**Земеделска професионална гимназия „Климент Аркадиевич Тимирязев“**



ДИПЛОМЕН ПРОЕКТ

За придобиване на трета степен на професионална квалификация - част от теория на професията

**НА ТЕМА: КИБЕРСИГУРНОСТ. КАК ДА ЗАЩИТИМ УСТРОЙСТВАТА.**

Изготвил: Ръководител-консултант:

Ученик от клас г-жа Красимира Пановска

Димитър Василев Дуев

Професия с код 482010 - ”Икономист-информатик”

Специалност с код 4820101 - ”Икономическа информатика”

гр. Сандански

2022 година

Съдържание

[Увод 3](#_Toc100559220)

[I. Киберпрестъпления 4](#_Toc100559221)

[1. Известни кибератаки и последствията от тях 5](#_Toc100559222)

[1.1. WannaCry 5](#_Toc100559223)

[1.2.Bad Rabbit 5](#_Toc100559224)

[1.3. Stuxnet: Супероръжието 6](#_Toc100559225)

[1.4. Dark Hotel: Шпиони в хотела 6](#_Toc100559226)

[2. Известни киберпрестъпници 6](#_Toc100559227)

[Дмитрий Голубьов 6](#_Toc100559228)

[Роман Вега 7](#_Toc100559229)

[Максим Ковалчук или Blade 8](#_Toc100559230)

[Ренукант Субраманиам или JiLsi 8](#_Toc100559231)

[RedBrigade 9](#_Toc100559232)

[Никълъс Джоел или Dron 9](#_Toc100559233)

[Хаким Б. или Lord Kaisersose 9](#_Toc100559234)

[Кийт Мъларски и Билял Шен 9](#_Toc100559235)

[Cha0 9](#_Toc100559236)

[Мерт Ортач или SLayraCkEr 9](#_Toc100559237)

[Адеуале Тейуо или Freddybb 10](#_Toc100559238)

[Детектив сержант Крис Доусън 10](#_Toc100559239)

[Детлеф Хартман или Matrix001 11](#_Toc100559240)

[Макс Вижън или Макс Бътлър или Iceman 11](#_Toc100559241)

[Lord Cyric 12](#_Toc100559242)

[3. Тъмен и дълбок интернет 12](#_Toc100559243)

[3.1. Нива и Поднива на Дълбокият Интернет 12](#_Toc100559244)

[3.1.1. Първо Ниво 12](#_Toc100559245)

[3.1.2. Второ Ниво 12](#_Toc100559246)

[3.1.3. Трето Ниво 12](#_Toc100559247)

[3.1.4. Четвърто Ниво 13](#_Toc100559248)

[3.1.5. Пето Ниво 13](#_Toc100559249)

[3.2. Тъмен Интернет 13](#_Toc100559250)

[3.2.1. Същност и характеристики на тъмен интернет 13](#_Toc100559251)

[4. Най-често срещани видове атаки 14](#_Toc100559252)

[II. Киберсигурност 17](#_Toc100559253)

[1. Какво е киберсигурност 17](#_Toc100559254)

[1.1. Киберсигурността в България 18](#_Toc100559255)

[1.2. Киберсигурността в САЩ 19](#_Toc100559256)

[2. Основни типове компютърни атаки 20](#_Toc100559257)

[3. Ролята на социалните мрежи в киберсигурността 21](#_Toc100559258)

[4. Техники за киберсигурност 22](#_Toc100559259)

[4.1. Контрол на достъпа и сигурност на паролата 22](#_Toc100559260)

[4.2. Удостоверяване на автентичността на данните 22](#_Toc100559261)

[4.3. Скенери за злонамерен софтуер 23](#_Toc100559262)

[4.3.1. Malware 23](#_Toc100559263)

[4.3.2. Ransomware 24](#_Toc100559264)

[4.3.3. Как се разпространяват malware и ransomware? 24](#_Toc100559265)

[4.4. Защитни стени 25](#_Toc100559266)

[4.5. Антивирусен софтуер 25](#_Toc100559267)

[4.6. Троянски кон 26](#_Toc100559268)

[5. Кибер етика 27](#_Toc100559269)

[6. Структура и управлиние на общественана и фирмена сигурност. 28](#_Toc100559270)

[7. Тенденции, променящи киберсигурността 30](#_Toc100559271)

[7.1. Уеб сървъри 30](#_Toc100559272)

[7.2. VPN 31](#_Toc100559273)

[7.3. Облачни изчисление и техните услуги 31](#_Toc100559274)

[7.4. АРТ и целеви атаки 32](#_Toc100559275)

[7.5. Мобилни мрежи 32](#_Toc100559276)

[7.6. IPv6: Нов интернет протокол 32](#_Toc100559277)

[7.7. IPv4 32](#_Toc100559278)

[7.8. Криптиране на кода 33](#_Toc100559279)

[8. Методи за предотвратяване на кибератака 33](#_Toc100559280)

[Заключение 34](#_Toc100559281)

[Източници: 35](#_Toc100559282)

# Увод

Днес човек е в състояние да изпраща и получава всякаква форма на данни, може да бъде електронна поща или аудио, или видео само с едно натискане на бутон, но дали някога е мислил колко сигурно се предават или изпращат данните му на друго лице безопасно, без изтичане на информация? Отговорът се крие в киберсигурността. Днес интернет е най-бързо развиващата се инфраструктура в ежедневието. В днешната техническа среда много от най-новите технологии променят облика на човека. Но поради тези нововъзникващи технологии ние не сме в състояние да защитим личната си информация по много ефективен начин и затова в наши дни киберпрестъпленията се увеличават с всеки изминал ден. Днес повече от 60 % от всички търговски сделки се извършват онлайн, така че тази област изисква високо качество на сигурността за прозрачни и най-добри сделки. Затова киберсигурността се превърна в актуален въпрос. Обхватът на киберсигурността не се ограничава само до защита на информацията в ИТ индустрията, но и до различни други области като киберпространството и т.н.

Дори най-новите технологии като изчислителни облаци, мобилни компютри, електронна търговия, мрежово банкиране и др. също се нуждаят от високо ниво на сигурност. Тъй като тези технологии съхраняват важна информация за дадено лице, тяхната сигурност е задължителна. Повишаването на киберсигурността и защитата на критичните информационни инфраструктури са от съществено значение за сигурността и икономическото благосъстояние на всяка държава. Повишаването на сигурността на интернет (и защитата на потребителите на интернет) се превърна в неразделна част от разработването на нови услуги, както и от правителствената политика. Борбата с киберпрестъпността се нуждае от всеобхватен и по-безопасен подход. Като се има предвид, че техническите мерки сами по себе си не могат да предотвратят нито едно престъпление, от решаващо значение е на правоприлагащите органи да бъде позволено да разследват и преследват ефективно киберпрестъпленията. Днес много държави и правителства налагат строги закони за кибернетичните ценни книжа, за да предотвратят загубата на част от важната информация. Всяко лице също трябва да бъде обучено на тази киберсигурност и да се предпази от тези нарастващи киберпрестъпления.

Целта на този дипломен проект ще се опитам да представя съвременните начини за киберпрестъпления и методите за защита от кибератаки. Също така и системите за защита на съвременните модели рутери.

## Киберпрестъпления

Киберпрестъпленията са термин за всяка незаконна дейност, която използва компютър като основно средство за извършване и кражба. Министерството на правосъдието на САЩ разширява определението за киберпрестъпление, като включва всяка незаконна дейност, която използва компютър за съхранение на доказателства. Разширяващият се списък на киберпрестъпленията включва престъпления, които са станали възможни благодарение на компютрите, като проникване в мрежата и разпространение на компютърни вируси, както и компютърни варианти на съществуващи престъпления, като кражба на самоличност, преследване, тормоз и тероризъм, които са се превърнали в основен проблем за хората и държавите. Обикновено на езика на обикновените хора киберпрестъпленията могат да се определят като престъпления, извършени с помощта на компютър и интернет, за да се подправи самоличността на дадено лице или да се продаде контрабанда, или да се преследват жертви, или да се нарушат операции със злонамерени програми.

### 1. Известни кибератаки и последствията от тях

### 1.1. WannaCry

WannaCry, който действаше в повече от 150 държави, се възползва от някои от изтеклите инструменти на американската служба за сигурност. През май криптовирусът атакува компании, използващи остарели версии на Windows софтуер, и блокира компютърните им системи. Хакерите зад WannaCry са искали паричен откуп, за да разблокират криптираните файлове. Повече от 300 000 компютърни системи са били засегнати в многобройни браншове, включително здравеопазване и автомобилни компании. От WannaCry е имало и човешки щети: във Великобритания болници с блокирани компютри са били принудени временно да прекратят дейност. Заразите с WannaCry са били толкова сериозни, че Microsoft предприел крайно необичайния ход да публикува patch-ове за Windows системи, за които вече са спрели ъпдейти.

### Bad Rabbit

Друга мащабна криптовирусна кампания, наречена Bad Rabbit, е извършила пробиви в компютри по цял свят като е имитирала инсталатор на Adobe Flash в новинарски и медийни уеб сайтове, до които хакерите са били получили достъп. След като криптовирусът заразява компютър, той сканира мрежата за споделени папки с често срещани названия и се опитва да открадне потребителска информация, за да достигне до други компютри.

### 1.3. Stuxnet: Супероръжието

Най-известната атака е сложният, многостранен, зловреден софтуер, който блокира центрофугите за обогатяване на уран в Иран, забавяйки ядрената програма на страната в продължение на няколко години. Червеят успява да се разпространи неусетно чрез USB флаш памети, прониквайки дори в компютри, които не са били свързани към интернет или локална мрежа. Атаката е излязла извън контрол и бързо се е разпространила по целия свят, заразявайки стотици хиляди компютри. Тя е създадена за много специфична задача. Червеят се проявява само на компютри, управлявани от програмируеми контролери и софтуер на Siemens. При проникване в такава машина той препрограмира тези контролери. След това, чрез намаляване на скоростта на въртене на центрофугите за обогатяване на уран, те фактически ги унищожават.

### 1.4. Dark Hotel: Шпиони в хотела

Не е тайна, че публичните Wi-Fi мрежи в кафенетата или летищата не са най-сигурните. Мнозина вярват, че в хотелите трябва да има по-добра защита. Такива погрешни схващания струват скъпо на различни топ мениджъри и високопоставени служители. При свързване към хотелска мрежа, те биват подканени да инсталират актуализация за популярна част от софтуера и веднага техните устройства се заразяват с шпионския софтуер на DarkHotel, който хакерите инсталират в мрежата няколко дни преди пристигането си, и премахват няколко дни след това. Скритият шпионски софтуер регистрира натискания на клавиши и позволява на киберпрестъпниците да извършват целенасочени фишинг атаки.

## 2. Известни киберпрестъпници

## Дмитрий Голубьов

След ареста му в Одеса хакерът Дмитрий Голубьов прекарва пет месеца и половина в затвора, през което време бе разпитван от американски служители на органите на реда, сред които и Грег Краб от Инспектората на пощенските служби на САЩ. Но благодарение на двама украински депутати той бе оправдан и освободен по всички обвинения от съда в Киев през 2009.

Висок около метър и осемдесет, с харизматични сини очи, Голубьов отрича всякаква връзка със Script, въпреки че във версията му за събитията има доста разминавания и дигиталните доказателства в ръцете на американските органи на реда разкриват съвсем различна история(включително и данните, открити на компютъра на Роман Вега, които говорят, че Script е Голубьов).

Script изчезва след освобождението си от затвора, но Голубьов се завърна с подновено желание за социални промени и начинания, като формира интернет партита на Украйна. Все още в Одеса, Голубъов излезе с политическа програма, която предвижда борба с корупцията , порнографията и търговията с наркотици в Мрежата.

Изненадващо изглежда, че въпреки яростните морални позиции на организацията свързани с престъпността, като например детската порнография, Голубьов организира кампания за освобождаването на прословутия кардър Maksik, излежаващ трийсет годишна присъда в турски затвор.

## Роман Вега

Роман Вега беше в затвора в Никозия през 2003. През юни 2004 по искане на САЩ бе прехвърлен в Калифорния и от тогава беше затворник, но не бе изправен пред съда. Докато пиша тези редове, той все още лежи във федерален затвор в Бруклин, мрачно заведение край залива Гоуанъс. През целия този период Вега нямаше никакви посетители, освен правните му защитници. През 2007 година бе насрочено изслушване пред съдията Чарлз Р. Брейър в Северния окръг на Калифорния. Прокуратурата и защитата бяха готови да се споразумеят за помилване, след което Вега щеше да бъде освободен – той бе излежал присъдата от 46 месеца и адвокатите приеха тези условия. Следобеда преди освобождаването му един прокурор от Източния окръг на Ню Йорк представи цял куп обвинения, като изиска Вега да бъде прехвърлен в Бруклин. Обвиненията по същество бяха идентични с предявените му в Калифорния. Прокуратурата в Ню Йорк обаче се позова на друг параграф, за да използва тези обвинения и да избегне дублиране на процеса.

От протокола от изслушването в съда ясно личи, че съдия Брейър, брат на члена на Върховния съд Стивън Брейър, бе смутен и ядосан от тактиката на Източния съдебен окръг на Ню Йорк. Новото обвинение се основаваше на информация, предоставена на от агенти на американската „Сикрит Сървис“.

След като закараха Вега в Бруклин, „Сикрит Сървис“ му предложи сделка: ако свидетелствата срещу Дмитрий Голубьов и други членове на украинския елит (не хакерския, а на висшите политици), те ще оттеглят обвиненията. Но ако откаже, ще повдигнат още обвинения в различни американски щати. Ще продължат, докато не се съгласи да сътрудничи.

Няма значение какво е направил или не е направил Вега, но той вече е прекарал три пъти по-дълго време в затвора от осъдените за аферата Shadowcrew, като над него тегнат още две нерешени дела. Вега страда от тежки проблеми със зъбите и изпитва постоянни болки от години, често пъти изобщо не може да се храни нормално. Въпреки това му беше отказана медицинска помощ от Бюрото на затворите и американската Шерифска служба. Така че не се очертава перспектива за скорошното освобождаване на Вега.

### Максим Ковалчук или Blade

Ковалчук беше арестуван приз май 2003 в Тайланд, и екстрадиран в САЩ. Където прекарва 4 години в затвора ФБР се съгласи на съдебно споразумение и той бе освободен в края на 2007 година, след което се върна към анонимността си в Украйна. Решението на ФБР контрастира рязко на тактиката „Сикрит Сървис“ за задържането на Роман Вега.

## Ренукант Субраманиам или JiLsi

На 27 февруари 2010 година той се признава за виновен по едно от обвиненията за измама с кредитни карти и по 4 обвинения с измами с ипотеки, за което съдията от Британския кралски съд в блекфрайърс го осъди на четири години затвор.

С намалена присъда за добро поведение се очаква той да излезе на свобода в края на юли 2012 година. Основната част от делото му не е свързана с DarkMarket, а с ипотечни измами. Обвинението се позова на пет такива случая (въпреки че три от тях бяха отхвърлени от финансовите институции). Макар че ипотечните измами сами по себе си са си престъпление, прокурорът предложи връзка между приходите на Субраманиам от DarkMarket и възможността да му плаща задълженията си по ипотеките. Субраманиам обаче твърди, че няма вина, защото е кандидатствал за ипотечни заеми от името на приятели, които не са имали право да го сторят лично. Освен това Субраманиам очаква да види какви ще са последствията от Закона за криминалните дела и дали ще трябва да връща още суми. Съгласно наложената му присъда, съобразена със законовите изисквания за предотвратяване на престъпления, той няма да има свободен достъп до компютри в течение на пет години след освобождаването му от затвора.

## RedBrigade

Той до голяма степен се поправи и понастоящем е в Европа.

## Никълъс Джоел или Dron

Джоел бе освободен от затвора, след като излежава присъдата си за измами с кредитни карти и незаконно производство на сканиращи устройства.

## Хаким Б. или Lord Kaisersose

Lord Kaisersose се намира в Марсилия и все още очаква процес, но е пуснат под гаранция. Франция е една от страните, където колелата на правосъдието се нуждае от малко смазване.

## Кийт Мъларски и Билял Шен

И двамата продължават да патрулират по основните артерии на киберпространството.

## Cha0

Cha0 или ръководи бизнеса си в Словения, или е в затвора в зависимост от това дали реалният Cha0 е Шахин, или пък Джагатай Евяпан. Вторият се намира в един от най-добре охраняваните затвори в Турция, в Текирдаг. Процесът му трябва да започне тази година, но обвинителят свали най-сериозните обвинения, свързани с организираната престъпност.

## Мерт Ортач или SLayraCkEr

Мерт лежеше в един истанбулски затвор по обвинения, свързани с делото за Акбанк, когато бе освободен поради технически причини през март 2010 година. Повторно бе арестуван през ноември 2010 г. и понастоящем все още е зад решетките. От всички, участвали в DarkMarket, Мерт е един от най-талантливите, макар и своеобразни и непредсказуеми персонажи.

## Адеуале Тейуо или Freddybb

На 1 януари 2009 г. Адеуале Тейуо бе осъден на четири години затвор от Кралския съд в Хъл за конспирация с цел измама между юни 2004 г. и февруари 2008 г. Той се призна за виновен през ноември 2008 г. по едно от обвиненията, по-точно, че е извършил измами на стойност под 600 000 паунда от банкови сметки по целия свят. Съдията препоръчва, след като излежи присъдата си, да бъде депортиран в Нигерия.

Поради намаляване срока на присъдата заради добро поведение, Тейуо трябваше да бъде освободен на 29 август 2010 г. Две седмици преди това той се появи в съда в град Гримзби, отвъд устието на Хъмбър, точно срещу Хъл. Това изслушване бе предизвикано от британския Закон за криминалните дела, една от малкото значими поправки на правителството на Тони Блеър в областта на наказателното право, според която държавата може да придобива имуществото от престъпниците. Краят се оказа фарс, макар и на едно сериозно дело. Прокурорът обърка ключова папка и това предизвика неочаквана реакция от страна на брадатия съдия Греъм Робинсън, чийто първоначално добронамерен хумор прерасна в сарказъм. Той обяви, че няма да пренасрочи изслушването, двете страни трябвало да стигнат незабавно до споразумение. Това постави Адеуале в много силна позиция. Съдията в крайна сметка прие, че става дума за малко над 53 000 паунда, извлечена от първоначалната преценка за щети, възлизащи на 353 067 паунда. Тейуо обяви, че няма да плати, което означаваше, че ще прекара още година в затвора. Така на 7 април 2011 г. той бе депортиран в Нигерия. Като една от най-интелигентните личности, огряла кардърските форуми, Тейуо почти успя да запази двойствения си живот като талантлив инженер-химик и киберпрестъпник.

## Детектив сержант Крис Доусън

Детектив сержант Крис Доусън работи по делото на Freddybb с изключителна прецизност, като посвети голяма част от времето си, за да направи бъркотията от числа, дати и технологични детайли разбираема за всеки лаик, преди делото да стигне до съда. Доусън твърди, че по време на консултациите при изслушването, наложително съгласно закона за криминалните дела, е чул Тейуо за казва: „Мамка им, няма да плащам.“ Когато съдията излезе от съдебната зала, детективът излетя навън бесен заради некадърността на английската съдебна система.

Доусън продължава да работи в Хъл като висш офицер, разследващ убийства.

## Детлеф Хартман или Matrix001

На 9 октомври 2007 г. Регионалният съд в Щутгарт постанови, че Хартман трябва да бъде съден по тринайсет обвинения за измами с кредитни карти. Но пак същият съд оповести, че обвинението, повдигнато срещу него за организиране на престъпна конспирация, е отхвърлено. След като най-сериозните обвинения отпаднаха, Хартман бе освободен от затвора „Щамхайм“, където бе прекарал предишните четири месеца. Причината, която попречи да бъде разследван по обвинение в конспирация, е в интерпретацията на съда на основния закон на Германия – нейната Конституция, която постановява, че ако лицето е член на дадена конспирация, то трябва да се чувства част от „обединена група“, в която се предполага „подчинение на индивида на волята на колектива“. Съдията твърдеше, че флуидната природа на интернет и на членските структури на DarkMarket не отговаря на тези критерии – решение, което, естествено, имаше важни последствия за законовите промени по отношение на последствия за законовите промени по отношение на престъпленията в Германия, осъществени чрез интернет. През юли 2008 г. Хартман получи условна присъда от 21 месеца по обвинение в измама. Оттогава продължава следването си в областта на графичния дизайн и напълно прекратил връзките си с подземния свят.

## Макс Вижън или Макс Бътлър или Iceman

На 12 февруари 2010 г. Маск Вижън беше осъден от съда в Питсбърг на тринайсет години зад решетките – най-дългата присъда, постановявана от американски съд за хакерство. Обвинението изчисли, че неговото хакерство на кредитни карти е довело до загуби от повече на 85 милиона долара. Сега е във Федералния затвор с облекчен режим „Ломпок“ в Южна Калифорния, където няма достъп до никакви компютри.

Хакерските умения на Вижън нямат аналог – той безспорно е един от най-интелигентните хора, които лежат в затворите на САЩ. На закрита конференция през есента на 2010 г. обсъждат случая му с един от най-висшите служители от Департамента по национална сигурност, който се занимава с киберзаплахите. Той се съгласи с мен, че да имаш хакер с уменията на Вижън, който чезне в затвора, е наистина прахосване на човешките ресурси на САЩ, но посочи, че егото на Вижън – почти толкова голямо, колкото интелекта му, също играе важна роля в цялата тази работа

## Lord Cyric

Кой е той? Ловът продължава…

### 3. Тъмен и дълбок интернет

### 3.1. Нива и Поднива на Дълбокият Интернет

Няма точна информация за големината на дълбокия интернет. Според много експерти изучаващи функциите на интернет търсачките, индексираното съдържание в чистия интернет е около 1-2% от цялото достъпно онлайн съдържание. В следващите редове ще дефинирам нивата на достъпност в интернет.

### 3.1.1. Първо Ниво

Тук разглеждаме частта от интернет, която ние посещаваме ежедневно. Ние достигаме до това уеб пространство чрез стандартните търсачки. Това е “чистият” т. нар. Интернет - отвореният интернет за масовата публика. Това са сайтове, които не изискват специален достъп, парола и т.н., като блогове, форуми и други публично достъпни уеб сайтове.

### 3.1.2. Второ Ниво

Тук разглеждаме т.нар. “Повърхностен” интернет. Услуги като Reddit, форуми, чат стаи, затворени блогове. Чат- канали и други социални мрежи могат да бъдат намерени в тази част на интернет, като това обикновено е част от интернет, използвана за комуникация между потребителите.

### 3.1.3. Трето Ниво

Това са услуги извън уеб страниците и уеб съдържанието. Тук се намират файлови сървъри, нюз групи, частни уеб сайтове, до които имат достъп само избрани потребители, частни комуникационни системи, до които отново имат достъп само избрани потребители.

### 3.1.4. Четвърто Ниво

Това е нивото на дълбокия интернет. Тук се намират вътрешните информационни системи на различни корпорации, банки, правителствени сайтове. Това е съдържание, което не може да бъде индексирано от уеб търсачките заради сензитивността на информацията. На това ниво могат да бъдат намерени и частни хакерски групи, забранени видео материали, книги и др.

### 3.1.5. Пето Ниво

На това ниво нещата са по- различни. Това е нивото на т.нар. Дарк Нет или Тъмен интернет. Това съдържание не е достъпно нито за уеб търсачките, нито за стандартните уеб браузъри, които използваме в ежедневието. Това е напълно отделна мрежа, наречена ТОР мрежа (TOR Network), достъпна само и единствено чрез специален уеб браузър наречен ТОР браузър (TOR Browser). Тази мрежа се състои от легално, но и от до голяма степен нелегално съдържание. Нелегалното съдържание включва: трафик на наркотици, хора, оръжия, както и частни педофилски мрежи и терористични сайтове.

### 3.2. Тъмен Интернет

### 3.2.1. Същност и характеристики на тъмен интернет

Това е най- дълбоката част от интернет, която е достъпна само чрез специализиран софтуер, наречен ТОР браузър (TOR browser), съкратено от The Onion Router - Лучен Рутер, тъй като архитектурата на ТОР наподобява глава лук, а името е препратка към слоевете на лука (onion - лук от англ.), заради приликата им с начина, по който програмата крие IP адреса ни. Всеки път, когато достигнем даден уебсайт или уеб апликация чрез браузъра си, ние даваме сигнал до сървъра, който поддържа тази страница или уеб апликация. Това автоматично оставя следа от нашия IP адрес в регистъра на системата. IP адресът е най-добрият и надежден идентификатор, чрез който може да бъде получена допълнителна информация за нашето местоположението, 14 страниците които сме посещавали, времето, което сме прекарали в тях, устройството/операционната система, която използваме, та дори размерът на нашият монитор. Когато отворим уеб страница през TOP, сигналът предаван от нашия компютър, бива препратен към голяма мрежа от други компютри и сървъри, като чак след това достига до сървъра на сайта в тъмната мрежа, който искаме да отворим. По този начин се образуват много "слоеве" от сигнали, в които е почти невъзможно да се локализира първоначалния IP адрес. Архитектурата на този тип мрежи е била разработена в самото си начало с военни цели от „Военноморските сили на САЩ“, поради това, че обикновеният интернет не гарантира нужната анонимност, което представлява сериозен риск. Тъмният интернет предоставя високо ниво на анонимност, но не и пълна такава и за това е особено популярен в средите на политически дисиденти, терористични организации, разузнавателните среди и журналисти, които живеят в страни със силно изявена политическа цензура. Съдържанието в тази част на интернет не е достъпно по друг начин освен чрез ТОР. Така например, ако потребителят реши да използвате ТОР браузър за достъп до сайтове в нормалния интернет, то той ще забележи че Гугъл, и други сайтове показват локация различна от реалната, като например Испания, Съединените Американски Щати, Русия, Камбоджа, Албания, Сърбия и други. Това е вследствие на анонимността, предоставена от браузъра. Реално всяка заявка към уеб сайт се създава чрез различен IP адрес.

### 4. Най-често срещани видове атаки

Средства и методи на социално инженерство се използват при много видове атаки. Всички те се основават на човешката слабост, сред които - любопитство, нужда, алчност, негодувание и др. Опитният нападател е в състояние да проведе проучените и подготвените атаки като се вземат предвид слабостите и уязвимостите на предполагаемата жертва. Нека разгледаме петте най-често срещани типа атаки.

* Фишинг

Фишингът е считан за най-честата атака въз основа на социалното инженерство. Носи името си от практиката на телефонни измами (телефонен фишинг), чиято цел е използвайки телефонната мрежа за тръпка и безплатни телефонни разговори. Натрапникът сякаш хвърля стръвта и наблюдава кой или какво ще се закачи. Въпреки че терминът „фишинг“ все още се използва за описване на измамен телефон разговор, най-широко поле на действие за хакери е електронната поща. Потвърдено, над 80% от успешното инсталиране на злонамерен софтуер се случва по този начин. Могат да се разграничат няколко форми на фишинг:

• „Спиър фишинг“ (Spear fishing) - целенасочена атака срещу едно лице или предмет.

• „Лов на китове“ (Whaling) - фишинг измами срещу високопоставени служители, жертви с висока стойност. Насочено към получаване на конфиденциални банкови данни на високопоставени, управляващи служители (президент, вицепрезидент и др.), с цел кражба на пари.

• „Гласов фишинг-вишинг“ (Vishing). За разлика от фишинга, в съобщението има молба да не се влиза в сайта, а да се позвъни на телефонен номер. Този, който се е обадил, чува гласово съобщение с молба за конфиденциални данни.

• „Смишинг“ ( SMShishing - от „SMS“ и „фишинг“) – тип фишинг с помощта на SMS. Измамниците изпращат на жертвата SMS, съдържащ адрес на смишинг сайт с мотивация да го посети. Друга възможност е на жертвата да се предложи да изпрати в отговор SMS съобщение с конфиденциална информация относно данни за плащане или персонален достъп до информационно плащане в Интернет. Списъкът може да бъде продължен. Ако нападателят е извършил щателно разузнаване на набелязаната цел, смишингът може да бъде много ефективен, тъй като е трудно да се открие и да се смекчат последствията.

* Претекст

„Претекст“ (Pretexting) е атака, чрез която се създава фалшив, убедителен сценарии, карайки жертвата да се довери на нападателя и с желание да предостави достъп до лична информация или акаунт данни. Нападателите използват разузнаване чрез отворени източници за информация (OSINT), т.е. информация, която е лесно да се намери в публикувани документи в Интернет и по-специално в социалните мрежи. Претекстът за общуване може да приеме много форми: оферта за работа, комуникация или секс, нещо безплатно срещу малка такса. Тези машинации са стари колкото света. Най-известният претекст е, „афера 419“. Носи името си от член 419 в Нигерийския наказателен кодекс, който измамниците нарушават. На жертвата се дава възможност да участва в получаването на наследство, печелене от лотария или др. Трябва само да се изпратят пари, за да се помогне на автора на писмото да получи наследството или наградата. Този претекст има много варианти в други страни, което изисква бдителност.

* Примамка

„Примамка“ (Baiting) е онлайн или физическа атака за социално инженерство, която обещава на жертвата награда. Използва се алчността на жертвата и любовта й към „облаги“: предлага й се нещо безплатно, ако тя кликва върху връзка в уебсайта. За разлика от кликбайта, който има за цел да увеличи трафика на страници и да увеличи броя показвания на реклами чрез „примамка“, измамниците се опитват да инсталират зловреден софтуер на компютъра на жертвата. Пример за този вид кибератака е невинно изглеждащи сайтове, предлагащи безплатна електронна таблица за финансово планиране. Докато електронната таблица бавно зарежда, нападателят има достъп до всичко, което притежава жертвата. Безплатни филми, музика и порнография – всички те могат да се използват като превозвачи за доставка на злонамерени програми. Друг вариант за „примамка“ е използването на заразени USB устройства, оставени на маса в кафе или на спирки. Неопитните потребители ги взимат от любопитство и ги свързват към компютрите си. Този метод на инсталация е използвана за инжектиране на червея Stuxnet в тайно иранско ядрено съоръжение, което не е свързано с външна мрежова комуникация. Червея Stuxnet, дори и за кратко, успял да спре иранската ядрена програма.

* Методът quid pro quo

„Услуга за услуга“ (Quid Pro Quo) е атака, разчитаща на обмен на информация или услуга, за да убеди жертвата да действа. Както „примамката“, тя предлага на жертвата предимство за предоставяне на информация, например награда, подарък или безплатна услуга. Този метод е особено ефективен в социалните мрежи. Един от често срещаните атаките от този тип са измамни действия на Айти персонала. Тези атаки не са много трудни и често се извършват в движение, т.е. жертвите се избират на случаен принцип. Едно проучване от Великобритания , показва, че хората на случаен принцип спрени в метрото може да предадат паролите си срещу шоколад, евтина химикалка или друга дрънкулка.

* Промъкване

„Промъкване“ (Tailgating) е често срещана физическа атака, чрез която атакуващият се промъква заедно с вас през точка за контрол на достъпа. Нападателят, представящ се за друг служител или куриер от службата за доставка, получава достъп до защитената зона, прониквайки в системата под прикритието на законния потребител или използвайки личната му карта. Най-разпространен метод е да бъде помолен някой да допусне нападателя, защото той си „е забравил своята лична карта“. Такива атака се използват за получаване достъп до защитени зони и изисква нападателят също да използва претекст, за да убеди жертвата в своята искреност и законността на действията си. Един от вариантите е нападател да подмами служител, който има достъп до защитената зона, да му услужи „буквално за минута“ с личната си карта, за да може да се приближи до колата си и да си вземе нещо. Резултатът е копиране на личната карта. Повечето хора искат да се доверяват един на друг. Нападателите са добре информирани и използват това за користните си цели.

## II. Киберсигурност

### Какво е киберсигурност

Поверителността и сигурността на данните винаги ще бъдат най-важните мерки за сигурност, за които се грижи всяка организация. Понастоящем живеем в свят, в който цялата информация се съхранява в цифрова или киберформа. Сайтовете за социални мрежи предоставят пространство, в което потребителите се чувстват в безопасност, докато общуват с приятелите и семейството си. В случая с домашните потребители киберпрестъпниците ще продължат да се насочват към сайтовете на социалните мрежи, за да крадат лични данни. Не само в социалните мрежи, но и по време на банкови транзакции човек трябва да вземе всички необходими мерки за сигурност.

Горното сравнение на инцидентите, докладвани на Cyber999 в Малайзия за периода януари-юни 2012 г. и 2013 г., ясно показва заплахите за киберсигурността. С нарастването на престъпността се увеличават дори и мерките за сигурност. Според проучването на американската продължителност.

- 98% от компаниите поддържат или увеличават ресурсите си за киберсигурност, а от тях половината увеличават ресурсите, отделяни за онлайн атаки през тази година.

- По-голямата част от компаниите се подготвят за това кога, а не дали ще се случат кибератаки.

- Само една трета от тях са напълно уверени в сигурността на своята информация, а още по-малко са уверени в мерките за сигурност на своите бизнес партньори.

Ще има нови атаки срещу устройства, базирани на операционната система Android, но те няма да са в масов мащаб. Фактът, че таблетите имат същата операционна система като смартфоните, означава, че скоро ще бъдат обект на същия зловреден софтуер като тези платформи. Броят на образците на зловреден софтуер за Mac ще продължи да расте, макар и много по-малко, отколкото при PC. Windows 8 ще позволи на потребителите да разработват приложения за практически всички устройства (персонални компютри, таблети и смартфони) с Windows 8, така че ще бъде възможно да се разработват зловредни приложения като тези за Android, следователно това са някои от прогнозираните тенденции в киберсигурността.

### 1.1. Киберсигурността в България

Организациите, които се грижат за киберсигурността у нас са:

1. Дирекция Сигурност на информацията

2. Главна дирекция Борба с организираната престъпност - ГДБОП

3. Дирекция Комуникационни и информационни системи

• Като Дирекция Сигурност на информацията се ръководи от служител по сигурността на информацията , който е пряко подчинен на министъра

• Главна дирекция Борба с организираната престъпност ГДБОП) е специализирана полицейска оперативно издирвателна служба на МВР за противодействие и неутрализиране на престъпна дейност на местни и транснационални престъпни структури

• Дирекция Комуникационни и информационни системи подпомага министъра при определяне на политиките и стратегиите за технологично развитие на комуникационните , информационните , навигационните и сензорните системи

Държавните разходи за киберсигурност в България:

В България отговорна за защитата на действащите информационни системи на администрациите в България е Държавна агенция „електронно управление“ ДАЕУ създадена със закон в края на 2016 г Тя се занимава с развитието и поддръжката на техническата инфраструктура, информационните центрове и комуникационните мрежи на администрацията. За тези си дейности, агенцията е изхарчила над 10 млн. лв. от държавния бюджет 2017 2018 г, сочат данни представени от министерския съвет. Средствата за киберсигурност преди ДАУЕ никой не е следил през годините Пробивът в НАП вероятно ще доведе до въвеждане на нови мерки за сигурност, което означава нови разходи.

Кибер войната в България

България е доста застрашена откъм киберзаплахи , защото не се отделя достатъчно финансиране за подобряване на киберсигурността , а със всяка година технологиите и дигиталната сфера се развиват . Годишно се отделят приблизително 5млн за киберсигурност , което е крайно недостатъчно спрямо развитието на онлайн сектора и събраната лична информация на много българи. Също така в някои сектори има много големи пропуски откъм киберзащита, пример за това е хакерската атака към НАП и източването данни за над 4 милиона живи и над 1 милион вече мъртви българи и фирми, което ги постави в реално уязвимо положение. В края на август Комисията за защита на личните данни глоби Националната агенция по приходите с 5 млн. лв.

### 1.2. Киберсигурността в САЩ

Кой е отговорен за Киберсигурността в САЩ ?

В САЩ департаментът за вътрешната сигурност ръководи за координиране на цялостните национални усилия за повишаване на киберсигурността на критичната инфраструктура на САЩ и осигуряване на защита на гражданските федерални правителствени мрежи и системи.

Националният отдел за киберсигурност (NCSC) отваря врати на 6 юни 2003 г. и е сформиран от:

• Службата за осигуряване на критична инфраструктура

• Националния център за защита на инфраструктурата

• Федералния център за реагиране на компютърни инциденти и заплахи

• Националната комуникационна система

Мисията на NCS C е да си сътрудничи с частния сектор, правителството, военните и др. и заинтересованите страни в разузнаването да извършват оценки на риска, и да смекчат уязвимостите и заплахите за активите и дейностите в областта на информационните технологии, засягащи работата на критичните киберинфраструктури на гражданското правителство и частния сектор. Настоящият директор на NCS C е Джон Стройфорд, бивш главен служител по сигурността на информацията ( CISO ) в Държавния департамент на САЩ, който поема поста през януари 2012 г.

В САЩ бюджетът на президента на за 2019 г. включва 15 милиарда долара за киберсигурност, 583,4 милиона долара 4,1%) увеличение спрямо 2018 г

В САЩ бюджетът на президента на Кибервойната в САЩ. Като основна развита икономика, Съединените щати са силно зависими от Интернет и затова са силно изложени на кибератаки. В същото време Съединените щати разполагат със значителни възможности, както в проектирането на отбраната, така и в силата благодарение на сравнително напредналите технологии и големия военен бюджет. Кибервойната представлява нарастваща заплаха за физическите системи и инфраструктури, които са свързани с интернет. Злобното хакване от вътрешни или чуждестранни врагове остава постоянна заплаха за САЩ. В отговор на тези нарастващи заплахи Съединените щати развиха значителни киберспособности.

Anonymous е децентрализирана международна хактистическа група , широко известна с различните си кибератаки срещу няколко правителства , правителствени институции и правителствени агенции , корпорации и църквата на сциентологията 2019 г. включва 15 милиарда долара за киберсигурност, 583,4 милиона долара 4,1%) увеличение спрямо 2018 г.

## 2. Основни типове компютърни атаки

Компютърната атака представлява злонамерено действие срещу компютърна система и/или мрежа с цел отказ на услуга, извличане на информация, манипулация на данни, изтриване на информация и други. В най-общия случай основна цел на компютърните атаки е, но не се ограничава до парична облага за атакуващия. Други подбуди за атака биха могли да бъдат дестабилизация, шпионаж, хактивизъм или дори форма на отмъщение. Според мотивацията извършителите на киберпрестъпленията биват крадци, шпиони, хактивисти и лица, раздухващи слухове (т.нар. whistleblowers).

Крадците могат да атакуват. както обикновени хора или корпорации, като най-често компютърните атаки са насочени към големи групи потребители. Често подходът им може да бъде засечен и по-нататък ще разгледаме начините, които използват.

Шпионите могат да бъдат измамници, конкуриращи се компании или правителства. Тяхна цел са научно-изследователска дейност, финансови, търговски или стратегически данни. Оттам може да се ескалира към кражба на самоличност, извличане на банкови данни, кражба на лична информация, локализиране на местоположение в реално време, обири и други.

Хактивистите, от друга страна, осъществяват атаки, за да се опитат да наложат техните политически убеждения. Често тяхната цел е свързана със свобода на словото, човешки права или просто негодуване срещу монопола. Подходите и атаките, които използват обикновено, са DoS атаки или обезобразяване на сайт, като заменят съдържанието на дадения сайт с подбрано от тях такова. Пример за хактивисти са групите Anonymous или Wikileaks.

Лицата, раздухващи слухове, не осъществяват атаки, за да получат парично обезпечение. Обикновено тяхната цел е да изобличат някаква измама или неправда, която те смятат за такава. В съвременния живот това се пренася и във формата на атаки над компютърни мрежи и системи. Най-известното лице, което успя да изнесе, разпространи и разобличи информация в последното десетилетие, е Едуард Сноудън.

В крайна сметка, независимо от целта и мотива на нападателите, и независимо дали са срещу компютърни терминали, информационни, индустриално контролни системи, мрежата или приложния слой, атаките основно се делят на DoS атаки, man-in-the-middle (MitM), malware атаки, XSS (cross-site scripting) и социално инженерство.

### 3. Ролята на социалните мрежи в киберсигурността

Тъй като ставаме все по-социални в един все по-свързан свят, компаниите трябва да намерят нови начини за защита на личната информация. Социалните медии играят огромна роля в киберсигурността и ще допринесат много за личните киберзаплахи. Възприемането на социалните медии от персонала расте главоломно, както и заплахата от атаки. Тъй като социалните медии или сайтовете за социални мрежи се използват от повечето от тях почти всеки ден, те са се превърнали в огромна платформа за киберпрестъпниците за хакване на лична информация и кражба на ценни данни.

В свят, в който бързо предоставяме личната си информация, компаниите трябва да гарантират, че са също толкова бързи в идентифицирането на заплахите, да реагират в реално време и да избягват пробиви от всякакъв вид. Тъй като хората лесно се привличат от тези социални медии, хакерите ги използват като примамка, за да получат необходимата им информация и данни. Следователно хората трябва да вземат подходящи мерки, особено при работа със социалните медии, за да предотвратят загубата на своята информация. Способността на хората да споделят информация с милионна аудитория е в основата на конкретното предизвикателство, което социалните медии представляват за бизнеса. Освен че дават на всекиго възможността да разпространява чувствителна търговска информация, социалните медии дават и същата възможност за разпространение на невярна информация, която може да бъде също толкова вредна. Бързото разпространение на невярна информация чрез социалните медии е сред новите рискове, посочени в доклада "Глобални рискове 2013".

Въпреки че социалните медии могат да бъдат използвани за киберпрестъпления, тези компании не могат да си позволят да спрат да използват социалните медии, тъй като те играят важна роля за публичността на компанията. Вместо това те трябва да разполагат с решения, които да ги уведомяват за заплахата, за да я отстранят, преди да бъдат нанесени реални щети. Въпреки това компаниите трябва да разберат това и да признаят важността на анализа на информацията, особено в социалните разговори, и да осигурят подходящи решения за сигурност, за да стоят настрана от рисковете. Човек трябва да се справя със социалните медии като използва определени политики и подходящи технологии.

### 4. Техники за киберсигурност

### 4.1. Контрол на достъпа и сигурност на паролата

Концепцията за потребителско име и парола е основен начин за защита на нашата информация. Това може би е една от първите мерки по отношение на киберсигурността.

### 4.2. Удостоверяване на автентичността на данните

Документите, които получаваме, винаги трябва да бъдат автентифицирани, преди да бъдат изтеглени, т.е. трябва да се провери дали произхождат от доверен и надежден източник, и дали не са променени. Удостоверяването на автентичността на тези документи обикновено се извършва от антивирусния софтуер, наличен в устройствата. Следователно добрият антивирусен софтуер също е от съществено значение за защитата на устройствата от вируси.

### 4.3. Скенери за злонамерен софтуер

Това е софтуер, който обикновено сканира всички файлове и документи, присъстващи в системата за зловреден код или вредни вируси. Вирусите, червеите и троянските коне са примери за зловреден софтуер, които често се групират и се наричат зловреден софтуер.

### 4.3.1. Malware

Malware е съкратено от ‘Malicious Software’ (зловреден софтуер). На практика е създаден да осигури достъп до чужд компютър, като подвежда собственика му да инсталира определен софтуер. Той може да следи действията на потребителския компютър и да причинява вреди, за които потребителят може и да не подозира. Malware най-често се среща във вид на вируси, червеи или шпионски софтуер. Също така може да се използва за крадене на информация или за разпръскване на спам през имейл. В наши дни обаче, този лъжлив софтуер най-общо се използва за генериране на значителни приходи чрез маскирана реклама.

Зловредният софтуер Fireball превърна повече от 250 милиона уеб браузъра по целия свят в генериращи приходи от рекламни машини. Почти 20% от корпоративните мрежи са били засегнати заради този malware. По-късно е било установено, че широкото разпространение на Fireball се дължи на пакетирането. Поради желани от потребителя програми като Deal Wifi, Mustang Browser, Soso Desktop и FVP Imageviewer, Мalware се инсталира без знанието от страна на потребителя. Едва седмица преди това 36.5 милиона Android устройства бяха засегнати от malware, наречен Джуди. Чрез фалшиви кликове по реклами, с цел генериране на печалби, този зловреден софтуер е бил открит в 41 приложения, всяко от които е разработено от корейската компания Kiniwini. Повечето от зловредните приложения се предлагаха в официалния Google Play Store, повдигайки сериозно въпроса за сигурността на Android.

Също така malware с името ‘Crash Override’ е бил засечен да се носи свободно из интернет пространството и предизвика прекъсване на електрическото захранване в украинската столица Киев. Това е първият malware, който атакува електрическа мрежа, подсказвайки за катастрофалните последици, които могат да последват.

### 4.3.2. Ransomware

Ransomware е тип malware, който заключва компютъра и забранява достъпа до него, докато не се плати исканият откуп (обикновено се изисква в Bitcoins). В днешно време, вместо да блокират достъпа на потребителя, конкретни файлове биват криптирани с помощта на личен ключ, който само авторите на съответния ransomware знаят. Няма гаранция, че плащането на откупа ще отключи компютъра.

През 2017 широкомащабна кибератака от ransomware Wannacry зарази повече от 300,000 компютъра в 150 страни. Тогава са били засегнати само компютри с операционната система Windows.

Друг Ransomware, Petya, е бил засечен в множество бизнеси, опериращи в Европа, Средния Изток и Съединените щати. Основната разлика между Petya и WannaCry е, че тя може да се разпространява само из местната мрежа. От друга страна WannaCry можеше да се разпространи експоненциално и безкрайно из интернет при липса на авариен прекъсвач.

Било е установено, че Petya не е ransomware, а смъртоносен “Wiper Malware”. Проучващите вируса са открили, че Petya е бил създаден само да прилича на ransomware. Софтуерната му рамка няма никаква схема за обработка на информация. След рестартиране на компютъра на жертвата, Petya криптира главната таблица на файловете на твърдия диск и прави първия зареждащ сектор (MBR) нефункционален. Криптираният код е заменен с техен собствен зловреден код, който забранява на потребителя да рестартира компютъра си, след което извежда съобщение за откупа на екрана. Новият вариант на Petya изобщо не поддържа копие на подменения MBR. Така че, дори и жертвата да получи декриптиращия ключ, няма да може да зареди компютъра си.

### 4.3.3. Как се разпространяват malware и ransomware?

Разпространението на malware става предимно чрез имейли, с връзки, които привличат вниманието на потребителя, предлагайки нещо, което би представлявало интерес за него. Щом потребителят веднъж кликне върху връзката, той бива пренасочен към фалшив уеб сайт, който обикновено изглежда като действащ такъв. След това, за да получат достъп до желаната информация или програма, очакват от потребителя да свали софтуер. Ако той стори това, компютърът му бива заразен.

Уеб сайтове с безплатно съдържание и изскачащи реклами са измежду основните източници на кибератаки. Пробивите в сигурността позволяват на нарушителите да следят поведението на компютъра, който се ползва и да отмъкват данните. Те могат да бъдат използвани за множество подправени дейности и последствията могат да бъдат много сериозни**.**

### 4.4. Защитни стени

Защитната стена е софтуерна програма или част от хардуера, която помага за отсяването на хакери, вируси и червеи, които се опитват да достигнат до вашия компютър чрез интернет. Всички съобщения, които влизат или излизат от интернет, преминават през присъстващата защитна стена, която разглежда всяко съобщение и блокира тези, които не отговарят на определените критерии за сигурност. Следователно защитните стени играят важна роля при откриването на зловреден софтуер. Докато антивирусният софтуер може да засече вирус и да се отърве от него, то защитната стена изобщо не му позволява да влезе в компютъра. Защитната стена в общи линии е подслушващ софтуер, който стои между компютъра и интернет. При работа с глобалната мрежа, постоянно се изпращат пакети с информация ,които се връщат обратно. Защитната стена филтрира тези пакети и действа като щит за всеки, който би могъл да нанесе вреда. Защитната стена не допуска проникване на вируси в системата, но ако даден вирус все пак успее да премине, то тя няма да може да го отстрани.

### 4.5. Антивирусен софтуер

Антивирусният софтуер е компютърна програма, която открива, предотвратява и предприема действия за обезвреждане или премахване на злонамерени софтуерни програми, като вируси и червеи. Повечето антивирусни програми включват функция за автоматично обновяване, която позволява на програмата да изтегля профили на нови вируси, за да може да проверява за нови вируси веднага след откриването им. Антивирусната програма е задължителна и от основна необходимост за всяка система. Докато кибератаките са насочвани директно, вирусите се срещат много по-често и се хващат произволно от интернет мрежата. Независимо че, един вирус няма да криптира данните, той може да ги открадне и да инфектира компютъра, забавяйки продуктивността му. Антивирусният софтуер често може да спре 99% от известните вируси. Той също така може да ни защити от нежелан спам и шпионски софтуер, предназначен да следи работния процес и да записва данни.

## 4.6. Троянски кон

Троянските коне са програми, които предлагат или изглежда, че предлагат, привлекателна функция или характеристика, но после тайно извършват злонамерени действия във фонов режим.

Кръстени на Троянския кон от гръцката легенда, троянските коне са програмирани, така че да изглеждат привлекателни за потребителя. Могат да изглеждат като игри, скрийнсейвъри, актуализации на приложения или друг вид полезни програми или файлове. Някои троянски коне имитират или дори направо копират популярни или добре-познати програми за да изглеждат по-надеждни. Целта на описанието е да се подмами потребителят, за да инсталира троянския кон.

След като бъдат инсталирани, троянските коне използват "примамки", за да поддържат представата, че са законни. Например троянски кон, прикрит като приложение за скрийнсейвър или файл на документ, ще покаже изображение или документ. Докато вниманието на потребителя е отвлечено от тези примамки, троянският кон може тайно да извършва други действия във фонов режим.

Троянските коне обикновено правят опасни промени в устройството (например изтриване или шифроване на файлове, или промени в настройките на дадена програма) или крадат поверителна информация, съхранена в него. Троянските коне могат да се групират по действията, които извършват:

* Троянски кон-изтеглящ: свързва се към отдалечен сайт, за да изтегля и инсталира други програми
* Троянски кон-пускащ: съдържа една или повече допълнителни програми, които инсталира
* Троянски кон-крадец на пароли: Краде пароли, съхранени на устройството, или въведени в уеб браузър
  + Троянски кон-банкиране: Специализиран троянски кон-крадец на пароли, които специфично търси потребителски имена и пароли за портали за онлайн банкиране
* Троянски кон-шпионин: Следи дейността на устройството и препраща подробностите на отдалечен сайт

### 5. Кибер етика

Кибернетичната етика не е нищо друго освен кодекс на интернет. Когато практикуваме тази кибернетична етика, има големи шансове да използваме интернет по правилен и по-безопасен начин.

По-долу са изброени някои от тях:

* НЕ използвайте интернет за комуникация и взаимодействие с други хора. Електронната поща и незабавните съобщения улесняват поддържането на връзка с приятели и членове на семейството, общуването с колеги от работата и споделянето на идеи и информация с хора от другия край на града или от другия край на света
* Не бъдете хулигани в интернет. Не наричайте хората с имена, не лъжете за тях, не изпращайте техни неудобни снимки и не правете нищо друго, за да се опитате да ги нараните.
* Интернет се счита за най-голямата библиотека в света с информация по всяка тема във всяка тематична област, така че използването на тази информация по правилен и законен начин винаги е от съществено значение.
* Не работете с акаунти на други хора, като използвате техните пароли.
* Никога не се опитвайте да изпращате, какъвто и да е зловреден софтуер в чужди системи и да ги повреждате.
* Никога не споделяйте личната си информация с никого, тъй като има голяма вероятност други да злоупотребят с нея и накрая да се окажете в беда.
* Когато сте онлайн, никога не се преструвайте на другия човек и не се опитвайте да създавате фалшиви акаунти на някой друг, тъй като това би вкарало в неприятности както вас, така и другия човек.
* Винаги се придържайте към информацията, защитена с авторски права, и сваляйте игри или видеоклипове само ако са разрешени.

Горепосочените примери са няколко от правилата на кибернетичната етика, които трябва да се спазват при използването на интернет. Винаги сме мислили за правилните правила още от най-ранните етапи на живота си, като същите прилагаме и в киберпространството.

### 6. Структура и управление на обществената и фирмена сигурност.

Един от най-сериозните проблеми свързани с организацията на работа по защитата на хора ,финансовите средства и информация в условията на пазарна икономика се явява въпросът за сигурността на службата за сигурност. За разлика от органичните и неорганичните природни структури, структурите на социалната сфера ,имат свои специфични особености ,строеж и управление. От тяхната оптималност и функционалност зависят крайните резултати или до колко дадени системи са способни да постигнат крайната цел, за която са създадени. Не е оправдано да се изграждат структури, задачи, да се разкриват нови щатове, които да оправдават ничие присъствие и неоправдано харчене на пари. Именно затова в теорията и практиката е прието въвеждане във всяка нова управленска структура да бъде добре регламентирано и защитено. За целта се разработват модели, макети, които да онагледят оказаната необходимост. Това е още по-необходимо за структурата ,която ще отговори за сигурността ,с която да се определи взаимовръзките вътре в системата и извън нея. Структурата на системата за сигурност зависи и от пазарната структура. В условията на пазарна икономика функционират няколко основни вида организации: еднолични, дружествени и корпоративни фирми. Тези формулировки се намират в остра конкурентна борба. Освен това те са постоянен обект на взимане на страна на т.нар. организирана престъпност. Критериите за изграждане на структурата на системата за сигурност са:

* да е съобразена с целите ,задачите и функциите на сигурност;
* да е оптимална по състав;
* да позволява взаимозаменяемост и съвместимост;
* да съществува ефективна координация и взаимодействие с останалите структури на организацията и други.

Съществуват и други модели за структурата на системата за сигурност. Обикновено се използва следната структура:

* физическа охрана на хора, собственост, финансови средства и информация.
* Структурата „ситуационна”, в която се включват дейности за противопожарна безопасност охрана на труда и авариино-спасителни процедури.
* Информационно-кадрова;
* Административно-техническа;
* Противодействие-в нея освен защитни се съставляват и разпознавателни дейности. В структурата на службата за сигурност основните направления имат следните разделения:

1. Физическа охрана:

* охрана въоръжена и невъоръжена на служебната собственост;
* пропускателен режим и персонална охрана и други.

2. Противопожарна безопасност, охрана на труда и авариxноспасителна дейност:

* пожар охранителна дейност на наличната собственост;
* организиране и провеждане на защитни дейности при БАК.

3. Информационно кадрова работа:

* изготвяне на законосъобразни нормативни документи;
* разработване на планове и отчети за дейността;
* изучаване и набиране на кадри и подготовка на обучението им;

4. Административно-техническа дейност:

* завеждане на документи;
* осигуряване на техническа защита с/у неправомерно използване;
* транспортни средства и грижи за обезопасяването им.

5. Противодействие:

* контрол за изпълнение на нормативните документи

Основни направления на работата в общинската и фирмена сигурност. Сигурността се гради в/у две направления: физическа и информационна закрила. Физическата защита на хора, собственост, фирмени средства от престъпни посегателства ч/з правно организационни и инженерни технически мерки. Много често липсва цялостна законова нормативна база и недостатъчно познаване и погрешно прилагане в практиката води до обезсмисляне на цялостната система за сигурност. Физическата защита обхваща административно правните мерки, които обхващат следните: Конституция, кодекси, укази, правилници, патенти и други. Също така физическата защита обхваща и организационните мерки. Те включват подбор на кадри, режим и охрана, разкриване и прекратяване на престъпни посегателства, аварийно спасителна дейност, информационно аналитична работа. Физическата защита обхваща и инженерно-технически мерки. А те включват: физически средства, програмни апаратни средства ,химично-биологични, лазерни средства и други. Новите условия, особено след влизането в ЕС, налага да се търси оптималност м/у охранителната дейност и информационната закрила. А това налага съотношение м/у структурите и функциите на звената, анализирани с физическата защита и информационната закрила. Същността на физическата защита се изразява в практическото прилагане на организационно-законосъобразни мерки за: опазване на живота и здравето на всички, имуществото, финансовите средства и ценности. Информационната закрила се изразява в опазване на информацията, която представлява служебна тайна, ползването на информационни средства и системи. В най-общ аспект престъпните посегателства към всички, в които се работи, се свежда до въвличането в престъпни дейности, психологически терор, въоръжени грабежи с цел обсебване на финансови средства или документи ,убийство. Така престъпните посегателства трудно могат да се разграничават в две направления, ако не съществува ориентировъчно правило ,да се различават престъпления от стопански и криминален характер, с престъпленията насочени главно към работата с информацията и организацията.

### 7. Тенденции, променящи киберсигурността

По-долу са посочени някои от тенденциите, които оказват огромно влияние върху киберсигурността.

### 7.1. Уеб сървъри

Заплахата от атаки срещу уеб приложения с цел извличане на данни или разпространение на зловреден код продължава да съществува. Киберпрестъпниците разпространяват своя зловреден код чрез легитимни уеб сървъри, които са компрометирани. Но атаките за кражба на данни, много от които привличат вниманието на медиите, също са голяма заплаха. Сега е необходимо да се наблегне повече на защитата на уеб сървърите и уеб приложенията. Уеб сървърите са особено най-добрата платформа за тези киберпрестъпници за кражба на данни. Следователно човек винаги трябва да използва по-безопасен браузър, особено по време на важни транзакции, за да не стане жертва на тези престъпления.

### 7.2. VPN

VPN е услуга, която може да се ползва отвсякъде и на почти всяко устройство. Тя криптира данните, правейки прихващането им значително по-трудно за хакерите.

VPN, или виртуални частни мрежи, първоначално са били създадени за големите компании и правителствените организации. Целта е била служителите, които работят от разстояние да могат безопасно да се свързват с мрежата на компанията, без да излагат на опасност корпоративните данни.

В днешни дни всеки може да се възползва от тази защита. VPN услугата създава тунел между устройството на потребителя и сървъра, предпазвайки го от хакери или други злонамерени страни, които биха искали да отмъкнат лична информация. Тя също криптира данните, така че дори да бъдат откраднати, е почти невъзможно да бъдат декриптирани.

### 7.3. Облачни изчисление и техните услуги

В наши дни всички малки, средни и големи компании бавно възприемат облачните услуги. С други думи, светът бавно се придвижва към облаците. Тази последна тенденция представлява голямо предизвикателство за киберсигурността, тъй като трафикът може да заобикаля традиционните точки за проверка. Освен това, тъй като броят на наличните в облака приложения нараства, контролът на политиките за уеб приложенията и облачните услуги също ще трябва да се развива, за да се предотврати загубата на ценна информация. Въпреки че облачните услуги развиват свои собствени модели, все още се повдигат много въпроси относно тяхната сигурност. Облакът може да предоставя огромни възможности, но винаги трябва да се има предвид, че с развитието на облака нарастват и проблемите, свързани с неговата сигурност.

### 7.4. АРТ и целеви атаки

APT (Advanced Persistent Threat) е съвсем ново ниво на киберпрестъпления. В продължение на години възможностите за мрежова сигурност, като например филтриране на уеб страници или IPS, играеха ключова роля в идентифицирането на такива целенасочени атаки (най-вече след първоначалното компрометиране). Тъй като нападателите стават все по-смели и използват по-неясни техники, мрежовата сигурност трябва да се интегрира с други услуги за сигурност, за да се откриват атаки. Следователно трябва да подобрим техниките си за сигурност, за да предотвратим появата на повече заплахи в бъдеще.

### 7.5. Мобилни мрежи

Днес можем да се свързваме с всеки във всяка част на света. Но сигурността на тези мобилни мрежи е много голям проблем. В днешно време защитните стени и другите мерки за сигурност стават все по-пропускливи, тъй като хората използват устройства като таблети, телефони, персонални компютри и т.н. Всички те отново изискват допълнителни защити освен тези, които са налични в използваните приложения. Винаги трябва да мислим за въпросите на сигурността на тези мобилни мрежи. Освен това мобилните мрежи са силно податливи на тези киберпрестъпления, затова трябва да се внимава много за проблемите със сигурността им.

### 7.6. IPv6: Нов интернет протокол

IPv6 е новият интернет протокол, който заменя IPv4 (по-старата версия), който беше гръбнакът на нашите мрежи и на интернет като цяло. Защитата на IPv6 не е само въпрос на пренасяне на възможностите на IPv4. Макар че IPv6 е цялостна замяна, която осигурява повече IP адреси, в протокола има някои много фундаментални промени, които трябва да се вземат предвид в политиката за сигурност. Ето защо винаги е по-добре да се премине към IPv6 възможно най-скоро, за да се намалят рисковете, свързани с киберпрестъпленията.

### 7.7. IPv4

Интернет протокол версия 4 (IPv4) е четвъртата ревизия при разработката на [Internet Protocol](https://bg.wikipedia.org/wiki/Internet_Protocol) (IP) и първата версия на протокола, която намира широко разпространение. Заедно с [IPv6](https://bg.wikipedia.org/wiki/IPv6" \o "IPv6) този протокол е в основата на стандартните мрежови технологии в [интернет](https://bg.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82" \o "Интернет).

IPv4 е описан в публикация [IETF](https://bg.wikipedia.org/wiki/IETF" \o "IETF) [RFC 791](https://tools.ietf.org/html/rfc791) (септември 1981), заменяйки по-ранната дефиниция ([RFC 760](https://tools.ietf.org/html/rfc760), януари 1980). Протоколът все още се използва за по-голямата част от интернет трафика в днешно време.[[1]](https://bg.wikipedia.org/wiki/IPv4#cite_note-:0-1) Използва 32-битово адресно пространство, което предоставя общо 4 294 967 296 уникални адреса, макар че големи блокове от него са резервирани за специални мрежови методологии (около 18 млн. адреса за [частни мрежи](https://bg.wikipedia.org/wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D0%B8_%D0%BC%D1%80%D0%B5%D0%B6%D0%B8" \o "Частни мрежи) и около 270 млн. [мултикаст](https://bg.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%82%D0%B8%D0%BA%D0%B0%D1%81%D1%82" \o "Мултикаст) адреса).

### 

### 7.8. Криптиране на кода

Криптирането е процесът на кодиране на съобщения (или информация) по такъв начин, че подслушвателите или хакерите да не могат да ги прочетат. В една схема за криптиране съобщението или информацията се криптира с помощта на алгоритъм за криптиране, като се превръща в нечетим шифров текст. Обикновено това се прави с помощта на ключ за криптиране, който определя как да бъде кодирано съобщението. Криптирането на най-начално ниво защитава поверителността на данните и тяхната цялост. Но по-широкото използване на криптирането води до повече предизвикателства в киберсигурността. Криптирането се използва и за защита на данни при пренос, например данни, които се предават чрез мрежи (например интернет, електронна търговия), мобилни телефони, безжични микрофони, безжични домофони и др. Следователно чрез криптиране на кода може да се разбере дали има изтичане на информация.

Следователно горепосочените са някои от тенденциите, които променят облика на киберсигурността в света.

### 8. Методи за предотвратяване на кибератака

За да се намали риска от човешка грешка, застрашаваща киберсигурността, се използват следните пет метода. Намаляване полето за атака Необходим е внимателен анализ на цялата Айти инфраструктура на съоръжението, погледнато през очите на нападателя. Трябва да се използват средства за контрол на достъпа чрез защитни стени, използване на биометрични данни и ограничаване достъпа до критически важни системи на болшинство служители. Обстойна проверка на персонала, тъй като най-слабото звено в областта на сигурността е човекът. Логична стъпка е максималното елиминиране на човешкият фактор, а именно допускане на минимално човешкото взаимодействие. Може да звучи като ерес, но сблъсквайки се с криза, ще се предотврати небрежността и неспособността на някои хора да разпознаят заплахата. Изграждане на екип за мрежова сигурност: Въпреки че обучението може да смекчи някои заплахи, препоръчителен е персонал, който след профилирано обучение ще може да разпознава заплахите, и да ги предотвратява, прилагайки редовно процедурите на безопасност и киберхигиена на служителите. Тези хора трябва да имат правомощия за отстраняване уязвимостите и да имат способността да коригират поведението на служителя-нарушител. „Ударна група“, като екип за бързо реагиране, състоящ се от мрежови администратори, охранителен персонал и старши служители, може бързо да открие нарушението, да се справи с него и след това да направи „аутопсия“, за да се определи как това се е случило и да се вземат необходимите превантивни мерки, за да се предотвратят подобни ексцесии в бъдеще. Организация и използване на ролево базиран контрол на достъп Нищо не може да попречи на служителя да пише пароли на листчета или да гледа на киберсигурността като на безполезна професия. С тази тип манталитет, борбата е трудна, в същото време такъв служител има достъп до мрежата и ресурсите в процеса на работа. Разделяне (разпространение на потребителска информация по категории или по обекти) е един от начините за решаване на този проблем. Ролево-базираният достъп (role-based access, RBAC) е ефективен метод на разделяне. Друг действащ метод е да се изисква официална заявка за достъп и след това наблюдение на служителите при достъпа до критични данни или системи. Многофакторното удостоверяване също може да бъде полезно, но не и ако служителят не го приема сериозно и е небрежен с телефона си или други вторични средства за удостоверяване. Избор на надеждни пароли Принуждаване на прилагането на политика на задължителна редовна промяна на паролата (или по-добре тяхното генериране) ефективно предотвратява възможността персонала да използва лесно познаваеми пароли като „1234567“ или също толкова популярната „парола“.

### 

### Заключение

Като заключение на всичко описано до момента мога да кажа, че киберпрестъпленията са болестта на компютърната ера, в която живеем. За да успеем да се преборим с киберпрестъпленията, е необходимо да се изгради “международна агенция за борба с киберпрестъпленията”, която да включва редица дейности, които да помагат на обикновенните потребители. Това би защитило по-малките фирми и големи корпорации по най-добрия начин. Мисля, че тази агенция трябва да обхваща всичко необходимо за борба с тази “заразна болест”. Агенцията трябва да разработва най- новия и модерен антивирусен софтуер, все по-защитен и модернизиран хардуер и най- важното - да са достъпни за всеки потребител на интернет.

За да се преборим с киберпрестъпността трябва да се създаде специален закон за киберпрестъпленията, който да изисква многократно завишени мерки за сигурност.

Компютърната сигурност е обширна тема, която придобива все по-голямо значение, тъй като светът става силно взаимосвързан, а мрежите се използват за извършване на важни транзакции. Киберпрестъпността продължава да се отклонява по различни пътища с всяка изминала нова година, както и сигурността на информацията. Най-новите и разрушителни технологии, заедно с новите кибернетични инструменти и заплахи, които излизат наяве всеки ден, поставят организациите пред предизвикателството не само как да защитят инфраструктурата си, но и как да изискват нови платформи и разузнаване за това. Няма перфектно решение за киберпрестъпленията, но трябва да се постараем на ниво да ги сведем до минимум, за да имаме сигурно и безопасно бъдеще в киберпространството.

## 

## Източници:

1. “DarkMarket: Киберкрадци, киберченгета и самият ти” Миша Глени
2. Предизвикателства пред ефективното прилагане на политиката за киберсигурност на ЕС. Информационно-аналитичен документ Март 2019 г.
3. https://www.globaldrugsurvey.com/past-findings/gds2017-launch/dark-net-markets-the-good-the-bad-and-ugly/

Пазари на тъмни мрежи: доброто, лошото и грозното?

1. <https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>

Криптополитика и тъмен интернет

1. <https://bg.vpnmentor.com/blog/malware-%D0%B8-ransomware-%D0%BA%D0%B0%D0%BA%D0%B2%D0%B0-%D0%B5-%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D0%BA%D0%B0%D1%82%D0%B0/>

Malware и Ransomware

1. <http://www-it.fmi.uni-sofia.bg/ReDisInfo/courses/modules/module2/parts/module1/part3/index.html> - Компютърна сигурност