инфраструктури за информациска безбедност не можат да гарантираат дека нема да се случат упади или други злонамерни активности во нивните системи. При компјутерски безбедносен инцидент од клучно значење за една институција е да има ефективен начин да одговори на истиот заради ограничување на штетата и намалување на трошоците за оправување. Со идентификување на компромитираноста на системите може брзо да се координира оправувањето како и да се предложат стратегии за ублажување и одговор.
Соработката со други CSIRT тимови и организации за безбедност може да придонесе да се споделуваат стратегии за одговор, рани сигнали за потенцијални проблеми, идентификување на ранливи области на организацијата, проценка на ранливоста и откривање на инцидентот како и да обезбедат стручност за превенција и да помогнат во намалувањето на идните закани. Исто така може да го фокусираат вниманието на безбедноста и да обезбедат обука на вработените во институцијата со цел да се зголеми свесноста за безбедноста. Создавањето на CSIRT во една институција како и бројот на вработени во него, зависи од бројот на ресурси и услуги кои треба да се обезбедат.

Во академскиот сектор воспоставен е CSIRT–ФИНКИ, основан во 2017 како организациска единица на Факултетот за информатички науки и компјутерско инженерство со цел да се обезбеди детектирањето, решавањето и превенцијата во врска со безбедноста на информациите и мрежата при факултетот.
Формирањето на тимовите е предвидено како активност во Националната стратегија за сајбер безбедност 2018-2022. Во акцискиот план на стратегијата со висок приоритет утврдена е активност за развој на дополнителни CSIRT/CERT/CIRT тимови на повеќе нивоа (секторски, институционални, академски итн.) од страна на сите организации и институции што имаат потреба и капацитет за развој на тимовите со почеток во 2019 година.

Состојбата со формираните тимови за одговор на компјутерски инциденти, кои извршуваат работни задачи поврзани со безбедноста на ИКТ системите, покажува дека 67% од институциите немаат формирано тимови за одговор на компјутерски инциденти додека кај 60% не се склучени договори со надворешни компании за пренесување на ризикот од безбедносен инцидент. Во однос на вработените ИТ лица во институциите, 87% воопшто немаат договори за нивно ангажирање во случај на потреба надвор од работното време, прикажани на графиконот број 30.

Графикон број 30 - Тимови за одговор на ИКТ безбедносни инциденти



Бидејќи успешноста кај справувањето со безбедносните инциденти, најчесто е со правилен и брз одговор, не ангажирањето на експерти за информациска безбедност по работно време, носи висок ризик по успешноста на мерките во насока на нанесување на што помала штета при инцидентот.

Иако се поминати 5 години од кога е предвидено формирање на тимови за одговор на компјутерски безбедносни инциденти во стратегијата за сајбер безбедност, најголемиот број на институции се уште немаат формирано вакви тимови, ниту имаат склучен договор за користење на услуги од трети страни, со цел да се намалат или минимизираат евентуалните штети при ИТ безбедносни инциденти.

Целата состојба носи исклучително висок ризик од успешен одговор при соодветен сајбер напад или ИКТ безбедносен инцидент. Истовремено справувањето со ризикот не е регулирано со договори со надворешни компании, а дури ни времето за кое би се ангажирале во случај на потреба, не дефинира период надвор од работното време заради брз одговор на инциденти доколку тие се случат.

4. ЗАКЛУЧОК

Веруваме дека спроведената ревизија ни даде основа да го изразиме следниот заклучок:

Преземените мерки од надлежните органи не обезбедуваат ефикасна и целосна заштита на критичните информациски системи. Имено, отсуството на законска регулатива од областа на безбедноста на информациските системи може да предизвика долгорочни последици по безбедноста на ИКТ системите во институциите. Исто така не е извршено усогласување на националното законодавство со европските директиви НИС од 2016 година и надградената НИС2 регулатива од 2023 година која претставува дефиниција на ЕУ за воспоставување на минимални мерки за сајбер безбедност во критичната ИКТ инфраструктура на земјите членки. Како земја на пристапниот пат кон ЕУ, оваа состојба е од исклучително значење за усогласување на домашното законодавство со ЕУ регулативата.

Подготвениот предлог закон за оваа област кој е подготвен во 2019 година не е донесен, а во 2023 година подготвен е нов кој се наоѓа во собраниска процедура.

Последната Национална ИКТ стратегија е со важност до 2017 година додека последната Националната стратегија за сајбер безбедност е со важност до 2022 година. И покрај тоа што се подготвени, Националната ИКТ стратегија и Националната стратегија за сајбер безбедност се уште се наоѓа во фаза на меѓуинституционално усогласување. Поради отсуството на стратешки документи како сет на активности и мерки, не се обезбедува безбедна, еластична и доверлива дигитална средина која ќе влијае државата да биде безбедно место за он-лине делување и работа со напредни човечки и технички капацитети.

Национален совет за сајбер безбедност е формиран во 2019 година заради координација и следење на спроведените активности согласно Националната стратегија за сајбер безбедност на Република Македонија 2018-2022. Од неговото формирање до периодот на известување од ревизијата одржал еден состанок, при што на ревизијата не и беа презентирани годишни извештаи за работата доставени до Владата, предложени мерки за подобрување на имплементацијата на Стратегијата и Акцискиот план, мерки за поголема ефикасност за управување со сајбер кризи како и стратешки насоки и препораки поврзани со сегментот на сајбер безбедност. Со тоа доведена е во прашање ефективноста, ефикасноста и релевантноста во справувањето со современите и идните предизвици за сајбер безбедноста, улогата и способноста да функционира за време на сајбер-криза.

Минимални безбедносни мерки и стандарди за заштита на информациските системи, регулатива за дефинирани критериуми и креирање на регистер со оператори на критична инфраструктура (ВИС и КИИ) не се пропишани. Истите не се усогласени со ЕУ директивите и претставуваат ризик од недоволни инвестиции, нивно маргинализирање како и одложување на мерки за подобра заштита на информациските системи. Од исклучителна важност е институциите

финансирањето во информациската безбедност да го гледаат како инвестиција, а не како трошок при што добивката е далеку поголема во инвестирање на превентивни мерки од штета во однос на трошокот направен по безбедносен инцидент.

Со воспоставениот начин на пријава и одговор при компјутерски безбедносен инцидент институциите не може да осигураат навремен и соодветен одговор на инцидентот. Исто така оневозможено е навремено исклучување од интернет мрежата на инфицираните и малициозни уреди кои се приклучени преку интернет операторите, со што се продолжува нивната штетна активност.

Кај голем број на институции не се формирани тимови за одговор на компјутерски безбедносни инциденти, недоволен е бројот на вработени за информациска безбедност и отсуствува постојана стручна обука што доведува до висок ризик од успешен одговор при соодветен сајбер напад или ИКТ безбедносен инцидент. Истовремено за намалување на штети не се склучуваат договори со трети страни и не е дефинирана обврска за ангажирање на вработените надвор од работното време во случај на инцидент.

Нагласуваме дека е неопходно да се прави анализа на ризици, да се креираат предлог мерки според приоритет на ризиците за нивно намалување, ублажување, пренесување или минимизирање на прифатливо ниво, со точна временска рамка за спроведување на истите.

Неопходно е спроведување на континуирана анализа, согледување на реалната состојба и дефинирање мерки и препораки за подигнување на нивото, извршување на редовни ревизии за детектирање на грешки и ранливости на безбедноста, развој и периодично тестирање на планови на информациската безбедност во институциите.

Улогата на државата во поглед на заштита на критичната инфраструктура од областа на ИКТ безбедноста е клучна, но исто така важна е и улогата на операторите, односно институциите што стопанисуваат со овие критични инфраструктури. Оттука, заштитата треба да обезбеди да не настане компромитирање на приватноста и угледот, финансиска загуба на поединци и компании, како и загрозување на личната и семејната безбедност.

5. ПРЕПОРАКИ

Од ревизијата произлегоа препораки за надлежните институции во насока на надминување и подобрување на утврдените состојби.

Владата во соработка со МИОА и АЕК да преземе активности за:

1. Усогласување на националното законодавство со директивата на ЕУ за ниво на безбедност на мрежни и информациски системи (Директива НИС2).
2. Донесување на законска регулатива од областа на безбедност на мрежни и информациски системи.
3. Донесување на Национална ИКТ Стратегија со прецизно дефиниран акциски план со рокови, носители на активности и потребни средства.
4. Донесување на Национална стратегија за сајбер безбедност со прецизно дефиниран акциски план со рокови, носители на активности и потребни средства.
5. Преиспитување на оправданоста, ефективноста, ефикасноста и релевантноста на Националниот совет за сајбер безбедност во справување со предизвиците за сајбер безбедност, улогата и способноста да функционира за време на сајбер-криза.
6. Дефинирање на критериуми и воспоставување на регистар на ИКТ системи на оператори на критична инфраструктура.
7. Дефинирање на рамка на минимални задолжителни стандарди за информациска безбедност.
8. Да се дефинира начинот на следење на имплементација на мерки за подобрувања на информацискатa безбедност во ИКТ системите.
9. Пропишување на обврска за задолжително пријавување на инциденти по информациска безбедност.
10. Зајакнување и пополнување на човечките, финансиските и институционалните капацитети во институциите од јавниот сектор за информациска безбедност.
11. Континуирано професионално надградување на лицата вклучени во информацискатa безбедност на ИКТ системите.
12. Континуирано подигнување на јавната свест од областа на информацискатa безбедност.
13. Формирање на тимови за одговор на инциденти на критични информациски системи вклучително и за период надвор од работното време, пренесување на ризикот на трети страни или групирање на сродни институции.
14. Зајакнување на човечките капацитети во МКД-ЦИРТ во делот на информациска безбедност.
15. Пропишување на регулатива за оневозможување пристап од интернет мрежата на инфицираните и малициозни уреди кои се приклучени преку интернет операторите.