ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ИКОНОМИКА И МЕНИДЖМЪНТ ПАЗАРДЖИК

ДИПЛОМЕН ПРОЕКТ

на **ГЕРГАНА АНГЕЛОВА СИНДОНАС**
ученик от **XII А** клас

Тема:

«ЗАЩИТА В УЕБ ПРОСТРАНСТВОТО И КИБЕРСИГУРНОСТ В УСЛОВИЯТА НА ГЛОБАЛНАТА ИКОНОМИКА»

Ученик:	**Гергана Синдонас** (име, фамилия)	..... (подпис)
Ръководител-консултант:	**Анета Зашева** (име, фамилия)	…… (подпис)
Директор**:**	**Таня Благова** (име, фамилия)	..... (подпис и печат на училището)

2023-2024 учебна година

ЗАДАНИЕ ЗА ДИПЛОМЕН ПРОЕКТ ДЪРЖАВЕН ИЗПИТ ЗА ПРИДОБИВАНЕ НА ТРЕТА СТЕПЕН НА ПРОФЕСИОНАЛНАКВАЛИФИКАЦИЯ – ЧАСТ ПО ТЕОРИЯ И ПРАКТИКА НА ПРОФЕСИЯТА

по професия код ***482010*** *„Икономист-информатик“*

специалност код ***4820101*** *„Икономическа информатика“*

ТЕМА В ЧАСТ ТЕОРИЯ : **Защита в уеб пространството и киберсигурност в условията на глобалната икономика.**

Изисквания за разработката на дипломния проект в част теоретична разработка:

1. Какво е киберсигурност?
2. Кои са ефективните начини за защита в интернет пространството?
3. Прокси сървър за защита на компютър - характеристика, предимства и недостатъци
4. Киберсигурността и изучаваните програмните езици
5. GDRP (General Data Protection Regulation) – същност и предназначение на проекта.

ТЕМА В ЧАСТ ПРАКТИКА: ***Да се създаде уеб сайт за видовете компютърни заплахи и начините за противодействие чрез изучаваните програмни езици.***

Изисквания за разработката на дипломния проект в част практика:

- Да се използват изходни ресурси със свободни права.
- Да се определи цветовия нюанс и да се направи правилен подбор на цветове за уеб страниците от вашия сайт, използвайки онлайн инструмент като https://coolors.co/ или https://www.w3schools.com/colors/colors_picker.asp, както и др. Изборът на цветова гама да бъде съхранена като снимка и приложена в раздел „Приложения“ като приложение №1 на разработката.
- Да се създаде проект на сайта, съдържащ архитектура на всяка отделна страница в него, цветова палитра с шестнайсетични кодове и коефициент на контраст в заглавията и в основната част чрез използване на онлайн инструмент като https://contrast-ratio.com/. Да се анализират писмено в проекта и да се направи извод за получените коефициенти. Според изискванията на World Wide Web Consortium (W3C) коефициентът на контраст трябва да бъде най-малко 4,5:1 за малък текст / измерен във main, footer, aside, section / и най-малко 3:1 за голям текст/ измерен във header/. Проектът да се вмъкне в разработката в раздела „Приложения“, като приложение №1.
- Сайтът да съдържа **7 страници**: **начало**, **за фирмата**, **каталог**, **галерия,**

промоция, контакти и автор.

- Всяка от страниците да има изградено вертикално меню със стил, стилизирано по избор на автора и съгласно изискванията на индивидуалното задание.
- На две от страниците във вашия сайт да бъде изготвен банер /размер 960x200/ с лого и име на фирмата, с подходящ фон или снимка, а на всички останали само лого с името на фирмата.
- В страницата **„начало“** да е вградено, авторско лого, съдържащо изображение и името на фирмата, създадено на платформа по избор, снимка, текст, или видео – по избор на автора, икони препратки, име на автора, дата/час и символ за всички права запазени!
- Страницата „**за фирмата“** да съдържа два вида интерактивна графика с продажбите на антивирусни програми за последните 4 години – кръгова и колонна, както следва: **2020г.-13 400 антивирусни софтуери** ; **2021г.-10 200 антивирусни софтуери**; **2022г.-11 840 антивирусни софтуери**; **2023г.-5 400 антивирусни софтуери**. Да се анализират данните от всяка диаграма с минимум 5 изречения.
- Страницата **„каталог“** да съдържа три секции с 6 артикула за предлагани антивирусни програми и защити с наименование, цена и снимка. Върху снимките да бъдат приложени ефекти – роловър, уголемяване или др. по избор на автора. Да има линк най-отдолу към наименованието на всяка секция и към началото на сайта.
- В страница **„промоция“** да се постави банер и да е представен промоционален продукт с поведение /изскачащо съобщение/ към него, а също и да има вградено рекламно видео. Да се включи снимка, стара/зачертана/ и нова цена на рекламирания продукт.
- Страница **“галерия“** да бъде изготвена с 15 изображения, които при кликане с мишката да имат приложен друг ефект със стил.
- Страницата **„контакт“** да се постави банер и да съдържа работеща форма за обратна връзка, изготвена с PHP. Да бъде с дизайн на целия сайт и да бъде тестван на Xampp. Самостоятелният файл или файлове с разширение php да бъде съхранен и в папката на сайта.
- Страницата **„автор“** да съдържа снимка на автора, кратко представяне и линкове към реализирани проекти, грамоти, награди или приза /ако има такива/.
- Да се приложи сянка и закръгление на елементи в поне една от страниците.
- Да се сложи favicon на всяка от страниците-умалена версия на логото, което сте създали използвайки онлайн конвертор като https://image.online-convert.com/convert-to-ico .
- Да се изготви и приложи като приложение №2 кода на страница по избор на зрелостника.

График за изпълнение:

а) дата на възлагане на дипломния проект	***20.11.2023***
б) контролни проверки и консултации	
1.	***10.01.2023***
2.	***23.01.2024***
3.	***08.02.2024***
4.	***08.03.2024***
в) краен срок за предаване на дипломния проект	***15.04.2024***

Съдържание и оформяне на дипломния проект

А. Съдържание на дипломния проект:

Оформяне на дипломния проект в следните структурни единици:

- титулна страница;
- съдържание;
- увод (въведение);
- основна част
- заключение;
- списък на използваната литература;
- приложения.

Титулната страница съдържа наименование на училището, населено място, тема на дипломния проект, трите и мена на ученика, професия и специалност, име и фамилия на ръководителя/консултанта.

Уводът (въведение) съдържа кратко описание на основните цели и резултати.

Основна част - Формулира се целта на дипломния проект и задачите, които трябва да бъдат решени, за да се постигне тази цел. Съдържа описание и анализ на известните решения, като се цитират съответните литературни източници. Съдържа приносите на дипломния проект, които трябва да бъдат така формулирани, че да се вижда кои от поставените задачи са успешно решени.

Заключението съдържа изводи и предложения за доразвиване на проекта и възможностите за неговото приложение.

Списъкът с използваната литература включва цитираната и използвана в записката на дипломния проект литература. Започва на отделна страница от основния текст. При имената на авторите първо се изписва фамилията. Всички описания в списъка с използваните източници трябва да са подредени по азбучен ред според фамилията на първия автор на всяка публикация.

Приложенията съдържат документация, която не е намерила място в текста поради ограниченията в обема й или за по-добра прегледност подредба. В текста трябва да има препратка към всички приложения.

Б. Оформяне на дипломния проект

Формат: А4; Брой редове в стр.: 30; Брой на знаците: 60 знака в ред; номера на страниците долу вдясно. Общ брой на знаците в една страница: 1800 – 2000 знака. Шрифт: Times New Roman, 12 pt, обем не по-малък от 20 страници разпечатани едностранно на хартиен носител. При оформяне на проекта да се използват фигури, таблици, графики, диаграми и други подходящи средства за онагледяване на съдържанието. Разпечатка на код от практическата част от разработката. Дипломният проект се предава подвързан **със спирала** по образец на титулна страница и цветни графики, таблици, диаграми, изображение и др. в определения от изпитната комисия срок.

В. Дипломния проект в частта теория да се представи чрез:

а) презентация;

б) графични материали;

Дипломния проект в частта практика да се представи чрез:

а) демонстрация;

б) компютърна мултимедийна симулация и анимация.

С ъ д ъ р ж а н и е

ПЪРВИ РАЗДЕЛ - УВОД

В днешния двадесет и първи век, технологиите проникват във всеки аспект на живота ни и поради тази причина мерките за сигурност придобиват все по-голямо значение. От личен план до влиянието върху глобалната икономика, защитата в уеб пространството е от първостепенно значение.

В личен план киберсигурността е ценна за опазването на всякакъв вид чувствителна информация. От онлайн банкирането до акаунтите в социалните мрежи - ние поверяваме множество лични данни на цифровата сфера. Киберсигурността ни дава възможност да направим своето онлайн присъствие защитено от потенциални заплахи.

Отвъд индивидуалните проблеми, значението на киберсигурността се простира до по-широкия обхват на човечеството. Една кибератака не само застрашава личните данни, но може да има и тежки последици за обществената безопасност, икономическата стабилност и националната сигурност.

Киберсигурността е ключов елемент в защитата срещу киберзаплахите, които могат да компрометират чувствителна информация и дори да повлияят на функционирането на инфраструктурата.

Основната цел на този дипломен проект е ролята на киберсигурността и защитата в уеб пространството, в условията на глобалната икономика. В изпълнението й, в основната част ще бъдат решени следните задачи:

1. Какво е киберсигурност?
2. Кои са ефективните начини за защита в интернет пространството?
3. Прокси сървър за защита на компютър- характеристика, предимства и недостатъци
4. Киберсигурността и изучаваните програмни езици
5. GDRP (General Data Protection Regulation)- същност и предназначение на проекта

ВТОРИ РАЗДЕЛ - ОСНОВНА ЧАСТ

1. Какво е киберсигурност?

Киберсигурността е начинът, по който системите, мрежите и програмите се използват, като практики за защита срещу цифрови атаки. Кибератаките често са насочени към чувствителна информация и данни, като след получен достъп до тези данни, киберпрестъпниците изнудват за пари потребители и компании, прекъсват нормалните процеси или премахват цели сайтове.

Ефективната киберсигурност е ключов компонент за всеки бизнес. В нашия модерен свят, управляван от данни, защитата от кибератаки става все по-голямо предизвикателство поради нарастващото количество налична информация, която предоставяме на устройствата си.

Фиг. №1

„Киберсигурност" е само общо понятие, но само по себе си обхваща голям спектър от области:

- Сигурност на критичната инфраструктура

Сигурността на критичната инфраструктура защитава компютърните системи, приложенията, мрежите, данните и цифровите активи, от които зависи националната сигурност, икономическото здраве и обществената безопасност.

- Мрежова сигурност

Мрежовата сигурност предотвратява неоторизиран достъп до мрежови ресурси, открива и спира кибератаки и нарушения в процес на изпълнение - като същевременно гарантира, че оторизираните потребители имат сигурен достъп до необходимите им мрежови ресурси, когато им трябват.

- Сигурност на крайната точка

„Крайните точки" - сървъри, настолни компютри, лаптопи, мобилни устройства - остават основната входна точка за кибератаки. Сигурността на крайните точки предпазва тези устройства и техните потребители от атаки.

- Сигурност на приложенията

Този вид сигурност защитава приложенията, работещи на място и в облака, като предотвратява достъп който хакерите могат да използват, за да проникнат в мрежата.

- Информационна сигурност

Информационната сигурност (InfoSec) се отнася до защитата на цялата важна информация на организацията - цифрови файлове и данни, документи на хартия, физически носители, дори човешка реч - от неоторизиран достъп, разкриване, използване или промяна.

1.1. Цели на киберсигурността

Целите на киберсигурността се определят от необходимостта да се защитят компютърните системи, мрежи и данни от различни видове заплахи и атаки. Нейната роля включва следните цели:

- Защита на конфиденциалността:

Киберсигурността има за цел да предпази конфиденциалната информация от неупълномощен достъп. Това включва лични данни, корпоративна информация, финансови данни и други чувствителни ресурси (assets). Защитата на конфиденциалността е от съществено значение, особено с оглед на нарастващите заплахи.

- Гарантиране на цялостта на данните:

Киберсигурността цели да осигури, че данните остават непроменени и цели в тяхната пълнота. Атаките могат да окажат сериозно влияние върху правилната функционалност на системите и данните, поради което е важно да се гарантира цялостта на информацията.

- Защита на достъпа:

Киберсигурността има за цел да ограничи достъпа само до упълномощени потребители. Това включва използването на проверки на идентичността и контрол върху правата за достъп, гарантирайки, че само оторизирани лица имат право да влизат в системите и да манипулират информацията.

- Предотвратяване на злоупотреби и атаки:

Киберсигурността се стреми да предотврати различни видове злоупотреби и атаки, включително вируси, троянски коне, фишинг атаки, DDoS атаки и други форми на киберзаплахи.

- Съответствие с регулаторни изисквания:

Киберсигурността играе съществена роля в поддържането на съответствие с регулаторните стандарти и закони, които уреждат защитата на данните. Това включва съответствие със законодателство като GDPR (General Data Protection Regulation), което заличава необходимостта за защита на личните данни на гражданите на Европейския съюз.

1.2. Видове неоторизиран достъп

Киберзаплахите могат да варират от очевидни, като например имейл от чуждестранен източник, предлагащ малко състояние, ако само предоставите номера на банковата си сметка - до хитроумно скрити, като например злонамерен код, който се промъква през киберзащитата и живее в мрежата месеци или години, преди да предизвика, скъпоструващ пробив в данните.

Схема №1

Например: зловреден софтуер (Malware) - съкращение от "злонамерен софтуер" - е софтуерен код, написан умишлено, за да навреди на компютърна система или на нейните потребители. Почти всяка съвременна кибератака включва някакъв вид зловреден софтуер. Участниците в заплахите използват атаките със злонамерен софтуер, за да получат неоторизиран достъп и да изкарат заразените системи от строя, като унищожават данни, крадат поверителна информация и дори изтриват файлове, които са от ключово значение за операционната система.

Често срещаните видове зловреден софтуер включват: (Ransomwere) Софтуер за откуп, който заключва данните или устройството на жертвата и заплашва да ги задържи заключени, или да ги разкрие публично, ако жертвата не плати откуп на нападателя. Друг пример за такъв тип атака е всеизвестният троянски кон, който е зловреден код, подмамващ хората да го изтеглят, защото изглежда като полезна програма или се крие в легитимен софтуер. Примерите включват троянски коне за отдалечен достъп (RAT), които създават тайна задна врата на устройството на жертвата, или троянски коне тип dropper, които инсталират допълнителен зловреден софтуер, след като се установят в целевата система или мрежа.

Друг вид са червеите, които се самовъзпроизвеждат и автоматично се разпространяват в приложения и устройства без човешко взаимодействие.

Социално инженерство и фишинг - са вид манипулация, подтикваща мишените да предприемат действия, които разкриват поверителна информация, застрашават тяхното собствено или на организацията финансово благосъстояние, или по друг начин казано компрометират личната или организационната сигурност. Фишингът е най-известната и най-разпространената форма на социално инженерство. При фишинга се използват фалшиви имейли, прикачени файлове към имейли, текстови съобщения или телефонни обаждания, за да се подмамят хората да споделят лични данни или идентификационни данни за вход, да изтеглят зловреден софтуер, да изпратят пари на киберпрестъпници или да предприемат други действия, които могат да ги изложат на риск от киберпрестъпления.

Често срещаните видове фишинг включват:

Spear phishing - силно насочени фишинг атаки, които манипулират конкретно лице, като често се използват данни от публичните профили на жертвата в социалните мрежи, за да бъде измамата по-убедителна.

Whale phishing - фишинг, който е насочен към корпоративни ръководители или богати лица.

Business email compromise - измами, при които киберпрестъпниците се представят за ръководители, доставчици или доверени бизнес партньори, за да подмамят жертвите да преведат пари или да споделят поверителни данни.

Друга често срещана измама, свързана със социалното инженерство, е подмяната на име на домейн (наричана още DNS подмяна), при която киберпрестъпниците използват фалшив уебсайт или име на домейн, който се представя за истински - например "applesupport.com" за support.apple.com - за да подмамят хората да въведат поверителна информация. Във фишинг имейлите често се използват подправени имена на домейни на подателя, за да изглеждат по-достоверни.

Man-in-the-Middle (MITM) attack - при този тип атака се подслушва мрежова връзка, за да се прихванат и предадат съобщения между две страни. Незащитените Wi-Fi мрежи често са щастливи ловни полета за хакери, които искат да извършват MITM атаки.

Denial-of-Service (DoS) attack - претоварва уебсайт, приложение или система с голям обем измамен трафик, като ги прави твърде бавни за използване или напълно недостъпни за легитимните потребители.

Password attack - при тези атаки киберпрестъпниците се опитват да отгатнат или откраднат паролата, или данните за вход в акаунта на даден потребител. При много атаки с пароли се използва социално инженерство, за да се подмамят жертвите да споделят неволно тези чувствителни данни. Хакерите обаче могат да използват и атаки с груба сила (brute force attacks).

1.3. Мащабни кибератаки

- През 2007 година Естонското правителство, банки и медии стават жертва на една от най-големите и сложни атаки в човешката история. Като причина за тях се счита демонтиран в Талин паметник, посветен на Втората световна война. Групата, която успява да свали онлайн услугите и сайтовете, се представя като "Nashi". Щетите, които претърпява Естония в резултат на безпрецедентната вълна от кибератаки, се изчисляват на десетки милиони евро.

- Най-мащабната кибератака в света, позната още като "Епсилон", успява да нанесе изключителни финансови щети на гиганти като JP Morgan и Best Buy. Кражбата на потребителски данни възлиза на 4 милиарда долара.

- Американското правителство е цел на много кибератаки, а най-ранният опит за разбиване на мрежа с престъпна цел е познат като Moon Maze. Атаката е изключително добре координирана и толкова добре скрита, че в продължение на две години кибертерористите успяват да събират конфиденциална информация за военни операции на САЩ.

- Titan Rain е друг кибер набез, който успява да проникне в мрежите на NASA, Пентагона и Lockheed Martin /оръжеен производител в САЩ/. Атаката не просто поразява компютърните мрежи, а ги оставя незащитени срещу кибертероризъм от трети страни.

От зората на модерните компютърни технологии, винаги се намира човек (или група хора), които да изявяват повече интерес към това как могат да експлоатират технологията по непредвиден или необичаен начин. Това често включва и получаването на достъп до права или данни, до които човек не би трябвало да стига, а именно това, което наричаме „хакване" днес. Въпреки че за много от хората, които го практикуват, това занимание служи за професия, задоволяване на лично любопитство или „за спорта", винаги има и такива, които решават да използват уменията си за престъпни цели. Образът на модерния хакер – такъв, какъвто го познаваме от телевизионния екран – сам, в тъмна стая, взиращ се в монитор, по който препускат редове от привидно непознати на

човечеството символи, може да не е напълно точен. Атаките, с които ще Ви запозная сега, обаче, могат да засенчат дори и тези от филмовата индустрия.

- The Morris Worm

Първият и един от най-вредните червеи, които се разпространяват онлайн е този, направен от Робърт Морис през 1988 година. Въпреки, че първоначално Морис цели просто да провери колко голямо е киберпространството, до което има достъп чрез код, който се разпространява из всички свързани онлайн компютри, той бързо прераства в бедствие, след като започва да причинява грешки в инфектираните системи. Около 6000 компютри биват инфектирани и изкарани извън строя, което по това време би оставило щети на сметка между 10 и 100 милиона долара.

- Веригата Target

В една от най-големите атаки от рода си в САЩ, уязвимост в онлайн услугите на веригата магазини Target бива експлоатирана и дава шанс на неустановените извършители да откраднат между 40 и 110 милиона записа за кредитни карти. Мащабът на атаката не се дължи толкова на уменията на извършилите, колкото на игнорирането на огромната уязвимост от страна на Target.

Този пример ни кара да осъзнаем, че сама по себе си уязвимостта не е опасна, тъй като тя може да не бъде използвана с години. Опасността идва, когато уязвисмостта е открита и се използва.

- Mirai Botnet DDoS

Internet of Things епохата ни носи много възможности, които сме виждали само в най-клишираните фантастични филми, но ни носи и много уязвимости. Поради все по-бързите темпове на напредване на електрониката, осигуряването на безопасност със сигурност не е приоритет, както ни показва тази атака. Mirai е мрежа от експлоатирани IoT устройства, която стои зад едни от най-големите и вредни DDoS (Distributed Denial of Service) атаки, които познаваме до днес, включително такава, която беше усетена по цял свят.

- Red October

„Червеният октомври“ е атака, която е намерена през 2012 година и е действала на глобално ниво с цел крадене на дипломатическа и бизнес информация от различни държави и организации. Не е ясно каква точно е била целта на атаката и кой стои зад нея, но след идентифицирането ѝ, интернет и домейн доставчици от цял свят се обединяват и намират всички 60 домейна, които са служели за приемане на информацията. След акцията, самите извършители на атаката я прекъсват без обяснение.

- Stuxnet

Stuxnet е атака, която бихте очаквали да видите на телевизионния екран. Смятана от много за обединено усилие от страна на САЩ и Израел. Атаката цели да изкара извън строя програмата за ядрено въоръжаване на Иран. Най-интересното при нея е начинът ѝ на работа - Stuxnet цели да зарази компютри в заводи за оръжия. Веднъж щом зловредният код достига до приемника си, той започва да търси определен тип софтуер, който служи за управление на всякакви видове машини. Щом бъде намерен такъв софтуер, Stuxnet започва да му подава случайни команди, но показва на потребителите, че всичко е наред. Това, естествено води до редица „нещастни инциденти“, за които, обаче, нямаме информация поради естеството на атаката.

Кибератаките са с по-голям потенциал за нанасяне на значителни щети от физическите терористични атаки, тъй като са на сравнително ниска цена, поради факта, че не се инвестира в реални оръжия и взривни устройства. Друго тяхно „предимство“ е, че се провеждат от разстояние и в повечето случаи анонимно. Множество институции в световен план се занимават със защитата на интернет потребителите. Все по-масовото проникване на информационните технологии и разрастването на интернет са предпоставки за разработване на относително нискоструващи кибероръжия, които представляват потенциална заплаха за поддържаната информация не само за системи и мрежи с военно предназначение, но и за мрежови структури с гражданско предназначение. Глобалната мрежа, световните информационни и комуникационни системи могат да се разглеждат като ново поле за водене на бойни действия, за което

разстоянията и местонахождението са без значение. През последните години се наблюдава тенденция на увеличаване на броя и разнообразието на констатираните кибератаки като обхват, използвани технологии и преследвани цели. Поради тази причина е необходимо да се проследяват, изследват и анализират различните случаи на кибератаки в световната мрежа и възможните щети, които биха нанесли.

1.4. Инструменти и технологии

Разбира се, за да се предпазим пълноценно от хакерите не е необходимо да сме компютърни гении, нито са достатъчни само теоритични знания, необходими са ни инструменти и технологии, които да приложим в ситуациите. Ако сте прекарвали известно време в обкръжението на ИТ специалисти или дори само сте гледали научнофантастичен филм, то вероятно сте чували за инструменти за киберсигурност, наречени защитни стени (Firewalls). Защитната стена ограничава неупълномощения достъп чрез динамично филтриране на опитите за достъп до системата чрез компютърната мрежа. Като резултат засича и предупреждава за атаки в реално време. Защитната стена представлява „граничен контролен пункт“ за желаещите да преминат пакети. Целият трафик се осъществява през този пункт, който има за задача да пропуска, само което е безопасно. При настройка на защитата има два генерални подхода:

- Пропускат се всички данни и услуги с изключение на изрично забранените,

- Забраняват се всички данни и услуги с изключение на специално разрешените.

Защитната стена, блокира данните, за които има вероятност да прикриват хакерски атаки, скрива информация за мрежата, като за изходящия трафик маскира IP адреса на мрежата с IP адреса на защитната стена, води дневници (logs) за информационния поток със записи на определени събития. Данните се блокират, когато не отговарят на правилата за сигурност, зададени от администратора на мрежата. Например, ако от определен източник са регистрирани опити за хакерски атаки или flooding, администраторът задава

правило за отхвърляне на всички пакети с IP адреса на този източник. Много често за подобно филтриране не е необходим допълнителен софтуер, а е възможно то да се извърши и от маршрутизатора (всички съвременни маршрутизатори имат такава функционалност). Освен входящите данни могат да се блокират и изходящите. По този начин се защитава останалият свят от локалната мрежа и могат да се забранят някои потенциално опасни услуги и действия от даден хост. Замяната на адресната информация осигурява анонимност на защитаваната мрежа. Така се прикриват вътрешните мрежови характеристики от външната мрежа. Най-често се скриват DNS, FINGER и други протоколи. Чрез тях би могла да бъде получена вътрешно мрежова информация, чрез която по-нататъшното проникване в мрежата ще бъде максимално улеснено.

В логовете на защитната стена обикновено се пази подробна информация за допуснатите и отхвърлените от стената пакети, като например мрежовите адреси на източника на пакета и дестинацията, номерата на портовете на източника, типа протокол и други. На базата на тази информация може да се прави одит на причините за възникване на дадено събитие.

Освен основните си функционалности, защитната стена между мрежи има и допълнителни възможности:

- филтриране на съдържанието (content filtering),

- преобразуване на мрежови адреси и номера на портове (network address translation, port address translation),

- балансиране на натоварването (bandwidth shaping, QoS),

- откриване на пробиви в системата (intrusion detection).

- Филтриране на съдържанието

Когато се налага ограничение за достъп от вътрешни хостове до определени данни и услуги от външната мрежа, то може да бъде реализирано, като се филтрира съдържанието на заявките по адрес или по ключови думи. Обикновено се блокира достъпът до сайтове с пиратско или порнографско

съдържание, сайтове за електронна поща. Блокират се и файлове с някои разширения - .AVI, .MP3, и exe. При тази функционалност на защитните стени списъкът със забранени (banned) сайтове трябва регулярно да се обновява. При филтрирането на съдържанието може да се избегне досадното или зловредно съдържание на pop-up рекламите, спама по електронна поща, Java аплети, ActiveX програми, троянски коне, вируси и др.

Антивирусният софтуер е още един от инструментите за киберсигурност. Обикновено се препоръчва всеки да инсталира някакъв вид антивирусен софтуер на своите устройства, за да предотврати заразяването им. Понастоящем най-мощният антивирусен софтуер се нарича “next-gen software”. Този тип антивирусен софтуер може да прилага в програмирането си машинно обучение, като например изкуствен интелект, поведенческо откриване и детонация на файлове в облака. Специалистите по киберсигурност трябва да са в крак с най-новите разработки в антивирусния софтуер, за да защитят компаниите, за които работят.

Друг вид техника е така наречения penetration testing - който симулира кибератака срещу дадена система. Прави се тест, който има за цел да идентифицира слабите места в дадена система и да определи вероятността от пробив. Също така помага на специалистите по киберсигурност да определят кои части на системата са най-силни и в момента не се нуждаят от подобрение. За да извърши penetration test, етичният хакер обикновено преминава през 6 различни фази:

Разузнаване: Разузнаването се дели на две части: активно, когато използваме системи и инструменти, генериращи трафик, и пасивно - когато информацията, до която получаваме достъп е публично споделена (например в различните социални мрежи). Тези тестове обикновено се извършват от човек, който не е запознат отблизо със системата, за да събере данни и да се създадат различни сценарии за пробив.

Сканиране: Атакуващият разполага с инструменти, които сканират мрежата и отварят портове, като по този начин допълнително увеличава количеството информация, която знае за мрежата.

Получаване на достъп: Хакерът използва данните, събрани от предишните 2 фази, за да проникне в мрежата. Това може да се извърши ръчно или със софтуер.

Поддържане на достъпа: След като е проникнал в мрежата, тестващият проникването, трябва да се опита да поддържа присъствието си в мрежата, за да открадне възможно най-много данни.

Премахване на доказателствата: След като събере данните, етичният хакер прикрива следите си, за да гарантира, че не може да бъде замесен в атаката. Това става чрез премахване на доказателствата за това какви данни са били събрани и елиминиране на събитията от дневника, за да се запази анонимността.

Завъртане: Атаката включва проникване в други машини в същата мрежа. Този процес повтаря стъпки от 2 до 5, за да се получат допълнителни данни.

След като приключи, етичният хакер, съставя доклад (report) за това как е успял да проникне в системата. Следваща стъпка е предаването на доклада към мрежовия администратор или специалистите по киберсигурност в компанията. Те използват тази информация, за да подсилят защитата на мрежата. Penteration тестовете обикновено се правят чрез операционната система с отворен код - Kali Linux. Използват се инструменти като NMAP, Burp Suite, Metasploit и други.

2. Кои са ефективните начини за защита в интернет пространството?

Кибератаките се увеличават. Въпреки че съвременните технологии предоставят много удобства и ползи, има хора, които злоупотребяват с тях, което представлява заплаха за данните в световен мащаб.

Един пробив в системата, може да има големи последици. Но винаги можем да се поучим от миналото.

Ситуациите са милиони. Всеки ден се извършват различни видове атаки, спрямо социалните мрежи и други апликации, в които споделяме чувствителна

информация. Да сме напълно защитени онлайн е невъзможно, но въпреки това можем да се защитим максимално.

2.1. Опазване на личната информация

Всичко, което публикувате онлайн, може да бъде видяно от целия свят, което означава, че когато кандидатствате за работа, вашият потенциален работодател или клиент ще може да научи за вас много повече от всякога. Уверете се, че единствените неща, които публикувате онлайн, са свързани с професионалната ви биография, постиженията ви и начина, по който да се свържат с вас. Никога не показвайте домашния си адрес, статуса на връзката си или друга лична информация, тъй като това не е необходимо и ви прави по-уязвими за онлайн атака.

Фиг. №2

2.2. Присъединяване към първокласен доставчик на VPN услуги

Няма да можете да избягвате всички обществени Wi-Fi връзки или никога да не въвеждате банковата си информация онлайн и това е нормално. Като използвате първокласна VPN услуга, не само ще криптирате целия си трафик, но и ще получите анонимен IP адрес, който спира следенето.

2.3. Бдителност

Редовната проверка на банковите сметки осигурява сигурност и бърза реакция при евентуална измама. Ето защо повечето банки и финансови институции препоръчват на потребителите си да следят внимателно и редовно движенията по банковите си сметки. Има различни начини, по които може да се разбере какви движения се извършват по сметката – онлайн банкиране, SMS известяване, телефонно обаждане от банката, приложения за смартфон и други.

2.4. Избор на подходяща парола

Хората, които избират слаби пароли, се излагат на по-голям риск. Никога не използвайте пароли, като "123456" или "парола", тъй като киберпрестъпниците ги изпробват първи, заради големия брой хора, които ги използват. Изберете силна парола, която не е лесна за отгатване и разбира се нека всяка идентификация за вход е различна за отделните апликации. Ако имате проблем със запомнянето на паролите си, можете да използвате софтуер за управление на пароли. За да бъде “трудно-разбиваема” една парола, трябва да се използват малки и големи букви, цифри, специални символи. Полезно е, също така да използвате многофакторна идентификация за онлайн акаунти, която изисква да въведете няколко елемента информация, потвърждаващи самоличността ви.

2.5. Защитна стена (firewall)

Защитната стена представлява, както вече споменах, но няма как да не спомена отново, поради нейната важност - представлява „граничен контролен пункт“, за желаещите да преминат пакети. Целият трафик се осъществява през този пункт, който има за задача да пропуска, онова което е безопасно. При настройка на защитата има два генерални подхода:

- Пропускат се всички данни и услуги с изключение на изрично забранените,

- Забраняват се всички данни и услуги с изключение на специално разрешените.

3. Прокси сървър за защита на компютър-характеристика, предимства и недостатъци

3.1. Характеристика

Прокси сървърът, представлява централен компонент в мрежовата сигурност, който осигурява редица характеристики с цел защита и оптимизация на интернет комуникацията.

Прокси сървърът е мрежова технология, която действа като посредник между компютъра на потребителя и интернет, целящ предоставяне на защита и подобряване на сигурността на компютъра. Една от основните характеристики на Прокси сървъра е неговата способност да отразява трафика, като по този начин скрива реалния IP адрес и гарантира анонимност при сърфиране в мрежата.

С разнообразните видове прокси сървъри, като HTTP, HTTPS, SOCKS и Transparent прокси, този инструмент предоставя гъвкавост и възможност за адаптация към конкретните нужди на сигурността на потребителя. Способността за кеширане на данни на прокси сървъра позволява по-бърз достъп до уебсайтове, като същевременно се намалява обемът на трафика.

Прокси сървърът изпълнява също и ролята на филтър за контрол на достъпа, позволявайки на потребителя да блокира определени уебсайтове или категории от съдържание. Това подобрява сигурността, предотвратявайки достъпа до потенциално вредни или зловредни сайтове.

Сигурността на комуникацията се увеличава чрез шифриране на трафика, което предоставя защита от потенциални атаки и откradване на лична информация. Прокси сървърът предоставя информация за сесии, заявки и събития, които могат да бъдат от полза при анализ на сигурността.

Лесната конфигурация и управление на настройките правят този инструмент достъпен и ефективен за широк кръг от потребители.

По друг начин казано, прокси сървърът предоставя баланс между повишаване на сигурността и оптимизация на интернет комуникацията.

Фиг. №3

3.2. Предимства от използването на прокси сървър

Използването на прокси сървъри предоставя редица предимства в различни сфери на интернет комуникацията и сигурността. Някои от основните предимства са анонимност и поверителност - прокси сървърите могат да скрият вашия IP адрес, предоставяйки анонимност при сърфиране в интернет. Това може да помогне за предотвратяване на проследяването на вашата онлайн активност от трети страни.

Прокси сървърите могат да филтрират и блокират зловреден трафик преди той да достигне до вашия уебсайт или мрежа. Това може да предложи допълнителен слой сигурност.

Друго тяхно предимство е конфигурацията за контрол на достъпа до ресурси в мрежата. Този контрол може да включва филтриране на URL адреси, блокиране на определени видове съдържание и други ограничения.

Чрез използването на прокси сървър, организации могат да оптимизират своя мрежов трафик чрез кеширане на често използвани данни и компресиране на трафика.

Прокси сървърите могат да предоставят защита на вашата връзка с интернет чрез шифриране на данните, което може да бъде особено важно при използване на обществени Wi-Fi мрежи.

Въпреки тези предимства, важно е да се отбележи, че използването на прокси сървъри има и своите недостатъци.

3.3. Недостатъци от използването на прокси сървър

Някои от недостатъците при използването на този тип сървър са:

Намалената скорост на връзката: Прокси сървърът може да забави скоростта на интернет връзката поради допълнителната стъпка в пренасочването на трафика.

Ако не се използва шифрована връзка, прокси сървърите могат да бъдат уязвими за атаки или наблюдение на трафика, което може да доведе до компрометиране на лични данни.

Някои прокси сървъри могат да записват логове на интернет активността, което може да застраши поверителността на потребителя.

Прокси сървърът може да бъде единична точка на отказ, което може да доведе до прекъсване на интернет връзката, ако сървърът е недостъпен.

Също така в някои случаи използването на прокси сървъри може да противоречи на законите или условията на ползване на дадена услуга.

Друг недостатък е изискването за конфигуриране на прокси настройките, в различни приложения или устройства може да бъде неудобство за потребителите.

3.4. VPN (Virtual Private Network) пред Прокси сървър

VPN е често предпочитана технология пред прокси сървъра поради няколко причини:

VPN предоставя шифрован “тунел” между устройството на потребителя и VPN сървъра. Това означава, че дори ако трафикът бъде прехванат, трудно ще може да бъде разбран. Прокси сървърите обикновено не предоставят този вид изолация.

VPN пренасочва целия интернет трафик, докато прокси сървърите често се използват само за определени видове трафик. Това означава, че с VPN целият интернет трафик на устройството е защитен.

VPN скрива реалния IP адрес на потребителя и маскира неговата идентичност. Това предоставя по-високо ниво на анонимност в сравнение с прокси сървърите, които често използват IP адреса на клиента.

В сравнение с конфигурирането на прокси на различни приложения или устройства, настройката на VPN е по-лесна и позволява обхватно покритие на целия интернет трафик на устройството.

VPN предоставя защита на всички приложения и услуги, използвани на устройството, докато прокси често трябва да бъдат конфигурирани за всяко отделно приложение.

Друго предимство, което предлага VPN е по-голяма надеждност и по-малко откази.

4. Киберсигурността и изучаваните програмни езици

Както вече стана ясно във века на бързо развиващите се технологии киберсигурността се превръща в една от най-значимите области. Всяка година кибер атаките стават не само по-чести, но и по-усъвършенствани, използвайки различни методи и техники. Според статистика от 2023 г., 95% от всички кибератаки в световен мащаб са резултат на човешка грешка.

Човешката грешка може да се прояви в различни форми, като например недостатъчна обученост на потребителите, небрежност при обработка на лична информация или дори неправилно конфигурирани настройки на сигурността. Кликането върху фишинг линкове или преглеждането на вредни файлове, използването на слаби пароли и пренебрегването на важни мерки за сигурност като инсталиране на антивирусен софтуер, предразполагат хакерите за зловредни атаки.

Важно е да се отбележи, че киберсигурността е пряко свързана с програмирането. Затова е важен изборът на програмен език, както осведомеността на разработчиците за потенциалните заплахи и уязвимости, свързани с всеки от тях.

Фиг. №4

4.1. C#

Както всеки един програмен език - C# притежава своите предимства и недостатъци.

- Предимства:

- C# е част от платформата .NET, която предоставя CLR (Common Language Runtime). Този механизъм за управление на паметта и контрол на достъпа може да помогне за предотвратяване на някои типични проблеми в сигурността.

- .NET предоставя обширни библиотеки и инструменти, които помагат на разработчиците да създават сигурен код. Тези библиотеки включват криптографски алгоритми, защита от SQL инжекции и други средства за сигурност.

- C# в комбинация с ASP.NET предоставя мощни механизми за управление на идентичността и контрол на достъпа, които са ключови за защитата на уеб приложения.

- Тъй като C# е разработен от Microsoft, този факт поддържа постоянната актуализация и поддръжка на езика, както и защита срещу някои уязвимости.

- Недостатъци:

- Въпреки старанието на Microsoft да предостави средства за предотвратяване на буферни препълвания, те все още могат да възникнат, особено при неконтролирано управление на паметта.

- C# и .NET са тясно свързани с платформата на Microsoft, което може да доведе до ограничения в портативността на приложенията, ако се изисква работа на различни операционни системи.

- Злоупотребата на C# за създаване на зловреден софтуер или експлоатация на сигурността не е невъзможна, и в ръцете на хакери този език може да се използва за нежелани цели.

4.2. SQL

Използването на SQL (Structured Query Language) за управление на бази данни също има своите предимства и недостатъци:

- Предимства:

- SQL е широко приет стандарт за управление на релационни бази данни, което улеснява съвместимостта и обучението на персонала.

- SQL предлага механизми за управление на достъпа и правата, които потребителите имат върху базата данни. Това позволява ограничаването на достъпа до чувствителна информация.

- SQL базите данни предлагат транзакционни механизми и ACID свойства (Atomicity, Consistency, Isolation, Durability), които осигуряват надеждност и цялост на данните.

- SQL предоставя възможност за деклариране на външни ключове, което подпомага цялостността на данните и предотвратява некоректни операции.

- SQL позволява оптимизация на заявките чрез използване на индекси, което подобрява ефективността на базата данни.

- Недостатъци:

- Един от най-честите видове кибератаки към бази данни е SQL инжекция, където зловреден SQL код се внедрява във входните полета, което може да доведе до компрометиране на информация.

- Някои атаки могат да насочат DoS атаки към SQL базите данни, което може да причини сериозни проблеми в обработката на заявки и нарушаване на наличната функционалност.

- SQL базите данни изискват редовни актуализации и поддръжка, включително поправка на сигурностни проблеми и управление на конфигурацията.

- Неправилната конфигурация на SQL сървъра, като например слаба паролна политика или липса на шифроване на данни, може да засегне сигурността на системата.

4.3. JavaScript

➢ Предимства:

- JavaScript работи непосредствено в браузърите, което позволява динамични и интерактивни уеб страници.

- JavaScript е лек и бърз, което подобрява изпълнението на уеб страниците и потребителското преживяване.

➢ Недостатъци:

- Най-честият проблем със сигурността на JavaScript са XSS атаките, които включват внедряване на вреден код в уеб страница, който се изпълнява в браузъра на други потребители.

- Друг недостатък са атаки, при които потребителят е принуден да изпълни нежелана заявка, често свързана с използването на JavaScript.

4.4. PHP

➢ Предимства при използването на PHP в киберсигурността:

- PHP е език с прост синтаксис, който прави писането на код достъпно за голяма аудитория. Това улеснява разработката на уеб приложения и системи.

- Поради широкото разпространение и употреба, PHP разполага с голяма общност от разработчици. Този фактор улеснява обмена на знания и решаването на проблеми.

- Съществуват различни PHP фреймуърки (като Laravel и Symfony), които предоставят вградени мерки за сигурност и стандартизирани практики при разработка.

➢ Недостатъци при използването на PHP в киберсигурността:

- PHP е слабо типизиран език, което може да доведе до неочаквано поведение и уязвимости, ако програмистите не са внимателни с обработката на данни.

- При неправилно обработени авторизационни механизми и контрол на достъп, могат да възникнат проблеми като IDOR (Insecure Direct Object References), които засягат сигурността на приложението.

- Несигурно обработени входни данни може да доведат до атаки като SQL инжекции, XSS (Cross-Site Scripting) и други видове атаки.

4.5. HTML и CSS

- Предимства на HTML и CSS в киберсигурността:

- HTML се използва за структуриране на съдържание, а CSS - за стилове. Това разделение на отговорностите прави кода по-четим, лесен за поддръжка и помага в предотвратяването на смесване на структурен и стилов код, което подобрява сигурността.

- HTML и CSS следват стандартите на уеб разработката и предоставят вградени механизми за сигурност като Content Security Policy (CSP), които могат да се използват за ограничаване на източниците на съдържание и предотвратяване на XSS атаки.

- HTML и CSS се използват за представяне на информацията и стилове в браузъра, което означава, че те обикновено имат ограничени привилегии и не са свързани с операции с висок риск като изпълнение на код на сървъра.

- Недостатъци на HTML и CSS в киберсигурността:

- HTML и CSS не предоставят много средства за защита от различни видове атаки като CSRF (Cross-Site Request Forgery) или инжекции на код.

- Неправилната обработка на външни данни в HTML и CSS може да доведе до потенциални атаки. Например, с включването на външни стилове или скриптове може да бъде злоупотребено.

- Също така с HTML може бъде злоупотребено, като се използва за провеждане на XSS атаки, ако не се внимава при обработката на входни данни. Вградените механизми за сигурност като CSP трябва да бъдат правилно конфигурирани, за да предотвратят този вид атаки.

5. GDRP (General Data Protection Regulation) - същност и предназначение на проекта

5.1. Същност на GDPR

GDPR или General Data Protection Regulation е общ регламент за защита. Изготвен от ЕС, той цели да укрепва правата на лицата, живеещи в страните-членки на ЕС, и да хармонизира законите за защита на правата и личните данни във всички страни, като ги прави еднакви. Цели да се постигне по-голяма “прозрачност” за хората относно събирането на данни от организациите за тях и за това, за какво ги използват, както и да се даде възможност на човека да предотврати ненужното събиране на данни.

Фиг. №5

5.2. Предназначение на проекта

Каква е целта на GDPR, или какво е наложило неговото приемане?

Отговорът на този въпрос се съдържа още в първите редове на Регламент (ЕС) 2016/679:

„Настоящият регламент има за цел да допринесе за изграждането на пространство на свобода, сигурност и правосъдие и на икономически съюз, за постигането на икономически и социален напредък, за укрепването и сближаването на икономиките в рамките на вътрешния пазар, както и за благосъстоянието на хората.“

Това е крайната „заветна“ цел на Европейския съюз, а в частност и на GDPR. Тя трябва да бъде подплатена, гарантирана с и в съответствие с принципите, правилата и ПРАВОТО на защита на личните данни на физическите лица, намиращи се на територията на ЕС.

Причините за поставянето на тези цели – да се гарантират сигурността и защитата на личните данни на физическите лица. Просперитетът на технологиите и икономиката са създали нови предизвикателства пред сигурността на личните данни на физическите лица, като едновременно трябва да се гарантират и всички права и свободи на човека. Именно тук се намесва GDPR. Общият Регламент за защитата на данните въвежда изисквания, касаещи потока на лични данни в публичния и частния сектор. „Той“ няма за цел да преустанови или забрани обмена и събирането на лични данни, а да го регламентира и канализира по начин, който да гарантира сигурността на данните. Прилагайки необходимите процедури за защита, ще бъде по-лесно да се установи изтичането на лични данни и да се преустанови, или ограничи нерегламентираният достъп. Всеки достъп, трансфер или обработка следва да остави своята следа.

ТРЕТИ РАЗДЕЛ - ЗАКЛЮЧЕНИЕ

В заключение, можем да констатираме, че бързото развитие на технологиите води до значителен напредък, но същевременно създава и по-сложни предизвикателства в областта на киберсигурността. С ускорените темпове на технологичните иновации, уязвимостите в сигурността са по-изразени, изисквайки постоянно внимание и ресурси за защита на личната и конфиденциална информация.

Важно е да осъзнаем, че политиките и правилата за защита в уеб пространството не могат да бъдат статични, а трябва редовно да се преразглеждат и актуализират, за да отговорят на новите заплахи в онлайн средата. Въпреки стремежа към увеличаване на устойчивостта на мрежата, трябва да приемем факта, че абсолютна защита е недостижима, поради човешките грешки, бъговете в софтуера и хардуерните дефекти.

Специалистите по киберсигурност имат ключова роля в повишаването на сигурността, но е съществено и потребителите да поемат отговорност. Поддържането на постоянно внимание и активно участие в киберсигурността на лично ниво са от съществено значение, за да гарантираме, че нашите системи са защитени и сигурни срещу различни видове заплахи от страна на злонамерени хакери.

Защото в свят, в който данните са всичко, защитата им е ключът към нашето бъдеще!

ИЗПОЛЗВАНА ЛИТЕРАТУРА

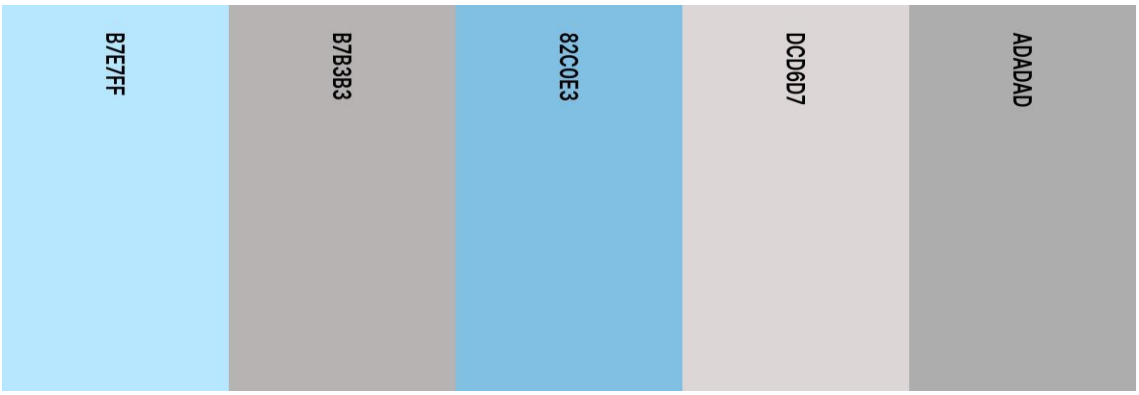
1. https://progressbg.net/blog/cybersecurity/kakvo-e-cybersecurity-i-zashto-e-vazhno/
2. https://www.ibm.com/topics/cybersecurity
3. https://www.ibm.com/blog/types-of-cyberthreats/
4. https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/
5. https://bg.if-koubou.com/articles/how-to/whats-the-difference-between-a-vpn-and-a-proxy.html

Приложения

Приложение №1

1. Избор на цветова гама

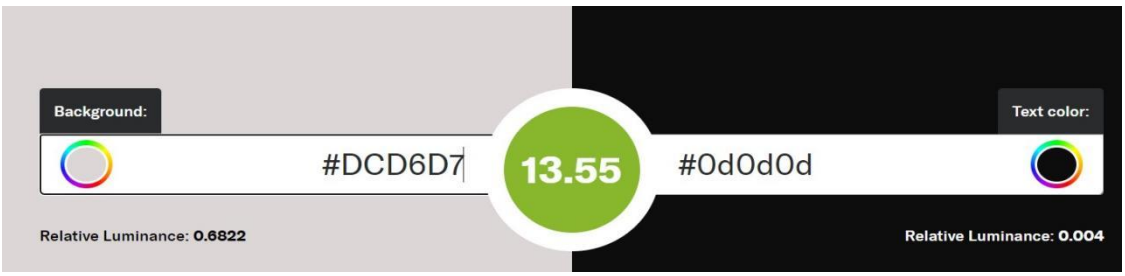
Изборът на цветова гама за сайт на тема „Защита в уеб пространството и киберсигурност в условията на глобалната икономика“ направих от Coolors - The super fast color palettes generator!. Ето подборът на цветове за уеб страниците ми:



2. Измерване и изчисляване на контрастно съотношение

Измерването и изчисляването на контрастното съотношение между два съседни цвята, извърших като използвах калкулатора от https://contrast-ratio.com/ . Резултатът от измерването на цветовете за моят сайт на тема „Защита в уеб пространството и киберсигурност в условията на глобалната икономика“ е следният:

Контраст на голям текст измерен в страницата index.html

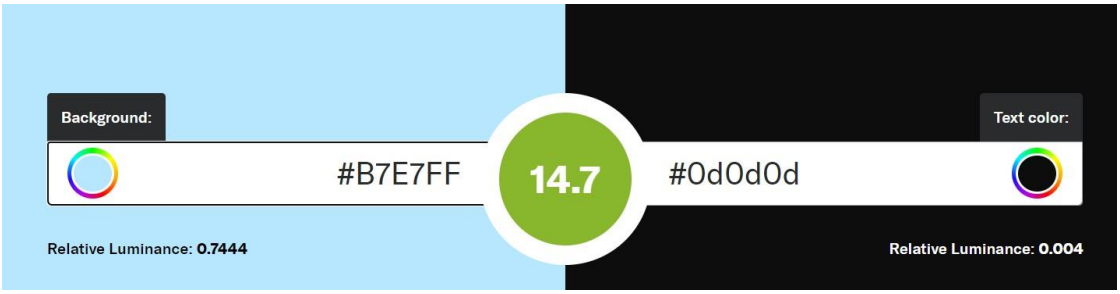


Извод: Измереният контраст на голям текст в *header* на страницата index.html е 13.55, при норма 3, зададена от W3C, констатирам / или ясно се вижда/ ,че отговаря на изискванията.

Контраст на малък текст измерен в страницата index.html

Извод: Измереният контраст на малък текст в *main* на страницата index.html е 13.55, при норма 4,5, зададена от W3C, констатирам / или ясно се вижда /,че отговаря на изискванията.

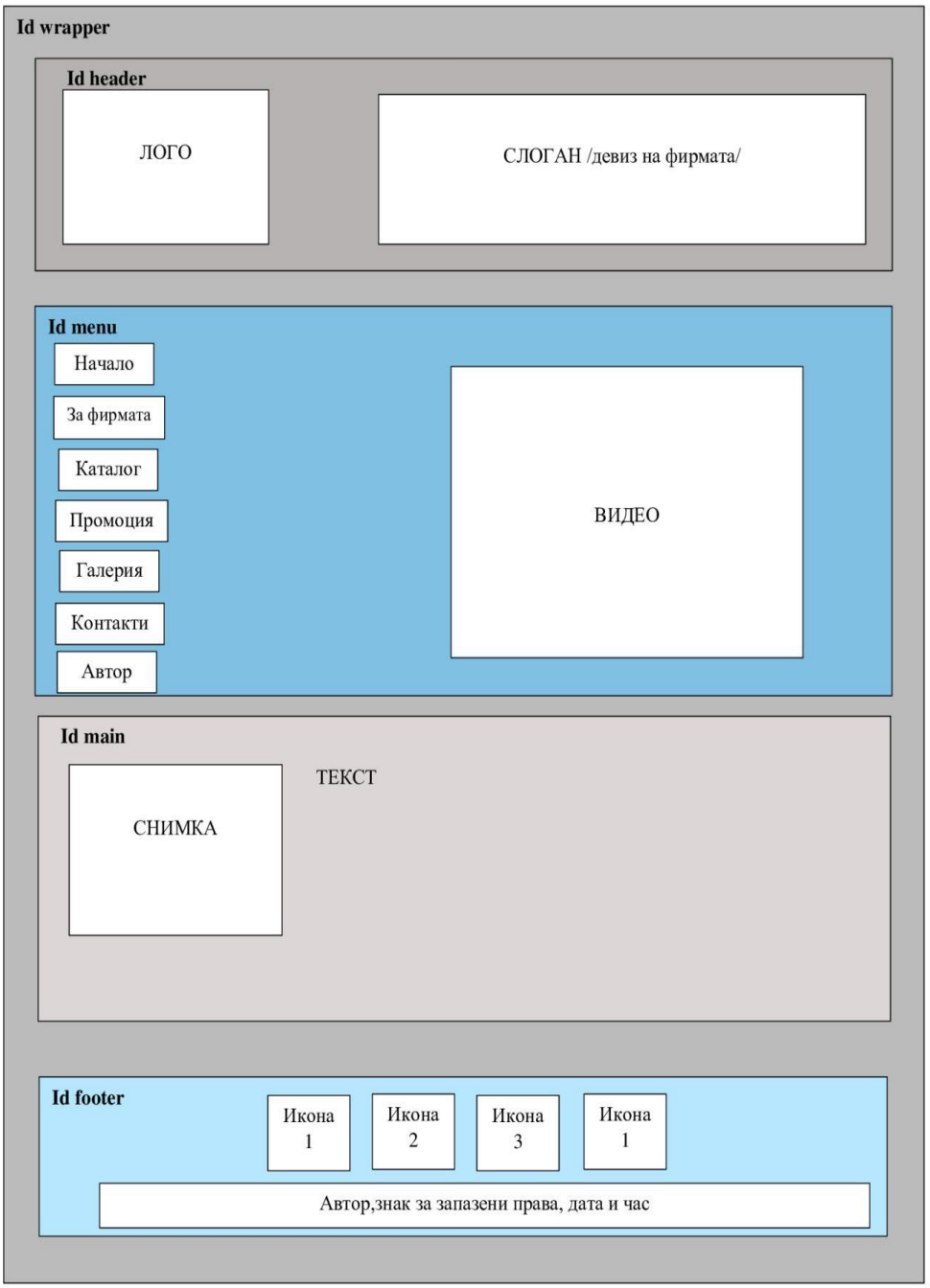
Извод: Измереният контраст на малък текст в *aside, section* на страницата index.html е 9.8, при норма 4,5, зададена от W3C, констатирам / или ясно се вижда /,че отговаря на изискванията.



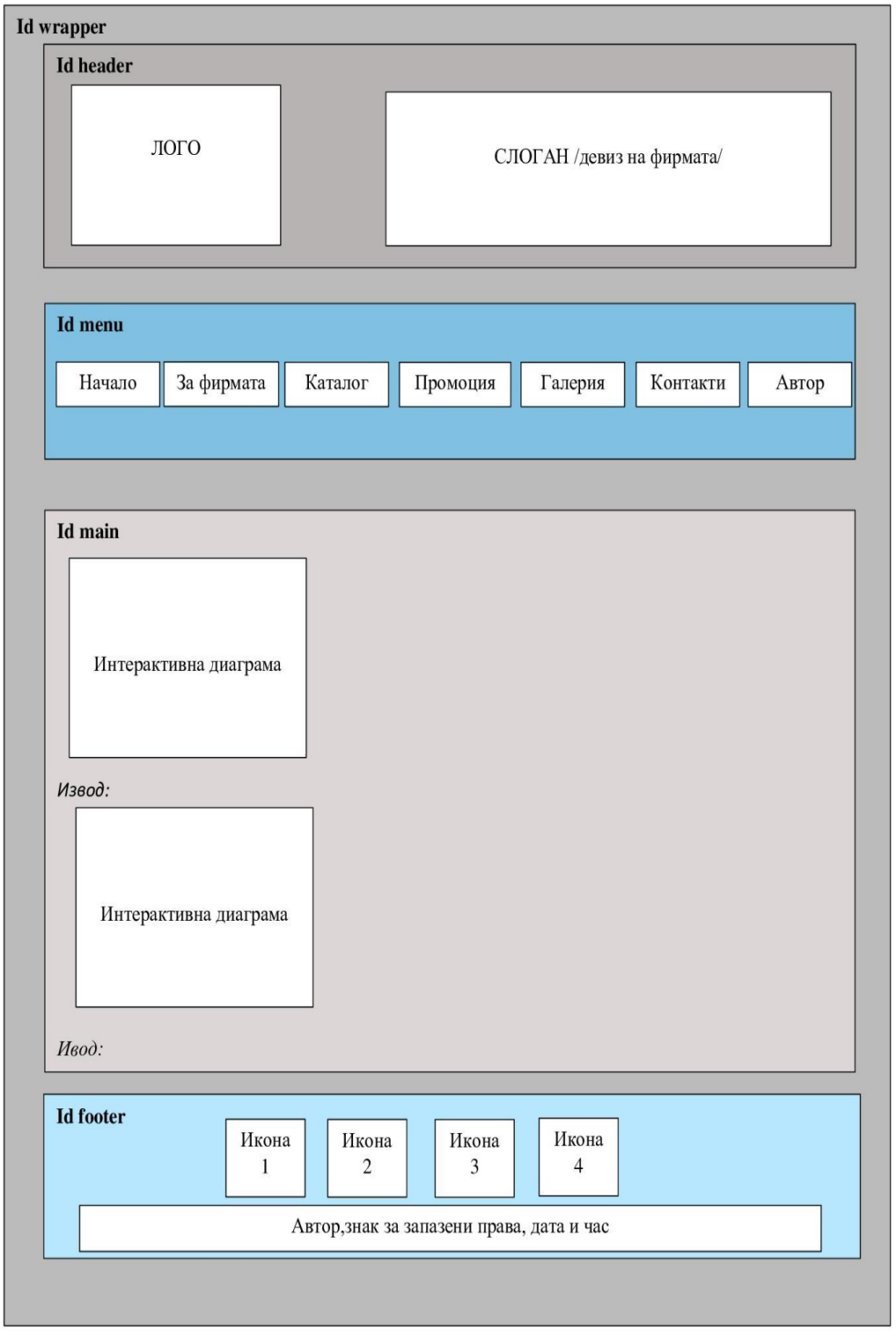
Извод: Измереният контраст на малък текст в *footer* на страницата index.html е 14.7, при норма 4,5, зададена от W3C, констатирам / или ясно се вижда /,че отговаря на изискванията.

3. Макети за структурата на уеб страниците

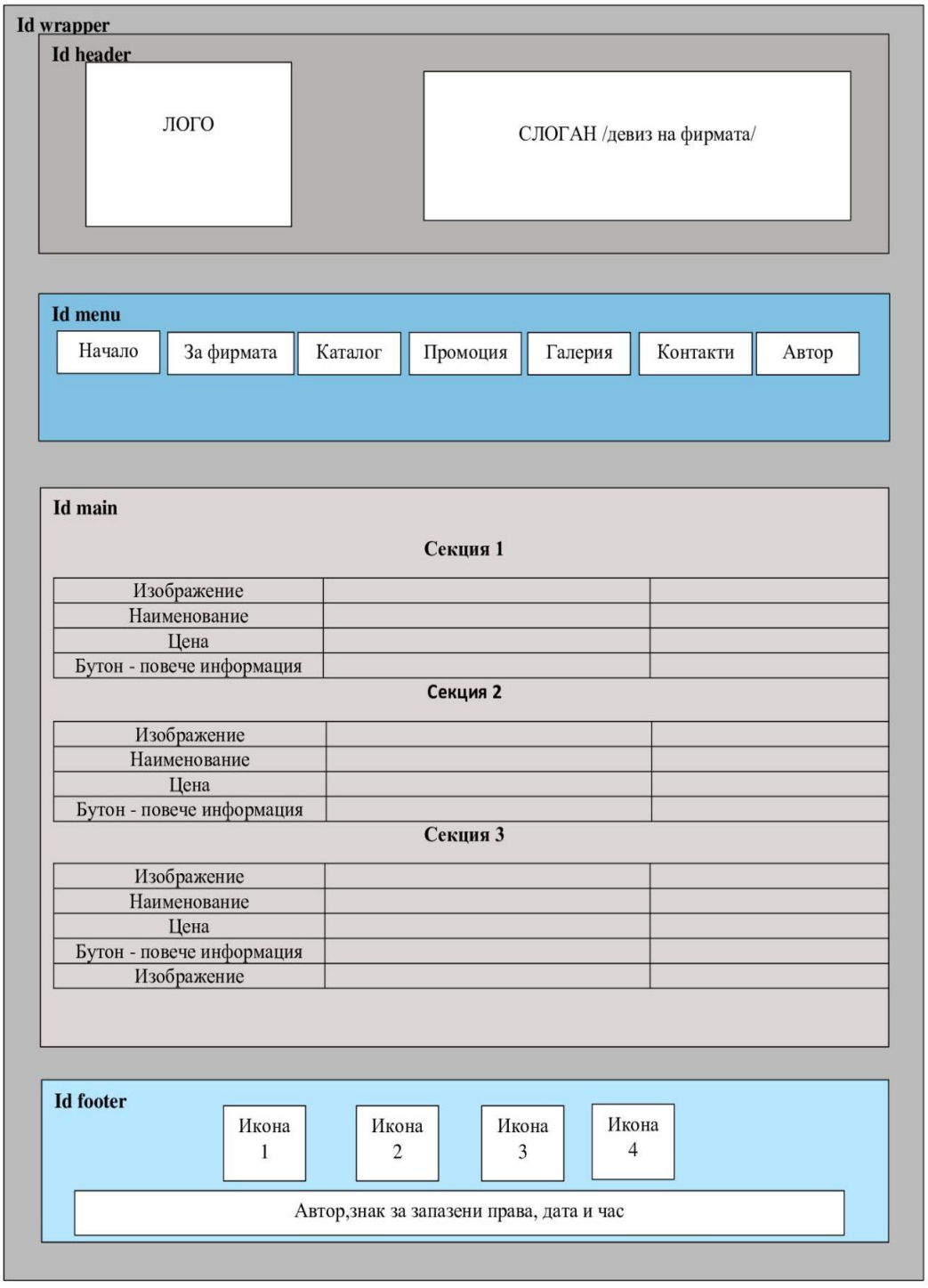
Index.html



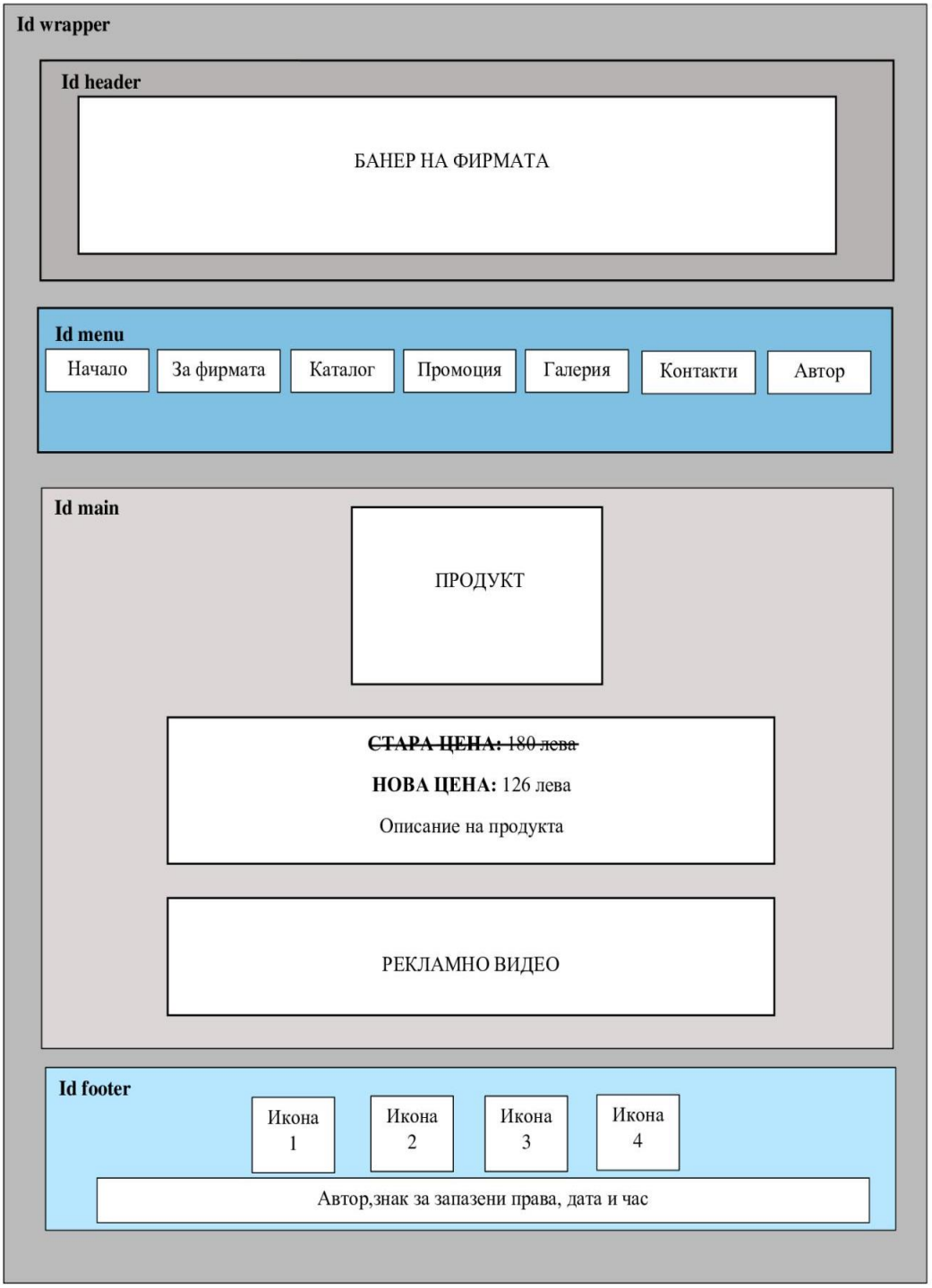
Za firmata.html



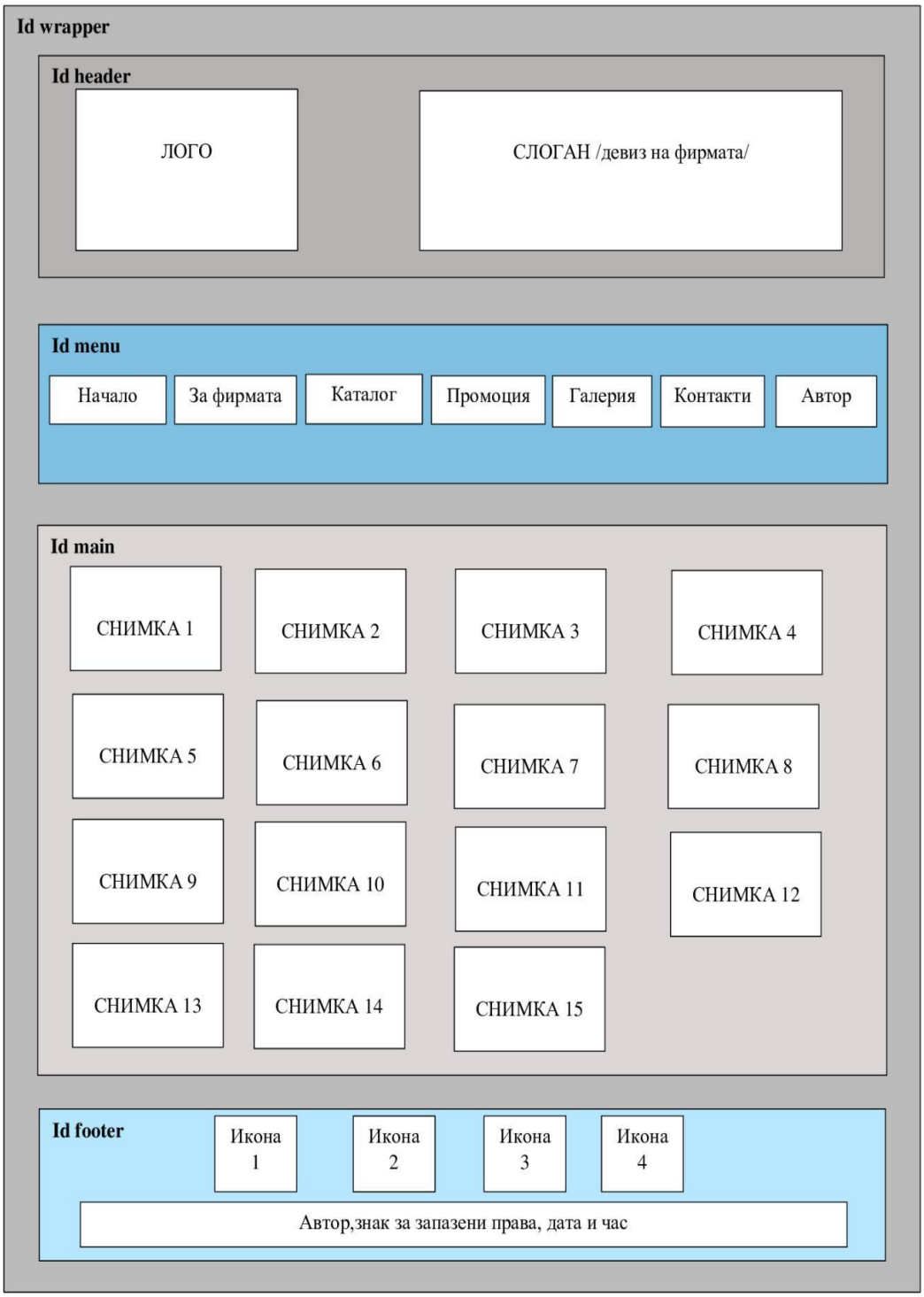
Katalog.html



Promociq.html

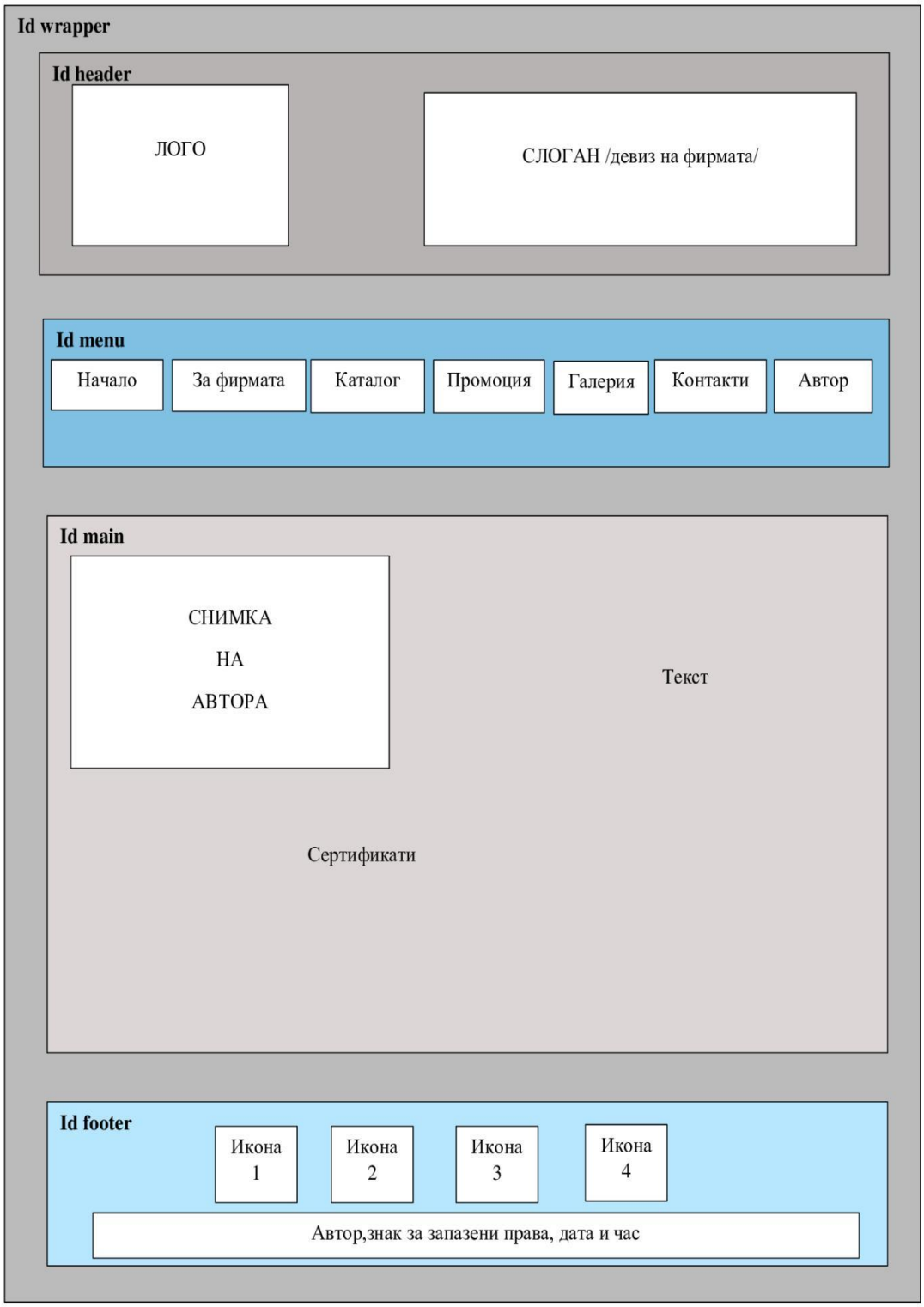


Galeriq.html



Kontakti.html

Avtor.html


Id wrapper
Id header
ЛОГО
СЛОГАН /девиз на фирмата/
Id menu
Начало
За фирмата
Каталог
Промоция
Галерия
Контакти
Автор
Id main
СНИМКА
НА
АВТОРА
Текст
Сертификати
Id footer
Икона 1
Икона 2
Икона 3
Икона 4
Автор,знак за запазени права, дата и час

Приложение №2

/Код на страница avtor.html/

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

 <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">

<title>Автор</title>

<link rel="icon" type="image/x-icon" href="../img d/favicon.ico"/>

<link rel="icon" type="image/x-icon" href="img/favicon.ico">

<meta name="viewport" content="width=device-width, initial-scale=1">

  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet">

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js"></script>


<style type="text/css">

<!--

#wrapper {

	font-family: "Times New Roman", Times, serif;

	color: #000066;

	background-color: #ADADAD;

	height: auto;

	width: 960px;

	margin-right: auto;

	margin-left: auto;

}

#wrapper #header {

	font-family: "Times New Roman", Times, serif;

	color: #000000;

	background-color: #BBBAC6;

	height: auto;

	width: 960px;

	margin-right: auto;

	margin-left: auto;

}

#wrapper #menu {

	font-family: "Times New Roman", Times, serif;

	color: #000000;

	background-color: #82C0E3;

	height: auto;

	width: 960px;

	margin-right: auto;

	margin-left: auto;

}

#wrapper #main {

	font-family: "Times New Roman", Times, serif;

	color: #000000;

	background-color: #E2E2E2;

	height: auto;

	width: 960px;

	margin-right: auto;

	margin-left: auto;

}

#wrapper #footer {

	font-family: "Times New Roman", Times, serif;

	color: #FFFFFF;

	background-color:  #B7E7FF;
```

```
            height: auto;
            width: 960px;
            margin-right: auto;
            margin-left: auto;
}

-->
ul {
            position: absolute;
            top: 1318px;
            left: 802px;
            transform: translate(-50%, -50%);
            margin: 0;
            padding: 0;
            display: flex;
   }

   ul li {
     list-style: none;
   }

   ul li a {
            display: block;
            position: relative;
            width: 50px;
            height: 50px;
            line-height: 100px;
            font-size: 40px;
            text-align: center;
            text-decoration: none;
            color: #404040;
            margin: 0 30px;
            transition: 0.5s;
   }

ul li a span {
  position: absolute;
  transition: transform 0.5s;
}

ul li a span:nth-child(1),
ul li a span:nth-child(3) {
  width: 100%;
  height: 3px;
  background: #404040;
}

ul li a span:nth-child(1) {
  top: 0;
  left: 0;
  transform-origin: right;
}

ul li a:hover span:nth-child(1) {
  transform: scaleX(0);
  transform-origin: left;
  transition: transform 0.5s;
}

ul li a span:nth-child(3) {
  bottom: 0;
  left: 0;
  transform-origin: left;
}

ul li a:hover span:nth-child(3) {
  transform: scaleX(0);
  transform-origin: right;
  transition: transform 0.5s;
}
```

```
ul li a span:nth-child(2),
ul li a span:nth-child(4) {
  width: 3px;
  height: 100%;
  background: #404040;
}

ul li a span:nth-child(2) {
  top: 0;
  left: 0;
  transform: scale(0);
  transform-origin: bottom;
}

ul li a:hover span:nth-child(2) {
  transform: scale(1);
  transform-origin: top;
  transition: transform 0.5s;
}

ul li a span:nth-child(4) {
  top: 0;
  right: 0;
  transform: scale(0);
  transform-origin: top;
}

ul li a:hover span:nth-child(4) {
  transform: scale(1);
  transform-origin: bottom;
  transition: transform 0.5s;
}

.facebook:hover {
  color: #3b5998;
}

.facebook:hover span {
  background: #3b5998;
}

.twitter:hover {
  color: #1da1f2;
}

.twitter:hover span {
  background: #1da1f2;
}

.instagram:hover {
  color: #c32aa3;
}

.instagram:hover span {
  background: #c32aa3;
}

.google:hover {
  color: #dd4b39;
}

.google:hover span {
  background: #dd4b39;
}

ul li a .twitter {
  color: #1da1f2;
}
```

```
   ul li a:hover:nth-child(3) {
     color: #c32aa3;
   }

   ul li a:hover:nth-child(4) {
     color: #dd4b39;
   }
</style>

<style type="text/css">
<!--

body {
        background-image: url(img/giphy.gif);
        background-repeat: repeat;
}
#apDiv1 {
        position:absolute;
        left:88px;
        top:393px;
        width:240px;
        height:235px;
        z-index:1;
}
#apDiv2 {
        position:absolute;
        left:84px;
        top:481px;
        width:254px;
        height:204px;
        z-index:1;
}
a:link {
        text-decoration: none;
        color: #000000;
}
a:visited {
        text-decoration: none;
        color: #000000;
}
a:hover {
        text-decoration: none;
        color: #660099;
}
a:active {
        text-decoration: none;
        color: #000000;
}
.style7 {font-size: 22px; }
.style8 {font-size: 20px; }
#apDiv3 {
        position:absolute;
        left:297px;
        top:751px;
        width:505px;
        height:272px;
        z-index:1;
}

#wrapper #menu {
        font-family: "Times New Roman", Times,
serif;
        font-size: 20px;
        font-style: italic;
        color: #000000;
        float: left;
        width: 100%;
}
#wrapper #menu p {
        font-family: "Times New Roman", Times,
serif;
```

```
            font-size: 22px;
            text-align: center;
}
#wrapper #menu #navigation {
  display: flex;
  justify-content: center;
}

#wrapper #menu a.button4 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}
#wrapper #menu #navigation a.button2 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button3:hover {
  background: linear-gradient(to right,
#493240,#c31432);
  color: #FFFFFF;
}
#wrapper #menu #navigation a.button4:hover {
  background: linear-gradient(to right, #c31432,
#f5af19);
  color: #FFFFFF;
}
#wrapper #menu #navigation a.button3 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button2:hover {
  background: linear-gradient(to right, #ff0099,
#493240);
  color: #FFFFFF;
}
#wrapper #menu #navigation a.button1 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button1:hover {
  background: linear-gradient(to right, #12c2e9,
#c471ed, #f64f59);
  color: #FFFFFF;
}
```

```
#wrapper #menu #navigation a.button5 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button5:hover {
  background: linear-gradient(to right,#f5af19 , #e94057,#8a2387);
  color: #FFFFFF;
}
#wrapper #menu #navigation a.button6 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button6:hover {
  background: linear-gradient(to right,#8a2387 , #ed213a);
  color: #FFFFFF;
}
#wrapper #menu #navigation a.button7 {
  display: inline-block;
  padding: 8px 15px;
    margin: 5px;
  background-color: #414041;
  border-radius: 5px;
  text-decoration: none;
  color:#FFFFFF;
  transition: background-color 0.3s ease;
}

#wrapper #menu #navigation a.button7:hover {
  background: linear-gradient(to right,#8a2387 , #ed213a);
  color: #FFFFFF;
}
#wrapper #main .style8 img {
        margin: 5px;
        padding: 5px;
        float: left;

}

.style12 {font-size: 24px}
.style15 {font-size: 16px}
.style16 {
        color: #000000;
        font-weight: bold;
}
.style17 {color: #000000}
.style18 {font-size: 36px}
.style20 {
        color: #B7E7FF
}
.style21 {
        font-size: 14px
}
```

```
.style22 {font-size: 16px; font-style: italic; }

.style23 {font-size: 16px; font-weight: bold; }

.style25 {color: #BBBAC6}

-->


</style>

</head>



<body>

<div id="wrapper">

 <p><a name="ddd" id="ddd"></a></p>

 <div id="header">

  <table width="962" border="0">

   <tr>

    <th width="337" scope="col"><p><span class="style25">dfhf</span></p>

     <p><span class="style25"> bfhh</span><img src="img/logo.jpg" alt="Описание на изображението" width="216" height="186" style="border-radius: 10px; overflow: hidden;" /></p>

    </th>

    <th width="615" scope="col"><p align="center" class="style1"> </p>

      <p align="center" class="style1 style18">&quot;SecureSquad&quot; ООД</p>

     <p align="center" class="style3 style12">Защитаваме кода - защитаваме Вас!</p>

    </th>

   </tr>

  </table>

 </div>

 <div id="menu">

  <div id="navigation">

   <p class="style7"><a href="index.html" class="button1 style8">НАЧАЛО</a></p>

<p class="style7"><a href="za firmata.html" class="button2 style8">ЗА ФИРМАТА</a></p>

<p class="style7"><a href="katalog.html" class="button3 style8">КАТАЛОГ</a></p>

<p class="style7"><a href="promociq.html" class="button4 style8">ПРОМОЦИЯ</a></p>

<p class="style7"><a href="galeriq.html" class="button5 style8">ГАЛЕРИЯ</a></p>

<p class="style7"><a href="kontakti.html" class="button6 style8">КОНТАКТИ</a></p>

<p class="style7"><a href="avtor.html" class="button7 style8">АВТОР</a></p>

  </div>

 </div>

 <div id="main">

  <p class="style8"></a><img src="img/me.jpg" width="307" height="400" /></p>

  <p align="justify" class="style15">Казвам се Гергана Синдонас и съм ученичка в 12 клас от „Професионална гимназия по икономика и мениджмънт&quot; - гр. Пазарджик. Страстта ми към компютрите ме накара да избера паралелката, в която уча - &quot;икономическа информатика&quot;.</p>

  <p align="justify" class="style15">От малка обичам да прекарвам времето си пред компютър и смятам, че да &quot;работя&quot; с кодове е моето нещо. Това беше и причината да продължа обучението си и чрез курсове в SoftUni по киберсигурност - за да придобия технически и практически умения, необходими за бъдещата ми реализация. Следващата стъпка в плана ми за професионално развитие след 12 клас е кандидатстването ми в „Технически университет" - гр. София, с киберсигурност. Мечтая да работя като penetration tester за Национална сигурност.</p>

  <p align="justify" class="style15">Осъзнавам, че пътят към целта ми не е лесен, но съм готова да вложа необходимите време и усилия, за да я постигна!</p>

  <p align="justify" class="style22">Вярвам, че няма нещо, с което да не мога да се справя.</p>

  <p align="justify" class="style23">Трудни за изпълнение задачи - има, но непосилни - няма!</p>

  </p>

  <p align="center" class="style15"> </p>

  <p align="center" class="style15"> </p>

  <table width="960" height="187" border="0">
```

```
    <tr>

     <th width="250" scope="col"><div
class="container mt-3">

<div class="card" style="width:250px">

   <div align="center"><img class="card-img-top"
src="img/sertifikat1.jpg" alt="Card image"
style="width:50%" /></div>

   <div class="card-body">

    <h4 class="card-title">Сертификат</h4>

    <p class="card-text style21">Cyber security and
Ethical Hacking</p>

    <a href="img/sertifikat1.jpg" class="btn btn-
primary">Виж сертификата</a>

   </div>

  </div>

  </th>

     <th width="250" scope="col"><div
class="container mt-3">


  <div class="card" style="width:250px">

   <div align="center"><img class="card-img-top"
src="img/sertifikat2.jpg" alt="Card image"
style="width:50%">

   </div>

   <div class="card-body">

    <h4 class="card-title">Сертификат</h4>

    <p class="card-text">Introduction to Cyber
Security</p>

    <a href="img/sertifikat2.jpg" class="btn btn-
primary">Виж сертификата</a>

   </div>

  </div></th>

     <th width="441" scope="col"><div
class="container mt-3">


  <div class="card" style="width:250px">

   <div align="center"><img class="card-img-top"
src="img/sertifikat3.jpg" alt="Card image"
style="width:50%">

   </div>

   <div class="card-body">

    <h4 class="card-title">Сертификат</h4>

    <p class="card-text">Reconnaissance
Fundamentals</p>

    <a href="img/sertifikat3.jpg" class="btn btn-
primary">Виж сертификата</a>

   </div>

  </div></th>

     <th width="10" scope="col"> </th>

    </tr>

   </table>

   <p align="center" class="style15"> </p>

   <p align="center" class="style15"><a
href="#ddd"><u>КЪМ НАЧАЛОТО </u></a></p>

   <p class="style7"> </p>

  </div>

  <div id="footer">

   <p align="center" class="style20">,

   <p align="center" class="style20">,


   <p align="center">


   <ul>

  <li>

   <a class="facebook"
href="https://www.facebook.com/">

    <span></span>

    <span></span>

    <span></span>

    <span></span>

    <i class="fa fa-facebook" aria-
hidden="true"></i>   </a>  </li>

  <li>

   <a class="twitter"
href="https://twitter.com/?lang=bg">

    <span></span>

    <span></span>

    <span></span>
```

```
    <span></span>
    <i class="fa fa-twitter" aria-hidden="true"></i>
   </a>
  </li>
  <li>
   <a class="instagram"
href="https://www.instagram.com/">
    <span></span>
    <span></span>
    <span></span>
    <span></span>
    <i class="fa fa-instagram" aria-
hidden="true"></i>
   </a>
  </li>
  <li>
   <a class="google"
href="https://www.google.com/?hl=bg">
    <span></span>
    <span></span>
    <span></span>
    <span></span>
    <i class="fa fa-google-plus" aria-
hidden="true"></i>
   </a>
  </li>
</ul></p>
   <p align="center"><span
class="style17">Автор</span><span
class="style16">: Гергана Синдонас </span><span
class="style17">/ &copy; Всички права запазени /
Wednesday, January 21, 2024 7:16 PM</span></p>
  </div>
  <p> </p>
</div>
</body>
</html>
```