КОНЦЕПЦИИ ЗА КИБЕРСИГУРНОСТ

CONCEPTS OF CYBERSECURITY

Yordan Shterev Ivanov
NMU "Vasil Levski", Veliko Tarnovo,
E-mail: jshterev@abv.bg

Abstract
This article summarizes, presents and develops technological concepts of cybersecurity according to the current state of the problem. Based on the OSI model, the main protocols used for it and hardware devices on the one hand, and the main vulnerabilities and threats on the other, the current protections against cyberattacks have been revealed.

Keywords: *concepts of cybersecurity, OSI model, threats, vulnerabilities, cyberattacks*.

1. ВЪВЕДЕНИЕ

Съвременните системи за управление се основават на събиране, съхранение и обработка на дигитална инфомация, а получените резултати подлежат на анализ. Това предполага пълнота, достоверност, ценност, адекватност, актуалност и ясност на информацията. Ето защо защитата на информацията излиза на преден план. Развитието на информационните технологии в хардуерен и софтуерен аспект от една страна и на комуникационните технологии доведоха до възможност за натрупване на големи количества данни и информация и тяхното бързо разпространение. Докато обществото ни се развива технологично експоненциално, в морален аспект е спорно да се укаже дори слабо линейно развите [3,11,12]. Настоящето развитие на информационните и комуникационните технологии заедно с натрупване на големи обеми от данни и шрокото им използване води до необходимостта от информационна сигурност (киберсигурност - КС). Тя се разглежда в контекста на ненарушимостта на притежаваните ресурси от една страна и от друга от потенциална реална възможност за тяхното нарушение. Ето защо с времето се появи необходимостта от защита на хардуера и софтуера в държавни и частни организации, на национално и на наднационално ниво. Важна област е също така и защитата на личните данни независимо от притежателя и мястото на тяхното съхранение.

Актуалността на КС като приоритет в дейностите на системите за управление се обуславя от: динамичността на съвременната дигитална среда; трансграничното киберпространство (КП) и способности на чужди държави и недържавни структури да реализират комплекс от деструктивни кибервъздействия. Има тенденция към използването на все по-сложни и интелигентни хакерски атаки. Ето защо възникна направлението „*Киберсигурност*".

В настоящия доклад е представена концепция на КС от гледна точка на заплахите и уязвимостите от една страна и от друга от въздействието им върху OSI (Open System Inetrconnection) модела.

2. ОСНОВНИ ТЕРМИНИ В КИБЕРСИГУРНОСТТА

„Киберсигурността" се дефинира от Оксфордския английски речник като „Състояние

на защитени срещу престъпно или неразрешено използване на електронни данни и мерките, предприети за постигане това". Това тълкуване обхваща само неразрешената и престъпна злоупотреба с информация. Но остава въпросаѝ за оперативните грешки, за защитата срещу човешка грешка в КП.

Също така възниква въпросът за манипулиране на физически активи. Дефиницията е с широк обхват и включва защита срещу разнообразие от рискове за организациите и данните [2]. От военна гледна точка към термина „киберсигурност“ се подхожда от още по-широка и много по-стратегическа гледна точка във връзка с термините „киберотбрана“ и „кибервойна“.

Защитата (сигурността) на една информационна и комуникационна система (ИКС) е намиране на баланс. Системите имат своите ограничения. Намирането на баланс между безопасност и използваемост определя използваемостта на системата. Балансът на ИКС в една организация се определя от целите на организацията, смисълът на защитата ѝ, измерване на заплахите на защитата. Системите насочени към потребителя имат висока степен на използваемост и ниска степен на безопасност. Докато вътрешните системи имат ниска степен на използваемост и висока степен на безопасност. КС е състояние определено и измерено чрез нивото на *конфиденциалност, интегритет* и *достъпност* на информационните ресурси, системи и услуги. Основава се на ефективно изграждане и поддръжка на активни и превантивни мерки като елемент на информационните и комуникационни технологии (ИКТ) [1, 6, 9, 13].

Конфиденциалността се отнася до защитата и поверителността на информацията. Тя е физическа и логичеста конфиденциалност. Логическата конфиденциалност включва съхраняване и предаване на данни, а физическата се отнася до хардуера.

Целостта осигурява точността на информацията. Това означава, че потребителите имат доверие в точността на информацията, тоест тя не е модифицирана при съхраняването и предаването ѝ. Целостта на информацията се защитава в две направления: съхраняване и предаване.

Достъпността означава, че когато легитимен потребител има нужда от информацията, тя е достъпна. Използват се архиви, масиви от дискове, отдалечено разположени носители на информация, за да се осигури достъпността.

Основни термини в КС са: рискове, активи, заплахи и уязвимости [6];

- *Рискът* е вероятност от възникване или реализация на заплаха. Основните рискови елементи са активи, заплахи и уязвимости.
- *Активите* са реални устройства (сървъри, мрежови устройства, устройства за съхранение и др.) и виртуални (бази от данни, таблици и др.). Имат икономическа стойност. Една ИКС не може да бъде 100% защитена. Винаги има остатъчен риск, след като са поставени предпазни мерки за защита на активите.
- *Заплахите* създават риск за активите. Те засягат конфиденциалността, целостта и достъпността на активите. Заплахите се причиняват от природни бедствия, катастрофи, атаки от хакери [3, 6] – външни и вътрешни, вируси и злонамерен софтуер, разкриване на конфиденциална информация, атаки за отказ от обслужване. Кибератаките (КА) са насочени към критично важни инфраструктури. Ако ИКС е уязвима за някои от тия заплахи, съществува увеличен риск от успешна атака.
- *Уязвимостта* е слабост от дизайна на системата до реализацията на процедура. Уязвимости може да има в приложенията, в операционните системи (ОС), сървърния

софтуер или техни компоненти, неправилна конфигурация на работата на софтуера и хардуера.

КС не е само защитата на КП, но също така защита на тези, които функционират в него и всички активи. КС се състои от непрекъснат цикъл на структурирани действия за:

- Идентифициране (разбира състоянието и рисковете за системи, активи, данни и възможности);
- Защита (прилагане на подходящите предпазни мерки);
- Откриване (внедряване на инструменти за идентифициране на КА за нарушаване на КС);
- Отговор (внедряване на инструменти за предприемане на действия срещу кибер-атаки);
- Възстановяване (възстановяване на нарушени активи и повишаване на КС).

Областите на приложимост на КС са :

1. *Комуникационна сигурност*: Защита срещу заплаха за техническата инфраструктура на кибер система, което може да доведе до нейната промяна на характеристиките ѝ, за да се извършват дейности, които не са били предназначени от неговите собственици, дизайнери или потребители.

2. *Оперативна сигурност*: Защита срещу умишлено повреждане на процедури или работни потоци.

3. *Информационна сигурност*: Защита срещу заплаха от кражба, изтриване или промяна на съхранявани или предавани данни в рамките на кибер система.

4. *Физическа сигурност*: Защита срещу физически заплахи, които могат да повлияят или засегнат състоянието на една кибер система. Например физически достъп до сървъри, вмъкване на зловреден хардуер в мрежа или принуда на потребителите или техните семейства.

5. *Обществена/национална сигурност*: Защита срещу заплаха, чийто произход е в КП, но може да застраши физически или кибер активи по начин, който ще има политическа, военна или стратегическа печалба за нападателят. Такива са „*Stuxnet*“ или широкомащабна атаки за отказ от услуги (DOS – denial of service), комуникационна финансова система или други критични обществени или промишлени инфраструктури.

ЗАПЛАХИ И УЯЗВИМОСТИ В КИБЕРСИГУРНОСТТА

Агенцията на Европейския съюз за КС (European Union Agency for Cybersecurity — ENISA) идентифицира основните заплахи [7, 14] от април 2020 г. до юли 2021 г. [4], но не са включени заплахите причинени от природни бедствия. През указания период основните киберзаплахи съгласно [4] са:

1. *Зловреден софтуер*: Софтуер специално предназначен да наруши, повреди или да получи оторизиран достъп до компютърни системи.

2. *Уеб базирани атаки*: Те използват активирани уеб системи, уебсайтове, ИТ-компоненти на уеб услуги, браузъри и уеб приложения. Включват експлойти на уеб браузър, уеб злоупотреби със сървъри и уеб услуги, атаки чрез drive-by attacks (drive-by downloads - злонамерен скрипт изтегля и инсталира програма на потребителско устройство без изрично разрешение), waterholing attacks (нападателят предполага или наблюдава уебсайтове често използвани от една организация и заразява някои от тях със

злонамерен софтуер; може да се атакуват само потребители, идващи от конкретен IP адрес), пренасочване на URL и man-in-the-browser-attacks (нападателят се вмъква в комуникационния канал между две доверени страни, компрометира уеб браузъра, използван от една от страните за целта на подслушване, кражба на данни и/или подправяне на сесия).

3. *Атаки на уеб приложения*: Атаките на уеб приложения са насочени срещу налични уеб приложения, уеб услуги и мобилни приложения. Те злоупотребят с API (Application Programming Interface), които са включени в мрежата приложения.

4. *Фишинг*: Фишингът е широко разпространен, защото основно използва социално инженерство за атака на крайни потребители. Той е важен инфекциозен вектор за всички видове заплахи. Широко е използван като първа стъпка в КА-ите. Най-успешният вектор е на инфекция за нарушения на данните и инциденти със сигурността както при целенасочена, така и при опортюнистична атака. Хора, които никога не са планирали да атакуват организация, могат да се превърнат в сериозна заплаха за КС. Необходимо е блокиране достъпа на уволнен служител до ИКС, да не се предоставя на изпълнител прекомерен достъп до ИТ инфраструктура. От решаващо значение е да не се дава възможност на вътрешни лица да се превърнат в злонамерени.

5. *Спам*: Спамът е един от най-разпространените и устойчиви киберзаплахи (КЗ).

6. *Атаката с отказ на услуга*: DOS атака е КА в което деецът се стреми да направи системен ресурс недостъпен за предвидените му потребители чрез временно или неограничено прекъсване на услугите на хост, свързан към Интернет.

7. *Ransomware*: Той е форма на злонамерен софтуер, който след като се установи в компютъра на потребителя, заплашва с вреда, обикновено чрез отказ на достъп до данни. Нападателят иска откуп от жертвата.

8. *Ботнет*: Вид зловреден софтуер е. Работи на съвкупност от устройства свързани с интернет като включват компютри, сървъри, мобилни и др. устройства, които са заразени и контролирани от него. Потребителите обикновено не знаят за ботнет заразяване на тяхната система. Чрез него може да се инициира distributed (разпределена) DDoS атака, да се крадат данни, да се разпраща спам, да се получи достъп до устройството и неговата свързаност.

9. *Вътрешна заплаха:* Тя се отнася до заплахата от вътрешен човек. Използва се неговия разрешен достъп, съзнателно или неволно може навреди на сигурността на организацията.

10. *Физическа манипулация/повреда/кражба/загуба*: Въпреки, че не винаги е техническа, КЗ може да е физическа манипулация, повреда, кражба, загуба има сериозно въздействие върху всички видове цифрови активи, ресурси.

11. *Нарушения на данните*: Пробив на данни е потвърден инцидент, при който върху чувствителни, конфиденциални или други защитени данни е извършен достъп и/или разкрити по неоторзиран начин.

12. *Кражба на самоличност*: КЗ, към която се стреми нападателят за получаване на поверителна информация, която се използва за идентифициране на човек или дори компютърна система. Такава поверителна информацията може да бъде: адреси, контактни данни, идентификационни имена и данни, финансови данни, здравни данни, регистрационни файлове и др. Впоследствие с тази информация се злоупотребява, за да се

представи нарушителят за собственик на откраднатите данни.
13. *Изтичане на информация*: Слабост на приложението, поради което то разкрива чувствителни данни: като негови технически подробности, средата или специфични за потребителя данни. Те могат да бъдат използвани от нападателят, за да експлоатира уеб приложението, неговата мрежа или потребители.
14. *Експлойт - комплекти (инструменти)*: Те включват съвкупност от готови инструменти обикновено се установяват в компрометирани уебсайтове или се използва в злонамерени рекламни кампании. Експлойт инструментите имат способността да идентифицират уязвимости, които могат да се използват в браузъра на потребителя или уеб приложения и автоматично да ги експлоатират.
15. *Кибер шпионаж*: Той е кражба на секретни съхранявани в цифров формат данни или на компютри и ИТ мрежи.
16. *Cryptojacking*: Зловреден софтуер за криптовалути, който заразява компютрите или мобилните устройства и използва ресурсите им, за получаване на криптовалути без знанието на потребителите. Това е нарастваща заплаха, която може да компрометира всички видове устройства: настолни компютри, лаптопи, смартфони и дори мрежови сървъри.

Основните тенденции на КЗ, които се наблюдават са [4]:
- Пандемията COVID-19 създаде възможности за киберпрестъпниците и за кибер шпионаж. Тя е все още доминираща примамка в кампаниите за емейл атаки;
- Правителствените организации увеличиха дейността върху национално и на международно ниво;
- Наблюдават се активни действия от страна на правителствата за предприемане на правни действия срещу КЗ с различен произход;
- Киберпрестъпниците все повече се мотивират от финасовото обвързване на дейността им, например ransomware;
- Криптовалутата остава най-често срещаният метод за изплащане от страна на жертвите;
- Кибератаките все повече са насочени и засягат критична инфраструктура;
- Остава използването на фишинг имейли и грубата сила чрез Remote Desktop Protocol (RDP) като най-често изплозвани вектори за заразяване с ransomware;
- Увеличаване на Ransomware като услуга през 2021 г., което прави трудно идентифициране на отделните заплахи;
- Намаляването на зловредния софтуер наблюдавано през 2020 г. продължава и през 2021 г. През 2021 г. се наблюдава увеличение на заплахите, които използват нови или необичайни езици за програмиране, за да пренесат своя разрушителен код;
- Контейнерни със злонамерен софтуер станаха много по-разпространени, като зловреден софтуер без файлове се изпълнява от паметта;
- Обемът на инфекциите с *cryptojacking* достигна високи нива през 2021 г., в сравнение с последните няколко години. Финансовата печалба свързана с *cryptojacking*

стимулира участниците в заплахата да извършват тези атаки;
- Извършва се преминаване от браузър към базиран на файлове *cryptojacking;*
- Бизнес моделът Phishing-as-a-Service (PhaaS) се разпространява все повече.
- Участниците в КА насочиха внимание си към информацията за ваксините;
- Наблюдава се ръст в нарушенията на данните, свързани със сектора на здравеопазването;
- Традиционните DDoS атаки се насочват към мобилни мрежи и IoT (Интернет на нещата);
- Ransom Denial of Service (RDoS) е нов етап на атаките за отказ на услуги;
- Споделянето на ресурси във виртуализирани среди действа като усилвател на DDoS атаките;
- DDoS кампаниите през 2021 г. станаха по-целенасочени, по-постоянни и все по-често многовекторни;
- Дезинформацията с активиран изкуствен интелект (AI) подпомага нападателите при извършването на техните атаки;
- Фишингът е в основата на атаките с дезинформация и силно експлоатира наивните хора;
- Дезинформацията като услуга (DaaS) нарасна значително, стимулирана от нарастващото въздействие на пандемията COVID-19 и необходимостта от повече информация;
- Налице е скок в инцидентите, свързани със сигурността в облачни структури.

Някои от значимите инциденти в ЕС и извън него с последващо въздействие върху потребителите, организациите, информационните и комуникационни структури са [4]:
- ransomware - 10 значими ransomware инцидента в периода април 2020 г. - юли 2021 г.;
- със злонамерен софтуер – 5 инцидента през юли 2020 г. - март 2021 г.;
- cryptojacking - 4 инцидента през август 2020 г. - април 2021 г.;
инциденти свързани със заплахи, насочени към електронните пощи - 9 инцидента през март 2020 г. - май 2021 г.;
- инциденти свързани със заплахи срещу данни - 9 инцидента през март 2020 г. - май 2021 г.;
- инциденти с отказ от услуга - 24 инцидента през януари 2020 г. - май 2021 г.;
- Web атаки - 11 инцидента през януари 2020 г. - май 2021 г.;
- инциденти свързани с дезинформация и липсваща информация – 10 инцидента през периода април 2020 г. – юли 2021 г.;
- инциденти свързани с пандемията – 9 инцидента 2020 г. – 2021 г.;
- инциденти свързани с грешки и неправилни конфигурации, свързани с управлението на ИКС – 9 инцидента през периода април 2020 г. – юни 2021 г.;
- инциденти свързани с грешки и неправилни конфигурации на ниво приложение – 8 инцидента в ЕС и извън него през периода юни 2020 г. – юни 2021 г.;
- инциденти свързани с грешки и неправилни конфигурации, направени по време на разработката – 12 инцидента през юли 2020 г. – юни 2021 г.;
- инциденти причинени от физически бедствия – 2 инцидента през периода февруари

– март 2021 г.

Следващият основен термин в КС е *уязвимостта* на софтуер, хардуер и неправилна конфигурация на ИКС [7,10,14]. Десетте най-критични уязвимости за КС за 2021 г. са [15]:

1. *Нарушен контрол на достъп*: Уеб приложенията предоставят достъп до съдържание и функции на определени потребители - контролът на достъпа (оторизация). Извършват се проверки след удостоверяване и управляват разрешените дейности на „упълномощените“ потребители. Контролът на достъпа на уеб приложението е тясно свързан със съдържанието и функциите, които сайтът предоставя. При нарушен контрол на достъпа, потребителите могат да попаднат в групи или роли с различни способности или привилегии.

2. *Нарушена криптография*: Чувствителните данни, които трябва да бъдат защитени, или *не са защитени*, или са защитени от *недостатъчна криптография* (*https://www.pullrequest.com/blog/what-are-cryptographic-failures-and-how-to-prevent-giant-leaks*).

Чувствителни данни са всяка информация, която организацията не би искала да бъде видима от широката публика.

Не са защитени данните - отклоняването от стратегия за защита след като тя е въведена.

Недостатъчната криптография - лесно да бъде компрометирана. Основната концепция на криптографията не е да се създават шифри, които е невъзможно да се разбият, а да се създават шифри, които е невъзможно да се разбият в рамките на разумен период от време, като се има предвид изчислителната мощност, налична в момента.

3. *Инжекции*: Техника за инжектиране на код, използвана за атака на приложения или на системи управляващи бази от данни, при която злонамерени изрази се вмъкват в поле за въвеждане и последващо изпълнение. Инжекцията използва уязвимост в сигурността на софтуера на приложението. Тя се ползва за атака за уебсайтове и на всякакъв тип база данни.

4. *Несигурен дизайн - уязвимости в дизайна*: Уязвимости, които съществуват поради липса на внедряване на сигурност в приложението по време на разработката. Такива са: генериране на съобщение за грешка, съдържащо чувствителна информация, незащитено съхранение на идентификационни данни, нарушение на границата на доверие - съхраняване на надеждни и ненадеждни данни в една и съща структура от данни или структурирано съобщение (https://gupta-bless.medium.com/insecure-design-vulnerabilities-what-are-they-and-why-they-occurs-3a56ae080ca4).

5. *Неправилна конфигурация на сигурността*: Възникват, когато настройките за защита не са дефинирани, внедрени и се поддържат стойности по подразбиране. Това означава, че настройките за конфигурация не отговарят на индустриалните стандарти за сигурност. Неправилно конфигуриране се случва, когато системен администратор или разработчик на база данни не конфигурира правилно рамката за сигурност на приложение, уебсайт, облачно хранилище, десктоп или сървър, което води до опасни отворени пътища за хакери.

6. *Уязвими и остарели компоненти*: Когато софтуерен компонент не се поддържа, остарял е или е уязвим към известен експлойт. Използване на уязвими софтуерни

компоненти представлява заплаха за уеб приложението. Много софтуерни компоненти работят със същите привилегии, както самото приложение, всякакви уязвимости или недостатъци в компонента могат да доведат до заплаха за уеб приложението. Атаки, които могат да са насочени към известни уязвимости на компонентите са: инжектиране на код; препълване на буфера; командна инжекция; междусайтови скриптове.

7. *Неуспешна автентификация и оторизация*: Възникнат, когато функциите, свързани с идентичността на потребителя, удостоверяването или управлението на сесията, не са внедрени правилно или не са адекватно защитени. Нападателите могат да използват неуспехите при идентификация и удостоверяване за компрометиране на пароли, ключове или да използват други недостатъци в реализацията, за да поемат самоличността на други потребители, временно или постоянно.

8. *Нарушения в целостта на софтуера и данните*: Грешките в целостта на софтуера и данните се отнасят до код и инфраструктура, които не защитават срещу нарушения на целостта. Това може да се случи, когато се използва софтуер от ненадеждни източници и хранилища или дори софтуер, който е бил променен в източника, по време на пренос или дори в кеша на крайната точка. Нападателите могат да използват това, за да въведат потенциално неоторизиран достъп, злонамерен код или компрометиране на системата.

9. *Нарушения при регистриране и мониторинг*: Нарушения при регистриране и мониторинг прави приложението податливо на атаки, насочени към което и да е приложение. Следните типове атаки могат да са резултат от неуспех при регистриране, мониторинг или докладване на събития за сигурност: инжектиране на код; препълване на буфера; командна инжекция; междусайтови скриптове; принудително сърфиране.

10. *Фалшифициране на заявка от страна на сървъра*: Недостатъците при фалшифициране на заявка от страна на сървъра възниква, когато уеб приложение извлича отдалечен ресурс, без да валидира предоставения от потребителят URL адрес. Уязвимото уеб приложение често има привилегии да чете, записва или въвежда данни с помощта на URL. За да изпълни тази атака, нападателят злоупотребява с функционалността на сървъра, за да чете или актуализира вътрешни ресурси. След това той може да принуди приложението да изпраща заявки за достъп до непредвидени ресурси, като често заобикаля контролите за сигурност.

OSI МОДЕЛ И КИБЕРСИГУРНОСТ

OSI е справочен модел за комуникацията на компютърните мрежи [5, 8]. Чрез него организациите могат да разберат местоположението на уязвимости в мрежата, в тяхната инфраструктура и да ги контролират по подходящ начин. OSI е йерархичен модел, указва движението на пакетите в мрежата, въздействието на КА на всяко ниво и разрушенията, които могат да възникнат.

Използването на OSI модела във всички информационни и комуникационни устройства е основа за КА върху неговите слоеве. Ето защо разясняването на връзката между характеристиките на всеки слой (дейност на слоя, преминаващите данни, използваните протоколи, среда за разпространение) и възможните видове атаки върху всеки от тях е от фундаментално значение за осъществяване на защитата на информационните и комуникационни ресурси. Възможни атаки върху OSI слоевете са:

Приложен слой 7: Експлойт, потребителски акаунти, пароли, снифинг (прихващане на данни чрез улавяне на мрежовия трафик със снифер за пакети. HTTP GET и HTTP

POST заявки. По време на атаката потребителят няма достъп до мрежовите ресурси. Разпространява се в http://www.url.com или cookies.

Презентационен слой 6: Фишинг, SSL (Secure Sockets Layer), TLS (Transport Layer Security) снифинг по време на сесията. Атакуващите използват SSL за да тунелират на HTTP атаките към сървъра. Засегнатите системи спират да приемат SSL връзки или автоматично се рестартират. Разпространява се в http://www.url.com или cookies.

Сесиен слой 5: Hijacking (отвличане на сесии), TELNET &FTP снифинг / TELNET DDOS атаки. HTTPS, SFTP и Secure Shell (SSH) да се ползват. Деактивирани са операциите по управление и достъп. Разпространява се в http://www.url.com или cookies.

Транспортен слой 4: Разузнаване, DDOS, TCP [8] сесия снифинг, port снифинг / SYN Flood - форма на атака с DDOS. Нападателят инициира връзка със сървър, без да финализира връзката. Нападателят изпраща SYN пакет, част от установяването на връзка.

Smurf Attack – DDOS е. Голям брой пакети на ICMP с IP адреса на жертвата се излъчват към компютърна мрежа. Повечето устройства по подразбиране отговорят, като изпращат отговор до IP адреса жертвата. Ако броят на машините в мрежата е много голям, компютърът на жертвата ще бъде наводнен от трафик. Забавя се компютъра на жертвата до невъзможност да работи. Ограничения на свързването с хост. Разпространява се в TCP порт 80 зar HTTP, UDP порт 161 за SNMP.

Мрежов слой 3: Man in the middle IP [8]. Нападателят тайно предава и ако е необходимо, променя връзката между две страни - изтриване или изкривяване на информация. Компрометира се комуникационния канал. Port снифинг се извършва– определяне на отворените портове. DDOS атака на инфраструктурата. Влияе върху честотната лента на мрежата и води до допълнително натоварване на защитната стена. Разпространява се в рутери.

Канален слой 2: Spoofing MAC, ARP Snifing/spoofing атака (подправяне, отравяне, измамване) изпращане на фалшиви ARP съобщения през локалната мрежа. Основава се на недостатъци в протокола ARP. Нападателят изпраща подправен протокол за разрешаване на адреси в локална мрежа. Цел - да се свърже MAC адресът на атакуващия с IP адреса на друг хост-жертва. Целият трафик на жертвата се препраща към атакуващия. Атаката се използва за други атаки като Man-In-The-Middle, DDOS, Session Hijacking, DNS Spoofing и др. MAC flooding. Смущава потока от данни от подателя към получателя през всички портове. Разпространява се в Ethernet мрежите, switches, hubs и др.

Физически слой 1: Sniffing (душене). Промяна на данните на ниво бит. Унищожава данни. Разпространява се в UTP, STP, оптични кабели, хъбове, патч панели и RJ45.

Освен указаните възможни атаки с времето непрекъснато се добавят и други. Киберзащита изисква регулярно оценяване на ИКС-ми съобразено с нововъзникващите заплахи и уязвимости, последвано от въвеждане на допълнителни мерки за защита.

ЗАКЛЮЧЕНИЕ

В статията е извършен преглед на областите на КС. Също така са обхванати и разяснени в тяхната цялост заплахите и уязвимостите съгласно данните от 2021 г. Освен това тяхната обвързаност с OSI модела, дейността на слоевете, използваните от тях протоколи, среда за разпространение и заплахите върху слоевете и възможности

уязвимости.

Приложение на основни инструменти за киберзащита, съобразени с всеки слой и възможните заплахи върху него е едно бъдещо такова поле за изследване и продължение на концепцията заплахи – уязвимости – OSI модел – въздействие – отбрана и реакция. Освен това необходимо е систематизирано детайлизиране на уязвимостите в операционните системи, приложния софтуер, ИКС с цел по-ясно да се разкрие зависимостта уязвимости – софтуер – отбрана. На базата на тази функционалност съответните софтуерни решения за киберзащита се разкриват по-явно.

ЛИТЕРАТУРА

[1] A. Jason (2019). *"Foundations of Information Security"*, No Starch Press, ISBN 9781718500051 (ebook),

[2] B. Charles and others. (2015). *"Definition of Cybersecurity - Gaps and overlaps in standardisation"*, European Union Agency For Network And Information Security, V1.0.

[3] E. Boradjieva, Y. Shterev. (2020). "Technological and Psychological Aspects of Cyber Security", NMU "V. Levski ", *Annual University Conference*, 28-29 June 2020, pp. 9, 123-131, Publishing complex of NMU "V. Levski", ISSN: 1314-1937, Vol. 5.

[4] Enisa Threat Landscape, (2021), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[5] Forouzan Behrouz. (2010). "*TCP/IP Protocol Suite*", ISBN:978-0-07-337604-2, McGraw-Hill Education.

[6] M. Greg, O. Santos. (2020). *"Certified Etical Hacker (CEH)"* Version 10 Cert Guide, 3 edition, published by Pearson Education, Bulgarian publishing house "Alexsoft".

[7] Kennedy David, O'Gorman Jim, Kearns Devon, Aharoni Mati. (2011). *"Metasploit: The Penetration Tester's Guide"*, Publisher: William Pollock.

[8] Komar Brian Smas (1998). *"Teach Yourself TCP/IP Network Administration in 21 days"*, ISBN 954-8455-55-9, Bulgarian publishing house "InfoDar".

[9] Mike O'Leary. (2019). *"Cyber Operations: Building, Defending, and Attacking Modern Computer Networks"*, ISBN-13 (electronic): 978-1-4842-4294-0, Towson, MD, USA.

[10] P. Stavroulakis, M. Stamp (Editors). (2010). *"Handbook of Information and Communication Security"*, e-ISBN 978-3-642-04117-4, Springer-Verlag Berlin Heidelberg.

[11] Y. Shterev. (2020). "Influence of cybersecurity on management systems", *NMU "V. Levski ", Annual University Conference*, 28-29 June 2020, pp. 11, 132-142, Publishing complex of NMU "V. Levski", ISSN: 1314-1937, Vol. 5.

[12] Y. Shterev. (2020). "Principles for building a cybersecurity system, regulatory framework", *NMU "V. Levski ", Annual University Conference,* 28-29 June 2020, pp. 11, 112-122, Publishing Complex of NMU "V. Levski", ISSN: 1314-1937, Vol. 5.

[13] Y. Shterev. (2020). "Systems for detection and prevention of intrusion into information and communication systems", *NMU "V. Levski ", Scientific Conference "Current Security Issues",* October 22-23, Vol. 5, p.10, pp.87-96, ISSN 2367-7465.

[14] https://seclists.org/pen-test/.

[15] https://owasp.org/www-project-top-ten/ - Open Web Application Security Project.