СТУДИЈЕ ПРИ УНИВЕРЗИТЕТУ, УНИВЕРЗИТЕТА У БЕОГРАДУ
СТУДИЈСКИ ПРОГРАМ "РАЧУНАРСТВО У ДРУШТВЕНИМ НАУКАМА"

ЗЛОУПОТРЕБА ПЛАТНИХ КАРТИЦА У САЈБЕР ПРОСТОРУ

– МАСТЕР РАД –

Студент: Нина Ђерковић
Бр. индекса: 195/2015.

Ментор: проф. др. Ивана Симовић Хибер

Београд, 2018.

СПИСАК СКРАЋЕНИЦА

1. Amex – American Express
2. ATM – Automated Teller Machine
3. BIN – Bank Identification Number
4. CIA – Confidentiality Integrity Availability
5. EMV – Europay Master VISA
6. ЕУ – Европска Унија
7. ISO – International Standard Organization
8. ITS – Internet Transactional Server
9. MC – Master Card
10. PAN – Personal Account Number
11. PCI – Payment Card Industry
12. PIN – Personal Identification Number
13. POS – Point of Sale
14. РС – Република Србија
15. УН – Уједињене нације

СПИСАК СЛИКА

САДРЖАЈ

УВОД

Нагли развој система који су базирани на информационо-комуникационим технологијама (ИКТ) утицао је на нов начин размене информација, што је омогућило транзицију пословања са традиционалног на електронско, и размену личних података електронским путем. Промене су захтевале добро осмишљен информациони систем због неопходне брзе обраде информација од значаја (финансијски извештаји, персонални подаци, пословне тајне).

Свака промена целовитости или садржаја битних информација може да утиче на кредибилитет или изазове последице које могу да, привремено или трајно, онемогуће размену битних података. Из тог разлога, елиминација или смањење потенцијалног ризика, и квалитетна организација информационог система, обезбеђују добар основ за борбу против људских и системских грешака, или малициозних напада.

Са становишта савремених ИТ, квалитет информационо-комуникационог система одређује на који начин ће подаци бити креирани, обрађивани, складиштени и преношени, на који ће начин бити изведена њихова заштита и како ће они бити уништавани. Ови поступци су основа информационе безбедности, тј. активности која обезбеђује заштиту података с циљем да буде минимализован утицај ризика и претњи. Она подразумева заштиту поверљивости, интегритета и доступности података уз примену контролних механизама који су унапред одређени, надгледани, и проверавани у реалном времену. Овакав систем познат је као CIA[1] триада (Протић, 2013:136-137).

Овај рад приказује специфичан пример злоупотребе података у сајбер простору – злоупотребу платних картица. Постоји низ упозорења о поступцима који се користе како би се обезбедила тајност података на картицама. Међутим, масовна је појава да се корисници не придржавају тих упозорења. Често се лозинке записују на папирима, дају другим особама, а подаци преносе телефонски или без да су заштићени на одговарајући начин. Такође, адреса, бројеви телефона, матични број, број личне карте, и слично преносе се тако да буду јавно доступни. Сваки од ових поступака може скупо да кошта корисника.

Пример једне од малициозних злоупотреба приказан је као студија случаја за Diners картицу.

[1] CIA – **C**onfidentiality (поверљивост), **I**ntegrity (интегритет), **A**vailability (доступност)

Рад је организован на следећи начин. Након увода и методолошко-хипотетичког оквира у којем су наведени циљеви, хипотезе и методе истраживања, у другом поглављу описана је заштита података у сајбер простору. Дефинисан је појам сајбер простора и дате његове карактеристике, а описане су и најчешће активности и елементи напада на сајбер простор. Такође, у овом поглављу су описани безбедносни ризици у електронским трансакцијама путем Интернета. У трећем поглављу објашњени су структура, начин рада и типови платних картица, и приказана је њихова класификација. Описана су средства, предности и мане електронског плаћања. Наведени су учесници електронског пословања и дат је опис терминалне опреме која се користити, односно банкомата и POS[2] терминала. Прво је описана хардверска структура картице, по слојевима, и одговарајућа заштита. Након тога описана је злоупотреба података са контактних и бесконтактних платних картица. Пето поглавље намењено је сајбер безбедности. Описана је заштита података у сајбер простору и заштита електронских платних картица и електронских трансакција. Посебно, шесто поглавље, намењено је разматрању кривично-правних аспеката злоупотребе платних картица. У оквиру овог поглавља прво су описане активности Уједињених нација на сузбијању компјутерског криминалитета, а потом активности Савета Европе. Последње подпоглавље даје приказ стратешког и правног оквира за заштиту од сајбер криминала у Републици Србији са два аспекта, подзаконске регулативе у области заштите података и правне регулативе у области електронских платних картица. Седмо поглавље даје пример напада на Diners Club платну картицу, а последње поглавље је закључак рада. На крају је дат списак коришћених референци.

[2] POS (**P**oint **O**f **S**ale) – продајно место (енгл.)

1. МЕТОДОЛОШКО-ХИПОТЕТИЧКИ ОКВИР

1.1. Циљ и предмет рада

У раду ће бити приказано на који начин грешке или малициозни напади могу изазвати компромитацију информација од значаја, а фокус истраживања биће на безбедности оних информација које се налазе на самој картици или се размењују у електронским трансакцијама као што су нпр. подизање средстава са банкомата или плаћање производа и услуга електронским путем.

Циљ рада је и, на основу докумената који важе и примењују се у свету, као што су резолуције Уједињених нација, стандарди и прописи Европске уније и закони и прописи који се односе на нарушавање информационе безбедности, а примењују се у Републици Србији, приказати на који начин је могуће борити се против злоупотребе информација у сајбер простору. Наиме, проблем заштите података препознат је као веома битан због последица које могу бити једнако тешке као и код прекршаја или кривичних дела која одговарају онима у реалном свету.

Као студија случаја приказана је Diners Club International платна картица, која је изабрана као пример јер се користи на више од 20 милиона продајних места у свету и постоји њена виртуелна апликација на мобилним телефонима.

1.2. Хипотезе

Рад треба да прикаже на који начин се изводе злоупотребе електронских платних картица у сајбер простору, што је могуће разматрати са аспеката сајбер простора као виртуелног окружења у ком постоје погодни услови за малициозне нападе, структуре електронских платних картица која омогућује промену или крађу података и заштите информационо-комуникационе инфраструктуре у смислу мера које се предузимају како би биле смањене могућности крађе информација од значаја. У том смислу у раду су постављене три хипотезе:

X1. У сајбер простору постоји реална опасност од последица малициозних напада на податке који се налазе на електронским платним картицама или се преносе путем рачунарских мрежа.

X2. Структура електронских платних картица омогућује промену или крађу података.

X3. Мере заштите информационо-комуникационих технологија могу утицати на смањење могућности крађе података са платних картица.

1.3. Методе истраживања

Да би хипотезе биле доказане, у раду ће бити коришћена теоријска истраживања дате теме која ће бити изведена на основу јавно доступне литературе и електронских референци. С обзиром на сложеност предмета истраживања, сврху и доступност података, методе истраживања које ће бити примењене у раду су следеће:

- дескриптивна метода биће коришћена за опис информационо-комуникационих система, приказ платних картица, банкомата и терминалне опреме и опис могућих малициозних напада на корисника,
- биће примењена метода анализе доступних података из литературе и података јавно доступних путем електронских претраживача и
- биће изведена синтеза коришћених података у циљу добијања увида у проблематику на студији случаја.

1) Дескриптивна метода биће коришћена за опис појмова сајбер простора и сајбер безбедности. Дескриптивном методом ће, осим сајбер простора и сајбер безбедности бити описано и следеће:

- на који начин се чувају подаци који се налазе на електронским платним картицама,
- како се процесуирају подаци и
- начин на који се врши пренос података електронским путем.

2) Квантитативна и квалитативна анализа биће примењене за прикупљање података из референци, и то двојако.

- За теоретску анализу нарушавања безбедности података који се налазе на платним картицама и безбедности трансакција биће коришћени научни радови у којима су дати: преглед карактеристика CIA триаде (Протић, 2013:137-138.), опис предности и мана сајбер простора, зависност од глобалне мреже као и заштита пословних процеса, обучавање корисника и заштита информационих система, у глобалу.
- За опис легислативе биће коришћене јавно доступне информације о резолуцијама Уједињених нација), стандардима Европске уније и законима који важе у Републици Србији.

3) Студија случаја биће коришћена за приказ Diners Club International картице, који је узет као конкретан пример за наведену проблематику (DinersClub, 2017.).

2. САЈБЕР ПРОСТОР И ЗАШТИТА ПОДАТАКА У САЈБЕР ПРОСТОРУ

Сајбер простор је виртуелни простор који директно утиче на савремене глобалне токове размене различитих врста информација, а низ његових предности обезбедио је повезивање друштвене и државне инфраструктуре, и побољшало савремени живот, свакодневно функционисање финансијског сектора, организација и институција разноврсног карактера (државне институције, школе, болнице), итд.

Инциденти који се појављују у сајбер простору постају све учесталији, а сценарији сајбер напада све комплекснији, почевши од вируса којима се мењају или уништавају финансијске евиденције (Hollis, 2007.) до пласирања лажних команди којима се мењају системи нпр. контоле летења, рад нуклеарних реактора, и сл.

Сајбер безбедност је процес заштите рачунарских система од нежељене употребе, дигиталних напада и грешака у сајбер простору. Данас, сајбер безбедност се посматра истоветно као и безбедност реалног света која се односи на заштиту писане или усмено пренесене информације, јер штета која може настати као резултат сајбер напада често изазива последице у реалном свету које се мере милионским губицима, тешким преварама, утицајем на омладину и друге рањиве групе, итд.

2.1. Појам сајбер простора

Сајбер простор је међузависна мрежа информационо-комуникационих и технолошких структура које обухватају Интернет, телекомуникационе мреже, рачунарске системе, и уграђене процесоре и регулаторе у разним делатностима (Buckland, Shierer & Winkler, 2004:9). Сајбер простор односи се и на сваку структуру у којој постоји хардвер, софтвер и опрема коју је могуће малициозно искористити. Треба бити свестан да, иако је сајбер простор виртуелан, у њему не сме да постоји мања толеранција на заштиту података, у односу на ниво заштите која се среће код коришћења и заштите не-електронских података.

Сајбер простор директно утиче на нове моделе образовања, информисања, побољшавање здравственог система, енергетску оптимизацију, одговорније управљање, принципе међународне сарадње, глобалне токове у сваком погледу, итд. Очигледне предности сајбер простора обезбедиле су повезивање друштвене и државне инфраструктуре, финансијског сектора и других сегмената друштва, што је, истовремено, изазвало

међусобну повезаност и зависност од глобалне мреже (Радуновић, 2015:4). Из тог разлога све предности које прате сајбер простор прате и претње везане за његову безбедност. Због сајбер криминала светска економија трпи велике губитке, постоји низ примера о крађама персоналних података, фалсификовању докумената, крађи софтвера, дечијој порнографији, сајбер тероризму, хакерским нападима, креирању и дистрибуцији вируса путем интернета, итд. (Pande, 2017:23). Сценарији напада крећу се у распону од уништавања финансијске евиденције и успоравања рада берзи (Hollis, 2007:1024-1025), преко угрожавања енергетских система (Мијалковић, 2011:213), до пласирања лажних порука и команди којима се ремете нпр. системи контроле летења (Милошевић, Матић & Миљковић, 2018: 542).

У свом раду, Путник и др. (2017:176-177), описују и сајбер односно виртуелни рат, који је нов вид сукоба са специфичним обележјима чији је основни принцип - сајбер ратовање има конкретне последице у реалном свету. Аутори такође указују на тезу Davida Bibighausa (2015.) који пише о разликама у промишљању у реалном свету у којем важи теорија случајности, односно понашање по Гаусовој расподели и у сајбер окружењу, које функционише по експоненцијалној расподели. Због физичке структуре - топологије комплексних рачунарских мрежа са огромним бројем чворова и преносних путева откривено је да у већини случајева оне имају Парето расподелу са експоненцијалним репом (Главинић, 2007:1). Исти принцип важи и за расподеле код web страница (Barbasi & Frangos, 2002:66).

Уколико се узме у обзир све наведено, могуће је закључити да постоје оправдани разлози за страх од последица које би напад на значајне информације, уколико се изведе у сајбер простору, могао да изазове као штету са последицама које би значајно могле да утичу на рад компанија или функционисање система у одређеним организацијама. Из тог разлога, водеће државе у свету показују растућу свест о потреби деловања с циљем повећања сајбер безбедности у сајбер простору. Постоје државе које имају дефинисане националне стратегије сајбер безбедности и успостављене системе којима се бране од сајбер криминала. У датим стратегијама, сајбер претње дефинисане су као најзначајније претње 21. века.

2.2. Карактеристике сајбер простора

Сајбер простор је виртуелни простор базиран на информационо-комуникационим технологијама, који карактеришу хардверско-софтверска структура и комуникационе везе

(Протић, 2013:135.). Сајбер простор је концептуално решење које подразумева и сваку структуру у којој постоји хардвер, софтвер, опрема и преносни путеви (жичне или бежичне везе) које је могуће малициозно искористити.

Иако виртуелан, сајбер простор има карактеристику комплексног окружења које је настало интеракцијом људи, софтвера и сервиса Интернета, уз помоћ технологије и повезаних мрежа које не постоје у физичком облику али имају директан утицај на ефективно глобално пословање, интернационалну комуникацију, отварање нових радних места у ИТ домену, итд. (Јонев, 2016:207).

Уместо термина *сајбер простор*, користи се и термин *сајбер окружење* које подразумева процесе, информације и комуникацију у директној или индиректној вези са мрежама. Карактеристика сајбер простора је употреба електромагнетског спектра за чување, модификацију и размену података електронским путем односно технологијом подржаног окружења у којем се информације генеришу, размењују или складиште.

У сајбер простору, сајбер активности и претње различите државе посматрају на различите начине. У основи, постоје две струје и концепције разумевања ових појмова, прозападна коју пропагирају влада и оружане снаге Сједињених америчких држава (САД), и происточна под утицајем Шангајске организације за сарадњу, коју предводе Руска федерација и Кина (Hathaway & Crootof, 2012:8).

2.3. Појам, дефиниција и карактеристике сајбер напада

По Националном савету САД за истраживање, сајбер напади су *„намерне акције којима се мењају, ометају, обмањују, деградирају или уништавају рачунарски системи, мреже или информација, као и програми који бораве или пролазе кроз ове системе или мреже“* (Owens, Dam & Lin, 2009.). На другој страни, Шангајска организација усвојила је ширу дефиницију сајбер напада и дефинише *„информациони рат“*, као *„масовно психолошко испирање мозга у циљу дестабилизације друштва или државе, као и ради притисака на државу да доноси одлуке у интересу неке супротне стране“* (Милошевић, Матић & Миљковић, 2018: 543). Шангајска организација усваја ширу визију сајбер напада у којој укључује употребу сајбер технологија за нарушавање политичке стабилности што, по западним коментаторима, представља начин да се оправда цензура политичког говора на Интернету.

2.4. Електронске трансакције путем Интернета и безбедносни ризици

Интернет је саставни део друштвене свакодневице који обухвата како комуникацију, пословање, трговину, образовање, културу, здравство, дипломатију, критичне инфраструктуре, друштвене интеракције, забаву, тако и традиционалне делатности као што је нпр. пољопривреда. Интеграција Интернета у све сегменте друштва чини да сајбер простор постаје кључна компонента свакодневног, реалног окружења (Јонев & Бериша, 2015:170). Умрежавање предузећа и развој јавне администрације довео је до великих промена у начину и ефикасности пословних система, изменили су начин и ефикасност рада, и обезбедили брзу и једноставну размену података, једноставно ажурирање софтвера и докумената, мултимедијални приступ, директно плаћање електронским путем, итд (Стојановић, 2009:4). Развијени су нови облици пословања (електронско пословање) и трговине (електронска трговина), који су базирани на облицима пословних трансакција и размену информација који се изводе коришћењем информационе и комуникационе технологије (Кончар, 1998.). Много је предности у пројектовању пословних процеса, реинжењерингу, и дељењу информационих ресурса. Побољшана је конзистентност, интегритет, независност и дељење података (Његуш, 2010.). Интернет је данас основа за размену података свих врста, а трансакције преко Интернета постале су најбржи начин комуникације корисника са банкама или картичарским организацијама (Милосављевић, Веиновић & Грубор, 2009.). Куповина електронским путем постала је најпрофитабилнији облик трговине због једноставности и малих трошкова, а коришћење Интернета је, између осталог, обезбедило плаћање електронским платним картицама.

И поред низа предности и великог потенцијала, Интернет оставља простор за низ злонамерних активности које су, последњих година, доводиле до значајних финансијских губитака, уништавања имовине или губитака живота (Ризмал и др., 2016:15-18). Електронска инфраструктура осетљива је на различите врсте напада. Са економске тачке гледишта, последице злоупотребе или отказа техничке природе могу бити: директни финансијски губици, губљење вредних и поверљивих информација, неовлашћена употреба ресурса, губљење пословног угледа и поверења, итд. Ризици које са собом носе електронске трансакције могу се избећи мерама безбедности, које су или технолошке (аутентификација, заштита интегритета, поверљивости и расположивости података) или процедуралне (процес приступа ресурсима или информација) (Вујовић, 2005.).

У тексту који следи биће описан значај пословања и могућности злоупотребе електронских платних картица

3. ЕЛЕКТРОНСКЕ ПЛАТНЕ КАРТИЦЕ

Интернет је променио класичан начин пословања јер је утицао на развој нових система и рачунарских мрежа у којима учетвују и трговци и корисници и банке. Појавила се нова техника дистрибуције банкарских услуга и омогућено је плаћање рачуна електронским путем (Шкорић, 2015:12). Електронско банкарство омогућило је интензивно коришћење рачунарских мрежа, уз постојање великог броја провајдера који својим клијентима омогућују приступ новцу у било којем тренутку, коришћењем једног од средстава плаћања која могу бити:

1. електронске платне картице,
2. електронски чекови,
3. дигитални новчаници са електронском готовином или
4. средства плаћања уз потврду одн. гаранцију треће стране од поверења (Симић, 2018.).

Платна картица је посебан начин безготовинског плаћања, коју издаје банка, трговачка или картичарска организација која омогућује власнику картице да измири своје трошкове продавцу или извршиоцу услуге (Шкорић, 2015:12-13).

3.1. Појам, значај и карактеристике електронских платних картица

Платна картица је инструмент безготовинског плаћања који кориснику омогућује да плати робе и услуге или подиже готов новац а, у зависности од намене, и издавача платних картица оне не морају бити назване искључиво као платне[3], него могу бити и EMV[4] чип картице, дебитне картице, кеш картице, итд. (НБС[5], 2007:2). У сваком случају, оне су замена за готов новац, са опцијом кредитирања, добар су борац против губитка кеша и, уз ограничење у смислу валуте, постоји могућност да се плаћање извршава свуда у свету.

Предности платних картица су вишеструке како за кориснике картица, тако и за трговце и банке које их издају, а могу бити следеће:

[3] Payment, енгл.
[4] **E**uropay **M**aster **V**isa
[5] Народна банка Србије

1. За кориснике је знатно сигурније користити платне картице уместо чекова, смањен је ризик од губљења готовине, већа је доступност средстава са рачуна, итд.
2. За трговце су платне картице поузданије од чекова, повећана је потрошња у односу на кеш, и лакше је управљање средствима.
3. Банке на овај начин смањују трошкове пословања са готовином, добијају најбоље средствао за кеш кредите, итд. (Шкорић, 2015:14).

Данас није познато колико има платних картица у свету, али се процењује у свету постоји преко 2 милиона банкомата (Суботић, 2010.). Поверење у електронске картице заснива се на општем прихватању овог начина плаћања.

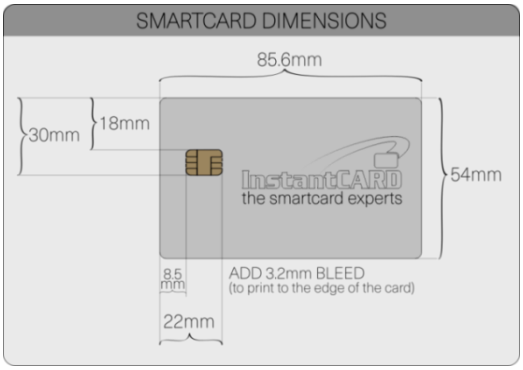
Разликујемо четири основна типа електронских платних картица:

1. чековне,
2. дебитне,
3. новчане и
4. кредитне (Балтић, 2014:6-7).

Такође, постоје две врсте картица:

1. класичне (са магнетном траком или пластичне)
2. интелигентне картице (са чипом) (Андрејевић, 2011: 40-41).

Димензије и карактеристике картица дефинисане су стандардом ISO/IEC 7810[6]. Сликом 1. приказан је изглед картице по овом стандарду. Димензије картице су: (1) 85.60x53.98x0.76mm (најчешће коришћена картица), (2) 125x88mm (за пасоше и визе), итд. Стандардом су дефинисани и отпорност на савијање, влагу, пламен, хемикалије, температуру и влажност ваздуха, и дозвољен ниво токсичности.



Слика 1. Стандардна платна картица
(Извор:http://saman.cinetonic.co/id-cards-size/, 2018.)

[6] ISO/IEC 7810:2003 Identification card – Physical characteristics; ISO – International Organization for Standardization; IEC – International Electrotechnical Comission.

Постоје и друге врсте картица, као што су:

1. картице са личним печатом клијента (разноврсних димензија са сликом у углу или преко целе картице),
2. мини картице (димензије су 40% од димензија стандардне картице, искључиво за POS терминале),
3. картице са батеријом (са струјним колом, прекидачем, екраном и батеријом чији је рок трајања дужи од рока валидности картице) (Ђорђевић, 2009:4), и
4. картице нестандардних облика (за посебне намене) (Ђорђевић, 2009:8-10).

Функције свих платних картица могу се сврстати у следеће групе (НБС, 2007:7-8):

1. гарантно средство плаћања,
2. средство идентификације за подизање готовине на самоуслужним шалтерима и банкоматима,
3. средство за телеплаћање,
4. средство за обављање малопродајне куповине,
5. средство за електронско потписивање и
6. средство за коришћење преносне новчане датотеке.

Концепти плаћања картицама такође се могу сврстати у групе (Васковић, 2008:146):

1. прво плати – картице са меморисаном монетарном вредношћу (при пејд), које се још називају и електронски новчаници,
2. плати сада – дебитне картице које омогућују да се одговарајућом апликацијом изврши пренос средстава са рачуна (штедног или чековног) корисника дебитне картице,
3. плати после – кредитне картице са апликацијом за повлачење готовине до предефинисаног лимита чиме је, уствари, кориснику картице одобрен кредит.

У пословању са картицама учествују (Шкорић, 2015:23):

- картичне организације (VISA, MasterCard (MC), Diners, American Express (Amex), Discovery, Dina),
- банке (банка издавалац и банка прималац),
- процесори (компаније које обезбеђују техничке услове за коришћење и обраду платних картица, и успоставу везе између банке и картичне организације),
- трговци,

- произвођачи опреме и
- корисници.

3.2. Типови платних картица

У тексту који следи описана три типа електронских платних картица (Шкорић, 2015:25):

1. картице са магнетном траком,
2. SMART картице и
3. бесконтактне картице.

Ове електронске картице служе за обављање финансијских трансакција и плаћање без употребе готовог новца. На овај начин постижу се велике уштеде у пословању, јер се штеди како у пословима, тако и у смањењу физичких ресурса компанија, потребом за папирном документацијом, итд. (Андрејевић, 2011:47-48.).

3.2.1. Картице са магнетном траком

Стандардне картице са магнетном траком имају три стазе (Слика 2.), односно садрже три податка:

1. BIN[7] (идентификациони број банке),
2. PAN[8] (број рачуна) и
3. PIN[9] (лични идентификациони број власника рачуна). PIN је шифра приступа и садржи и контролни број који се рачуна по Луновом алгоритму који је јавно доступан (Шкорић, 2015:26.).

Подаци који се налазе на овој картици могу се оштетити или мењати, тако да се картица користи искључиво као меморијска, без уписивања података. У општем случају, картице са магнетном траком је лако фалсификовати и злоупотребити и поред уграђених заштитних механизама.

[7] Bank Identification Number
[8] Personal Account Number
[9] Personal Identification Number

Слика 2. Картица са магнетном траком
(Извор: Simović, B., 2014.)

3.2.2. Интелигентне – SMART картице

Постоји низ разноврсних *паметних* картица, односно SMART[10] картица, као што су: меморијске, контактне, картице са интегрисаним колом, картице са микропроцесором или комбиноване (Слика 3.). Ове картице се, поред плаћања, користе и за идентификацију, а њихова примена смањује злоупотребу неколико пута. Ове картице су биле полазна основа за развој електронског новца. Прву верзију SMART картица чине чип-картице са могућношћу уписа и читања података, који не могу да се мењају. Следећа верзија имала је могућност ажурирања (НБС, 2007:2-4.). Картице са мкропроцесором имају могућност аутоматске обраде података и криптографију, а мобилни телефони добили су могућност обраде, као бесконтактне картице.

Према намени SMART картице се деле на (Patrika, 2018.):

1. једнонаменске, за куповину једне врсте роба или услуга, или куповину код једног трговца и
2. вишенаменске, које се користе за куповину врше врста роба или услуга код различитих послодаваца.

Слика 3. SMART картица
(Извор: patrika, 2018.)

[10] SMART (енгл.) - паметан

Конфигурацију SMART картице чине:

1. микрорачунар са процесором,
2. меморија са оперативним системом,
3. меморија која се користи у току обраде,
4. меморија са бројем рачуна, сертификатом и кључевима и
5. меморија са промењљивим подацима (Ђорђевић, 2009:11).

Интегрисано коло и чипови су саставни део картице, а контакти на картици су веза са напајањем и подацима. SMART картицу чини паметном интегрисано коло на коме се налазе процесор, радна меморија и програмабилне меморије. Када се картица убаци у терминал њено напајање се изводи преко терминала, а целокупна комуникација одвија се преко једног од контаката (Ђорђевић, 2009:12-15).

3.2.3. Europay Master VISA стандард

Микропроцесори SMART картица омогућили су настанак електронског новчаника, већу безбедност и мобилно банкарство. Компатибилност је обезбедио договор између Europay, Master и Visa компанија, па је 1999. године прихваћен EMV стандард картице која садржи и магнетну траку и чип. На овај начин се дефинише интеракција између физичке структуре картице и реализације трансакција дебитном или кредитном картицом (НБС, 2017:2-4).

3.2.4. Бесконтактне картице

Напредна верзија SMART картица су бесконтактне картице (Слика 4.), које у себи садрже антену која прихвата сигнал са читача. На овај начин не захтева се контакт са терминалом.

Слика 4. Бесконтактна картица
(Извор: patrika, 2018.)

Картице могу имати форму класичне картице, али могу бити и уграђене у привеске, стикере, накит и сл. Време које је потребно да се обави трансакција бесконтактном картицом је око 25% дуже него у другим случајевима. Картица мора да се налази на одаљености мањој од 3cm од читача, да би пренос функционисао (Ђорђевић, 2009:8). Поред овог недостатка, још један од недостатака је висока цена. Поред тога, потребна је и неопходна инфраструктура за примопредају. Међутим, основна предност картице је у томе што се PIN не објављује другима, односно, не захтева се његов унос, па је избегнута обрада ове врсте података.

3.3. Терминална опрема

Терминална опрема служи као периферија за електронску комуникацију корисника са банком или картичарском организацијом. Терминалну опрему чине банкомати и POS терминали.

3.3.1. Банкомат

Банкомат[11] је уређај са периферијама за: (1) издавање новца, (2) штампање рачуна, а садржи (1) монитор, (2) тастатуру и (3) комуникациони систем. Такође, банкомат има и оклопљено кућиште са сефом. Банкомат је повезан за банку прихватиоца захтева, и подразумева телекомуникациону примопредају захтева, као и одобрење захтева (Андрејевић, 2011:16). Револуцију у банкарском пословању започела је још 1967. године Barclays банка. Уместо платних картица које су данас у употреби, овај банкомат је могао да препознаје чекове. Банкомат је настао као надоградња машине за продају чоколадица јер је његов аутор, инжењер John Shepherd-Byron дошао до закључка да би на исти начин као што постоји *испорука* чоколадица могла да ради машина за испоруку новца. Савремени банкомати појавили су се као резултат истраживачког рада фирме IBM неколико година касније, 1972. године, када је први такав уређај инсталиран у Енглеској. Сликом 5. приказане су различите врсте банкомата.

[11] Банкомат се среће и под називом ATM, што је скраћеница за аутоматски бројач: **A**utomated **T**eller **M**achine (енгл.)

Слика 5. Терминална опрема. Банкомати.
(Извор: Андрејевић, М., 2011:14)

Према подацима Удружења за производњу банкомата ATM, данас на планети постоји преко 3 милиона инсталираних банкомата, а највећи произвођачи у свету су Wincor Nixdorf, NCR и Debloid. Приказ у процентима, и у односу на друге произвођаче, са уделом ових произвођача на тржишту је дат Сликом 6.

Слика 6. Удео произвођача банкомата на светском тржишту
(Извор: http://ivicadj.com/2016/09/sta-sve-atm-bankomat-moze-u-2016/, 2016.)

Банкомати се деле у две групе Cash Out (за исплату новца) и Cash In (за прихват новца), с тим да овај други може, поред класичног облика (новац се похрањује као у сеф) имати и облик банкомата ‘за рециклажу’ који омогућује кориснику да уплати веће своте новца, а онда их користи по потреби.

Још једна од подела банкомата је на оне који су уграђени у зид[12] и оне који нису уграђени у зид[13].

Банкомат има и низ погодности за корисника (Андрејевић, 2011:17-18):

1. аутентификација препознавањем PIN-а, или са биометријским методама аутентификације,
2. уплата новца на банкомат:
   a. опција за трговце који на овај начин не морају да предају пазар у банку;
   b. размена валуте (мењачки послови); банкомати су опремљени уређајима за препознавање фалсификованих новчаница;
   c. рад 24/7;
3. банкомат може да ради као:
   a. е-банкинг уређај (ово је напредна верзија банкомата са посебном тастатуром, а корисник приступа свим својим рачунима),
   b. може извршавати опције сличне m-банкингу или Интернет пословању као што су уплата новца на рачун, пребацивање средстава са рачуна на рачун, новчане трансакције, итд.

У зависности од банке, банкомат може да има и друге погодности као што су:

1. плаћање услуга куповине карата (концерти, биоскопи, позоришта),
2. допуна при пејд кредита,
3. плаћање рачуна,
4. штампање мини-извода,
5. могућност одобравања кредита, итд.

Од банака такође зависе дозвољени лимит за подизање новца, вредност апоена, издавање идентификационог броја, начин комуникације са корисником, итд.

Безбедност је једна од оптицаја која се увек поставља пред кориснике банкомата. Ова тема посебно је описана у поглављу које следи. Сликом 7. приказана је напредна верзија банкомата са биометријским очитавањем Ogaki Kyoritsu Banke из Јапана.

[12] Through the Wall (енгл.)
[13] **L**obby (енгл.)

Слика 7. Банкомат са биометријским очитавањем
(Извор: https://www.muskiportal.com/, 2012.)

3.3.2. POS терминал

POS терминал је електронски уређај који омогућава прихват, односно плаћање платним картицама на продајном месту. Операције које се изводе путем POS терминала су: прикупљање података са картице и износа трансакције, повезивање на банку – прихватиоца, и штампање рачуна по одобрењу трансакције. Сликом 8. приказан је преносиви POS терминал.

Основна предност овог терминала је мултифункционалност која посебно одговара продавцу робе или услуге. Купци нису ограничени традиционалним начином плаћања па се промет значајно повећава, наплата се брзо реализује, а контакт са банком је релативно једноставан. Наплата трансакција се одвија аутоматски, и нема потребе за посебним одласцима у банку. Трансакције је, такође, лако контролисати, а извештаји о трансакцијама су стално доступни.

Слика 8. POS терминал
(*Извор: Андрејевић, М., 2011:16.*).

Посебне погодноси POS терминала су и:

1. прихватање више врста и типова платних картица,
2. плаћање на рате,
3. предауторизација (за хотеле и Rent-a-Car агенције) и
4. могуће повезивање на електронску касу (Андрејевић, 2011: 16.).

Уређај се повезује путем класичне телефонске линије, али и мобилне телефоније. Такође, уређај може бити повезан у локалну мрежу продавца.

Врста уређаја и модел се бира према његовој намени, у складу са потребама особе која ће га користити или система у који ће бити укључен (Васковић, 2007.).

У понуди POS терминала они су, најчешће, конфигурисани тако да прихватају Dina, VISA и Maestro/Master картице, уз опције додавања других картица, што се посебно уговора са свим учесницима у пословању са картицама (Андрејевић, 2011:15-16.).

4. ЗЛОУПОТРЕБА И ЗАШТИТА ЕЛЕКТРОНСКИХ ПЛАТНИХ КАРТИЦА И ЕЛЕКТРОНСКИХ ТРАНСАКЦИЈА

У раду са електронским картицама велика пажња се поклања заштити података о кориснику картице, финансијским трансакцијама, али и процесуирању података, њиховом смештању на одговарајуће медије, итд. У општем случају користе се стандарди безбедности, а конкретно везано за картице користе се PCI[14] стандарди[15]. PCI стандарди за безбедност платних картица односе се на милионе људи широм света што, на једној страни, доноси компатибилност издатих картица и терминала (глобално), а на другој омогућује *стандардизацију* малициозности.

PCI стандарде доноси Савет, односно веће PCI. Савет PCI је стандардизациона организација коју су 2006. године основали American Express, Discover, JCB International, MasterCard и VISA Inc., који имају подједнако учешће и раду савета (PCI Security Standard Council, 2006.). Ово веће има два приоритета:

1. да помогне трговцима и финансијским институцијама да схвате и имплементирају стандарде за безбедност у пословним политикама, технологијама и одговарајућим процесима који штите њихове платне системе од претњи које могу да изазову власници картица, и
2. да помогне продавцима да схвате и примене стандарде како би креирали безбедна решења за плаћање.

Поред PCI заштите, област заштите електронских картица подразумева и ИТ безбедност, безбедност података и (евентуално) додавање оних елемента у заштити који ће послужити за откривање или праћење напада односно напада у ширем смислу, у сврху санкционисања потенцијалних нападача[16]. ИТ безбедност подразумева заштиту процесуирања информација у систему против малициозне манипулације и економске штете да би се минимизовали ризици напада на поверљивост, интегритет и доступност информацијама.

---

[14] PCI Compliance – Payment Card Industry (енгл.), низ закона; Payment Card Industry – Индустрија платних картица (превод са енглеског)

[15] PCI Data Security Standards (DSS) – постоје три верзије стандарда са корекцијама, прва верзија PCI DSS 1.0 -1.1 је објављена 15.12.2006., са ревизијом 1.1 из септембра 2006. Верзија PCI DSS 2.0 ступила је на снагу у октобру 2010. године. Верзија 3.0 важи од новембра 2013., а њена последња модификација PCI DSS 3.2.1 на снази је од маја 2018. године (PCI Security Standard Council, 2018.).

[16] Овај израз на енглеском гласи: eDiscovery (електронско откриће)

Да би била обезбеђена заштита, мора да постоје технички и организациони услови, и мере којима се гарантује да неће долазити до погрешног коришћења или губитка података у процесу обраде, преноса или складиштења.

eDiscovery је релативно нова техника, из тог разлога јер су декларације о законским санкцијама у сајбер свету релативно нове. Овај начин заштите је, уствари, трагач, који омогућује да подаци буду лоцирани, обезбеђени, и претраживани, с намером да се користе као докази у званичним (правним) ситуацијама или као докази криминалних активности[17].

У тексту претходног поглавља наведене су препоруке корисницима како да сачувају платне картице у ситуацијама у којима сумњају да може доћи до крађе PIN-а, сумњивих трансакција, итд. Тема овог поглавља је други вид заштите који се може поделити на: (1) физичку односно хардверску заштиту структуре картице, и (2) заштиту стофтвера и трансакција између корисника, терминалног уређаја и банке, односно издаваоца картице.

4.1. Заштита физичке структуре платне картице

Картице се могу поделити у четири групе:

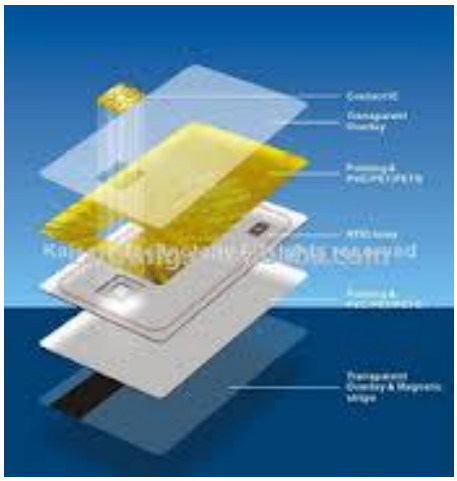
1. према изгледу – глатке или ембосиране;
2. према запису – са магнетном траком или са чипом;
3. према примени – међународно валидне, националне и корпоративне;
4. према року доспећа – кредитне, дебитне, новчане и електронске (Бабовић, 2015:64.).

Структура једне хибридне картице која садржи и магнетну траку и чип приказана је на Слици 9. Део са магнетном траком је контактни део картице, а чип представља њен бесконтактни део. Доњи слој картице је магнетна трака са меморијом и делом за потпис корисника, који је утиснут на пластичну фолију. У наредним слојевима постоји основа за чип, микропроцесор са електричним колом, меморијама за чување, обраду и измену података, и антеном. На последњем слоју се налази сам чип (Bulanan, 2014).

Сваки од физичких делова картице може бити оштећен намерно или ненамерно сечењем, стругањем, излагањем високој или ниској температури, киселини и сл. Микропроцесор и електронски делови картице могу бити уништени и високим напоном. Међутим, у овим случајевима, картица није елемент злоупотребе података, него је у питању класично

[17] На енглеском језику овај израз има облик: For the purpose of obtaining critical evidence.

физичко оштећење које захтева њену замену. Малициозности су, углавном, везане за софтвер и трансфер података, односно трансакције, у случају електронског плаћања.



Слика 9. Структура хибридне електронске картице
(Извор: www.ChinaCardMfg.com, n.d.)

4.2. Злоупотреба података са платне картице

У примерима који следе биће описана контактна и бесконтактна крађа идентификационих бројева и података корисника платних картица.

4.2.1. Злоупотреба контактних платних картица

Сликом 10. приказан је скиминг. У питању је примена савременог, и релативно једноставног уређаја који се ставља на банкомат, али је, уствари, склоп који се ставља на постојећи део за унос картице и на тастатуру, као додатак.

Слика 10. Скимер
(Извор:http://www.cwbchicago.com , 2018.)

Иако релативно једноставан принцип, малициозност скимингом је тешко открити, а то се најчешће дешава кад корисник открије недостатак средстава на рачуну и интервенише код банке. По уговору који корисник потписује захтевом за издавање картице банка се одриче одговорности за овакве случајеве. Добро у целој ситуацији је то што је на банкоматима постављен дневни лимит.

Модерни банкомати користе активне анти-скиминг уређаје који емитују ометајући сигнал и на тај начин онемогућавају рад скимера. На Слици 11. приказан је скимер који се често користи код плаћања на бензинским пумпама, ишчитавањем PIN-а са картице.

Слика 11. Скимер PIN-а картице за плаћање горива
(Извор: https://krebsonsecurity.com/tag/gas-pump-skimmers/, 2018.)

4.2.2. Злоупотреба бесконтактних платних картица

Бесконтактни читачи картица обесмишљавају скиминг, па се могућност злоупотребе овим путем значајно смањује. Међутим, постоји тзв. замка за кеш, која спречава испату новца кориснику. Заштита модерних банкомата је изведена њиховим дизајном.

Основа код малициозног напада на бесконтактну платну картицу је прићи особи неком врстом скенера. Битно је да уређај има пријемну антену и да се налази довољно близу картице коју ће скенирати (отприлике до максималне удаљености од 15cm), најчешће се то изводи мобилним телефоном.

Сви подаци који се односе на каритцу налазе се у чипу, који има предајну антену, која одашиље податке пријемној антени, уколико се нађе у близини. Из тог разлога, особа која скенира бесконтактну картицу мора да се приближи особи која врши подизање новца или плаћање. Иако су бесконтактне картице такве да маскирају податке о кориснику, постоје софтвери којима се ови подаци лако екстрахују. Нападач може да се приближи и у ходу, држећи у руци ‘скенер’. Очитавање података је могуће и када се картица налази у новчанику или торби (Bichoff, 2016.). Постоји једноставан трик да се овакав проблем реши. Картица се увије лаком фолијом која значајно смањује домет предајне антене. Код малициозног напада, нападач не може да очита картицу.

5. САЈБЕР БЕЗБЕДНОСТ

Сајбер безбедност обухвата изазове који прелазе државне границе, док одговори на ове изазове који су, уз то, и недовољни, остају у државним видокруговима. Евидентне су празнине у разумевању проблема сајбер безбедности како у техничким тако и у системским способностима да се са њима изборимо.

Од 1860. године, када је прву електронску трансакцију извео Western Union (помоћу телеграфа) сајбер безбедност постаје све актуелнији проблем. Када је решавање пораста обимне папирологије и платног промета почело да буде замењивано рачунарским трансакцијама, промениле су се и методе и техничка решења за трансакције, али је суштина концепта остала иста (Барјактаревић, 2012:12). Интернет је увео значајне промене како у свакодневни живот, тако и у начин пословања банака (Online Интернет трансакције, трансфер са рачуна на рачун, плаћање рачуна) па, у том смислу, сајбер безбедност данас можемо посматрати и кроз заштиту информација (веродостојност, правовременост, актуелност, поузданост, релевантност, тајност) (Спасојевић, 2013:23).

Једно од нарочитих обележја сајбер безбедности је што је, у огромном броју случајева, тешко идентификовати починиоце напада. Појединац или група сајбер нападача могу прикрити властиту умешаност у напад или могу да се „преруше“ у другог корисника (Markoff, Sanger & Shanker, 2010.). Зато што је нарочито тешко утврдити извор напада тешко је и спречити даље наношење штете (Libicki, 2009.).

Један од највећих изазова, везан за претходно наведену чињеницу, је и чињеница да, док су владе у извесној мери одговорне за информационо комуникационе мреже, власници тих мрежа су, углавном, приватни актери.

Посебне потешкоће у овом домену представља и глобална природа како проблема сајбер безбедности тако и његовог решења (Wood & Dupont, 2006.). Управо из тог разлога ово је подручје у којем међународни актери имају велики утицај што се односи на развој међународних стандарда, идентификацију најбољих пракси, подстицање хармонизације међународних прописа о истрази, гоњењу, чувању података, заштити приватности, приступу одбрани мрежа и одговору на нападе. У тексту који следи биће посебно речи о заштити података у сајбер простору и, посебно, о заштити електронских платних картица и заштити електронских трансакција од злоупотребе.

5.1. Зштита података у сајбер простору

Заштита података или информација, односно безбедност информација[18] је низ стратегија и поступака којима се обезбеђује превенција, детекција и документовање претњи и напада на дигиталне или не-дигиталне податке. Задаци заштите података укључују успостављање низа пословних процеса који штите све делове информационог система без обзира на формат информације и то да ли се она преноси, обрађује или складишти (Rouse, 2016.). Основа заштите је обезбедити следеће:

1. да подаци буду доступни искључиво ауторизованим особама (поверљивост података),
2. превенцију од неауторизоване модификације података (интегритет) и
3. гаранцију да ће подацима приступити искључиво ауторизоване особе, на захтев (доступност).

Уколико се посматра са овог становишта, принципи информационе безбедности (ИБ), у информационо-комуникационим системима, могу бити водич онима којима је потребна помоћ да одговоре на изазове које носи савремена дигитална комуникација што, у ствари, значи побољшавање технологије безбедности и едукацију персонала/корисника да креирају окружење у којем могу безбедно да користе рачунарске ресурсе (ISACA, 2017.).

Дакле, сајбер безбедност представља низ поступака и процеса којима се штите информације у сајбер простору.

Из наведених разлога, сајбер безбедност се (више) не посматра одвојено од безбедности у реалном свету, јер штета настала као резултат сајбер напада изазива стварне последице у физичком свету. Врсте напада, повезаност са коришћењем савремених технологија, као и починиоци и жртве напада, захтевају посебну врсту надзора и бриге да би биле спречене могуће последице по особу или информациони систем (делимично или у целости).

Сајбер безбедност је изазвала пажњу друштва оног момента када се, због великог броја корисника, показало да технологија може да буде једнако корисна, бескорисна или претећа.

[18] Information Security; InfoSec (енгл.)

Сајбер безбедност одређују три параметра:

1. акција која се изводи (пресретање, ометање, илегални приступ подацима, шпијунажа, саботажа, ускраћивање услуга, крађа идентитета)
2. врста починиоца напада (хакери, сајбер криминалци, сајбер терористи)
3. циљ напада (компаније, институције, појединци).

Кривична дела која настају као последица ових напада дефинисана су домаћим и страним законима и регулативама, а наведена су и упоређена у тексту који следи (Мирковић, 2017:47).

5.2. Заштита електронских платних картица и електронских трансакција од злоупотребе

Као плод банкарске праксе, електронске платне картице од њиховог настанка средином прошлог века, до данас постају све распрострањенији инструмент плаћања који је потиснуо друге инструменте плаћања, као што су нпр. чекови (Koch, 2010.). Тренд плаћања платним картицама, указује на њихов велики значај у банкарском платном промету, а тиме и на значај које картице имају за кориснике. Из тих разлога, платне картице су у последње две деценије изазвале посебну пажњу законодаваца који настоје да обезбеде регулативу како би заштитили и кориснике картице и банкарско-картичарске организације. Циљ регулативе је заптитити безготовински платни промет, интересе трговаца, банака, издавалаца и ималаца картица (Вуковић & Радовић, 2014:69).

У раду са електронским картицама велика пажња се поклања како заштити података о кориснику картице и финансијским трансакцијама, тако и о процесуирању података, њиховом смештању на одговарајуће медије, итд. Велики део заштите електронске платне картице налази се у њеној структури и у намени коју има (чековне, дебитне, новчане, кредитне картице). У овом случају примењују се PCI стандарди безбедности који се односе на компатибилност издатих картица и терминала на глобалном нивоу. PCI стандардизација обезбедила је и да се смањи ризик од физичког напада као што је нпр. промена температуре, фреквенције и напона напајања. Поред тога, примењују се мере заштите од логичких напада (испитивање одлазног и долазног саобраћаја ради стицања увида у трансакције), вируса, тројанских коња, непажње корисника и администратора, и сл. (Ђорђевић, 2009:16).

У комуникацији која подразумева новчану трансакцију, за заштиту информација користи се вишенивоовска архитектура у безбедносном систему, односно вишеслојна архитектура заштите. За приступ корисника одређеној апликацији у систему тражи се његова идентификација (user id, user name), аутентикација/аутентификација (password, PIN) и ауторизација (уколико је у питању нпр. службено лице).

Електронске трансакције често се изводе коришћењем платних картица које се могу злоупотребити на низ начина почевши од погрешног руковања картицом, преко пресретнутих банкарских трансакција, до малициозних злоупотреба и слично. Такође, могућа је злоупотреба код трговине путем Интернета, пријема или предаје налога за плаћање роба и услуга електронским путем, и сл. Интернет трансакција изводи се Интернет трансакционим сервером[19], интерфејсом који обезбеђује ефикасну комуникацију између апликационог и web сервера, контролише проток података и обезбеђује приступ Интернету.

Злоупотреба платне картице означава употребу оригиналне или фалсификоване платне картице од стране неовлашћеног лица. Лице је неовлашћено уколико није корисник картице (налогодавац) из закљученог уговора са банком, односно ако није заступник корисника картице у овом послу (Бараћ и др., 2007:13).

Уколико је за употребу платних картица потребно њено приказивање злоупотреба је могућа уколико неовлашћено лице на било који начин дође у посед платне картице или је фалсификује преснимавањем података са магнетне траке или чипа. Уколико је уз картицу потребан потпис, злонамерник мора и да фалсификује потпис власника.

Код картица чија употреба захтева унос PIN кода, злоупотрба је могућа искључиво крађом PIN кода (погађањем, огледалом, лажном тастатуром, и сл.) (Шкорић, 2013:34-35).

Картице за плаћање путем Интернета, телефонских или каталошких поруџбина најпогодније су за злоупотребе јер је довољно да неовлашћено лице сазна податке написане на површини пластичне картице. Сазнати ове податке не представља тешкоћу имајући у виду приступ подацима који се лако могу запамтити како са картице тако и са рачуна који је плаћен том картицом (Урош, 2012:118).

[19] Internet Transaction Server (ITS)

За предузимање заштитних мера на располагању су бројни сервиси:

- тајност података остварује се шифровањем, одосно коришћењем алгоритама криптозаштите,
- аутентификацијом порука прималац има могућност да поуздано утврди идентитет пошиљаоца,
- безбедносни сервиси за заштиту интегритета података, гарантују да није дошло до промене поруке од стране неауторизоване особе,
- дигитални потпис је сервис који обезбеђује непорецивост поруке (немогућност порицања пријема поруке),
- контрола приступа је сервис који обезбеђује контролисани приступ ресурсима система (корисничка имена са тајним лозинкама, примена интелигентних картица за приступ) (Ђукић, Бјелица & Ристић, 2004.).

Треба напоменути да је битан елемент заштите електронских платних картица и електронских трансакција едукација корисника картице и особа који изводе трансакције електронским путем.

6. КРИВИЧНО-ПРАВНИ АСПЕКТИ ЗЛОУПОТРЕБЕ ПЛАТНИХ КАРТИЦА

Борба против on-line претњи захтева од држава да сајбер безбедност посматрају „изнад“ целокупне парадигме државне власти и да, уместо тога, прихвате приступ који се заснива на глобалној сарадњи. У том смислу, потребно је побољшати овлашћења и мандат релевантних надзорних органа који би требало да се изборе са сајбер претњама и рањивостима. Поред тога, неопходно је да државе донесу регулативе и ускладе их са међународним регулативама за заштиту и реакцију на сајбер нападе, итд. Путник и Бошковић (2013:128-129) указују на чињеницу да идеја парадигме сајбер безбедности реферира на „обједињене напоре и покушаје“ с циљем да се осмисле и побољшају активности везане за безбедност сајбер простора и ниво његове заштите. У том смислу, идеја је да се обухват међународног права прошири на сајбер свет, да се утврде одговорности државе за сајбер нападе и њене дужности да спречи сајбер нападе са њене територије. Аутори, такође, указују на чињеницу да нема међудржавног консензуса јер постоје супротнстављени интереси великих светских сила и по овом питању.

Значај заштите података у сајбер простору препознале су и Уједињене нације које су донеле две резолуције 55/63 и 56/121 о борби против злоупотребе информационих технологија.

Одржана је Будипештанска Конвенција Савета Европе о високотехнолошком криминалу (2001.[20]) и донет додатни Протокол који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система.

Стратегија сајбер безбедности Европске уније је један од стратешких докумената којим Европска комисија одређује свеобухватни стратешки приступ питању сајбер безбедности у Европској унији. У оквиру свог стратешког приоритета она наглашава потребу за јачањем капацитета држава чланица и приватног сектора да спрече, открију и носе се са сајбер инцидентима (Ризмал, Радуновић & Кривокапић, 2016:22).

Конвенцију и Протокол је Република Србија (РС) ратификовала 2005. године. Значај овог потписивања посебно је битан због формирања државних органа који ће бити специјализовани за борбу против сајбер криминала. У периоду од 2005. до 2009. године у законодавство Србије укључено је више прописа којима је Конвенција имплементирана у

[20] Доступно на: http://www.entel.rs/info/software/sajber kriminal-konvencija EZ.pdf

домаћи правни систем. Између осталих то су: Кривични законик[21], Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[22], Закон о полицији[23], Правилник о условима пружања интернет услуга и садржају одобрења, Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању[24], итд.

6.1. Активности Уједињених нација на сузбијању компјутерског криминалитета и резолуције 55/63 и 56/121 о борби против злоупотребе информационих технологија

Правно регулисање компјутерског криминалитета у оквиру Уједињених нација почело је 1990. године, усвајањем Резолуције о законодавству у области компјутерског криминалитета[25] (Мирковић, 2017:23). Средином 1994. године донет је Приручник УН о спречавању и контроли компјутерског криминала[26] да би, на 55. скупштини Генералне скупштине Уједињених Нација, донета Резолуција 55/63 о борби против злоупотребе информационих технологија[27] (2001.), са основним принципом – потребом за усаглашавањем законских решења на међународном нивоу. Резолуцијом је утврђено да постоји потреба да свака држава усвоји подесан законски оквир за борбу против сајбер криминала (Тренкић, 2013.). Ова врста стратегије названа је 'Safe Heavens', тј. 'Сигурна небеса'. Такође је указано на потребу за разменом података и сарадњу међу државама. При томе националне стратегије и регулација права простора треба да регулишу права појединца који користсти Интернет (у оквиру одређене територије). Ово може бити изведено надоградњом постојећих закона у областима које би се односиле на сајбер безбедности, или би било потребно увести нове законе који ће регулисати појаве везане за сајбер безбедност. Државе су, такође, упозорене да у борби против компјутерског криминалитета морају да очувају баланс између индивидуалних права и слобода

[21] Кривични законик. "Сл. гласник РС", бр. 85/05, 88/05-исправка, 107/05-исправка, 72/09, 121/12, 104/13, 94/16 (члан 243. Злоупотреба и фалсификовање платних картица)
[22] Закон о организацији и надлежности државних органаза борбу против високотехнолошког криминала. "Сл. гласник РС", бр. 61/2005 и 104/2009.
[23] Закон о полицији, "Службени гласник РС", бр. 6/2016 i 24/2018
[24] Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, "Сл. гласник" бр. 94/2017.
[25] UN resolution on computer crime legislation (1990.)
[26] United Nation Manual on the Prevention and Control of Computer-related Crime (1994.)
[27] UN resolution A/res/55/63 on combating the criminal missuse of information technologies (2001.).

гарантованих сваком појединцу с једне стране и права држава да кривично гоне извршиоце кривичних дела, са друге (Мирковић, 2017:25-26).

Овакве препоруке резултат су снимања стања о порасту одређених криминалних активности које су омогућене или олакшане у сајбер простору, као што су:

1. пораст стандардних сајбер напада типа phishing, pharming,
2. пораст кривичних дела везаних за порнографију,
3. пораст кривичних дела у намери стицања финансијске добити,
4. пораст кривичних дела у области заштићених ауторских права,
5. пораст кривичних дела прања новца, итд.

Допуњена Резолуција 56/121 о борби против злоупотребе информационих технологија[28] усвојена је на 88. пленарном заседању Генералне скупштине Уједињених нација 2002. године, а допуна се односи на поступак у коме, приликом усвајања појединих закона и политике кривичног прогона, треба да се узму у обзир и резултати рада Комисије за превенцију криминалитета и кривично правосуђе (Мирковић, 2017:25).

Једно од најактивнијих тела Организације УН данас је и Међународна телекомуникациона унија која има седиште у Женеви, у Швајцарској. Институција активно ради од маја 2007. године када је донет Меморандум о глобалној сајбер безбедности[29], с циљем стварања глобалног оквира за дијалог и међународну сарадњу приликом предлагања стратегије за повећање безбедности у сајбер простору (Мирковић, 2017:26).

6.2. Активности Савета Европе и директиве Европске уније о борби против комјутерског криминала

У време одржавања Европске конференције о криминолошким аспектима привредног криминалитета, која је одржана у Стразбуру 1976. године, покренута је прва иницијатива за правно регулисање и санкционисање компјутерског криминалитета на међународном нивоу[30] (Мирковић, 2017:16). Савет министара је, 1989. године, усвојио Препоруку о криминалним активностима везаним за употребу рачунара[31], којом су државе чланице позване да размотре увођење нових прописа који се односе на сузбијање и санкционисање

[28] UN resolution A/res/56/121 on combating the criminal missuse of information technologies (2002.).
[29] Global Cybersecurity Agenda of the International Telecommunication Union (2007.)
[30] A paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Stratsbourg, 15-18 November 1976. pp.225-229.
[31] Council of Europe Computer-related Crime Rrecommendation No. R(89) 9.

компјутерског криминалитета, а Препорука за кривично процесно право у вези са информационим технологијама[32] усвојена је 1995. године. Препорука садржи 18 принципа борбе против компјутерског криминалитета и представља први покушај дефинисања процедура проналажења и заплене, надгледања, прикупљања и оцене електронских доказа, шифровање података и установљавања принципа међународне правне помоћи у области кривичних дела компјутерског криминалитета путем сарадње држава на међународном плану.

Европски комитет за проблеме кривичног права Савета Европе је, половином деведесетих година, формирао експертску групу, Комитет експерата за кривична дела у сајбер простору[33], чији је задатак био сачињавање текста прве међународне конвенције чија би материја обухватала превенцију, хватање и кажњавање учинилаца кривичних дела из области високотехнолошког криминала.

Конвенција Савета Европе усвојена је 23. новембра 2001. године у Будимпешти, а ступила је на снагу 1. јула 2004. године (Мирковић, 2017:16-17). Разлози за доношење Конвенције су бројни:

- постојање ризика да се због дигитализације, конвергенције и сталне глобализације, рачунарске мреже и електронске информације могу користити и за извршење кривичних дела и да докази, који се односе на та дела, могу бити сачувани и пренесени преко тих мрежа,
- потреба међународне сарадње између држава због транснационалног карактера компјутерског криминалитета,
- потреба заштите легитимних интереса у коришћењу и развоју информационе технологије,
- олакшавање откривања, претраге и гоњења кривичних дела комјутерског криминалитета на националном и међудржавном нивоу,
- потреба заштите права на приватност, личних података, сопственог мишљења и слободе изражавања, итд. (Мирковић, 2017:18).

Додатни Протокол уз Конвенцију о високотехнолошком криминалу донет је 28. јануара 2003. године и ступио је на снагу 01. марта 2006. године, а односи се на расистичко и ксенофобично ширење мржње преко рачунарских система (јавно вређање преко компјутерског система лица или групе лица која се разликују по раси, боји коже,

[32] Recommendation No. R(95) 13 of the Comitee of Ministers to Member States concercing problems of Criminal Procedural Law connected with Information Technology.
[33] Comitee of Experts on Crime in Cyberspace (енгл.)

наследном, националном или етничком пореклу или вери). Основна сврха овог Протокола је инкриминација понашања која нису обухваћена Конвенцијом.

Поред тога што упућује препоруке земљама чланицама да потписују и усвајају конвенције закључака Савета Европе, ЕУ је донела низ аката чији је циљ борба против компјутерског криминалитета. У оквиру ЕУ је, 2000. године, усвојена Директива о електронској трговини[34], а 2004. године формирана је Европска агенција за безбедност мрежа и информационих система (Мирковић, 2017:21-22). Директива Европског парламента и Савета 2006/24 о чувању података који су доступни или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа[35] донета је 15. марта 2006. године са основним циљем да се ускладе одредбе држава чланица које се односе на чување јавно доступних података. Директива се примењује искључиво на податке о промету и локацији правних и физичких лица и то на повезане податке неопходне за идентификацију претплатника или регистрованих корисника.

Почетком 2007. године ЕУ је усвојила Стратегију за безбедно информационо друштво у Европској Унији[36] којом се наглашава да вредности ЕУ морају да се поштују и у сајбер свету (Ризмал, Радуновић & Кривокапић, 2016:23; Војводић, 2017.).

Европска агенција за безбедност мрежа и података објављује извештаје о сајбер инцидентима, организује радионице и подстиче унапређење јавно-приватних партнерстава. Еуропол и надлежни органи за заштиту података обављају и дају заштитно-информациону подршку у борби против сајбер криминала (Ризмал, Радуновић & Кривокапић, 2016:25). Еуропол је, такође, основао Европски центар за сајбер криминал. Циљ је успоставити сарадњу базирану на принципима добре безбедносне праксе и, што је више могуће, усвајање стандарда у области сајбер безбедности.

Представници ЕУ не позивају на креирање нових међусобних правних односа, правних аката и инструмената власти у глобалу, него се залажу за измену постојећих правних инструмената који гарантују људска права, а могу се примењивати у сајбер простору. На

[34] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market. *Official Journal of the European Communities*. L 178, 17.07.2000, pp.1-16.

[35] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communication services or of public communication networks and amending Directive 2002/58/EC.

[36] Joint Communications to the European Parlament, the Council, the European Ecconomic and Social Comitee and the Comitee of Regions Cybersecurity Strategy of the European Union. An Open, Save and Secure Cyberspace. 7.2.2013. JOIN (2013) 1 final.

овај начин, стратегије ЕУ, дефинишу скуп принципа и активности који се заснивају на заштити и промовисању права грађана.

6.3. Стратешки и правни оквир за заштиту од сајбер криминала у Републици Србији

Милошевић и Путник (2017:186) разматрају вишедимензионалност окружења сајбер безбедности и потребу за нормативном регулативом у овој сфери. Наводе да *„уколико изостану стратегије, политике, акциони планови и мере којима се имплементирају законска решења“* сви напори законодаваца остају узалудни. Аутори указују на чињеницу да је Република Србија унапредила национални правни оквир за борбу против сајбер криминала али да нису донете посебне стратегије сајбер безбедности и сајбер одбране, што указује на непостојање системског приступа решавању овог проблема.

Иако се у Републици Србији расправе на тему о компјутерским кривичним делима воде готово две деценије, регулатива везана за сајбер простор није адекватна и потпуна. Милошевић и Путник (2017:180-181) дају опис правно-нормативних оквира, материјално-правне и процесно-правне димензије супротстављања српског законодавства сајбер криминалу, кривично-правних норми, имплементације регулативе, усклађивање са Конвенцијом Уједињених нација, итд. У раду наводе да правни оквир сајбер безбедности у првом делу усклађивања са Конвенције обухвата следеће:

- прописе којима се регулишу надлежности органа за управљање безбедносним ризицима и сузбијање радњи којима се нарушава функционисање ИКТ системима;
- норме којима се регулише заштита од високотехнолошког криминала (превентивне и репресивне мере);
- кривично-правне норме као инструмент заштите од кривичних дела којима се угрожава функционисање ИКТ система и интегритет, доступност, аутентичност и тајност рачунарских података;
- материјално-правне и процесно-правне норме које је српски законодавац био у обавези да донесе због обавеза преузетих усвајањем међународно-правних

споразума (Конвенција о високотехнолошком криминалу и Додатни протокол из 2001. године)[37], итд.

Током 2003. године у Републици Србији је измењено кривично законодавство инкриминисањем кривичних дела против безбедности рачунарских података. Кривичним закоником Републике Србије је уведен појам компјутерских кривичних дела и третирање кривичних дела против безбедности рачунарских података[38]. Законодавац уводи санкционисање за готово сва кривична дела осим оних дела која се односе на пресретање комуникације електронским путем (Стојановић, 2012.). Кривични законик Републике Србије сврстава кривична дела против безбедности у сајбер простору у следеће групе[39] (приказано уз вредности минималне и максималне казне за учињено дело):

- оштећење рачунарских података и програма (новчана казна, казна затвора до 5 година) (члан 298.),
- рачунарска саботажа (казна затвора 6 месеци-до 5 година) (члан 299.),
- прављење и уношење рачунарских вируса (новчана казна, казна затвора до 2 године) (члан 300.),
- рачунарска превара (новчана казна, казна затвора до 10 година) (члан 301.),
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи или електронској обради података (новчана казна, казна затвора до 3 године) (члан 302.),
- спречавање и ограничавање приступа јавној рачунарској мрежи (новчана казна, казна затвора до 3 године) (члан 303.) и
- неовлашћено коришћење рачунара или рачунарске мреже (новчана казна, казна затвора до 3 месеца) (члан 304.) (Кривични законик, 2016.).

Поред ових, постоје и дела против безбедности деце (Ланзарот конвенција[40]), повреде ауторских права, и прикупљања персоналних података, као што су: договарање састанка са малолетном децом електронским путем, приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију, неовлашћено искоришћавање ауторског дела и неовлашћено коришћење личних података (прикупљање, преузимање и употреба), итд.

---

[37] Закон о потврђивању Конвенције о високотехнолошком криминалу, 2009. и Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, 2009.

[38] Закон о изменама и допунама Кривичног законика Републике Србије, 2003.

[39] Кривични законик. "Сл. гласник РС", бр. 85/05, 88/05-исправка, 107/05-исправка, 72/09, 121/12, 104/13, 94/16 (чланови 298.-304.)

[40] Council of Europe, Convention on the Protection of Children Against Aexual Exploatation and Sexual Abuse, CETS No.: 201, Lanzarote, the 23 October 2007.

Повезани закони и стратешки документи везани за сајбер криминал, које је Република Србија имплементирала у своје законодавство односе се и на кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат јављају рачунари, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику (Мирковић, 2017:32-33).

Други део активности законодаваца који је везан за потпуну имплементацију Конвенције УН захтевао је додатне законске реформе које су отпочеле усвајањем Закона о надлежности државних органа за борбу против високотехнолошког криминала[41] којим се прецизирају дела на која се закон примењује и уводе посебне целине у оквиру тужилаштава и судова (Више јавно тужилаштво, Виши суд, Служба за борбу против високотехнолошког криминала Министарства унутрашњих послова) (Милошевић & Путник, 2017:181).

Трећи, веома важан део, у борби против високотехнолошког криминала представља и доношење Законика о кривичном поступку (2011.) у којем откривање, кривично гоњење и суђење за дела високотехнолошког криминала имају специфичности које препознају упоредна права (Урошевић, и др., 2012:37). У овом законику предвиђена је могућност пресретања комуникације (тајни надзор на предлог тужиоца у трајању до три месеца, рачунарско претраживање података који се односе на осумњиченог и кривично дело по законски предвиђеним условима) (Милошевић & Путник, 2017:182).

6.3.1. Правни оквир и подзаконска регулатива у области заштите података

У правном оквиру регулисања сајбер безбедности велики значај има и регулатива која се односи на заштиту података. У осетљиве податке спадају:

- тајни подаци,
- подаци о личности,
- информације од јавног значаја,
- пословне тајне,
- професионалне тајне,
- државне тајне, итд.

Заштита ових података регулисана је Законом о тајности података (2009.), Законом о заштити података о личности (2009.), Законом о заштити пословне тајне (2011.) и Законом

[41] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 2005.

о слободном приступу информацијама од јавног значаја (2004.) (Милошевић & Путник, 2017:185).

6.3.2. Правна регулатива у области заштите електронских платних картица

У Кривичном законику Републике Србије, чланом 225, регулисано је фалсификовање и злоупотреба платних картица. По овом члану дефинисане су консеквенце за учиниоца кривичног дела у шест области – ставова:

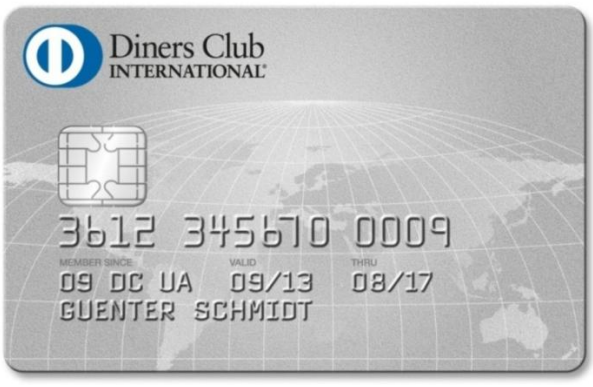
- израда лажне или преиначавање праве платне картице у намери да је употреби као праву или уколико је употреби као праву,
- прибављање противправне имовинске користи употребом картице,
- прибављање противправне имовинске користи у износу од преко 1.5 милиона динара,
- неовлашћена употреба туђе картице или поверљивих података који јединствено уређују ту картицу у платном промету,
- набавка лажне платне картице у намери да је употреби као праву или прибављање података у намери да их искористи за прављење лажне платне картице и
- одузимање лажних платних картица (као последица претходних ставова).

Поред тога, казне су предвиђене и за особе које праве, набављају, продају или дају другоме на употребу средства за прављење лажних платних картица (Члан 227, став 2). Чланом 228, став 1, регулисане су консеквенце за кориснике дебитне платне картице без покрића и кориснике кредитне платне картице за коју нису обезбедили покриће у уговореном року, па тиме себи или другоме обезбедили противправну имовинску корист у износу преко 10.000 динара.

7. СТУДИЈА СЛУЧАЈА – DINERS CLUB ПЛАТНА КАРТИЦА

Diners Club International платна картица, која је приказана Сликом 12. је прва универзална међународна кредитна картица која регулише свакодневне трошкове и штеди време. У овом систему компанија која послује кредитним картицама (Diners Club) наплаћује корисницима годишњу провизију, а њихове рачуне задужује месечно или годишње. Фирме кооперанти Diners Club-а плаћају месечне провизије у распону 4-7% од укупног износа рачуна (Андрејевић, М., 2011:42). Картица се, данас, користи се на више од 20 милиона продајних места и банкомата Diners Club-а и Discover-а (www.diners.rs, 2017.), а њене основне предности су:

1. Омогућује подизање готовог новца са банкомата, користи се на великом броју аеродрома, у хотелима и ресторанима широм света (преко 750 аеродрома у свету има посебне аеродромске ложе за чланове Diners клуба).
2. Нуди погодности при резервацијама (флексибилно пријављивање и одјављивање из хотела, услуге Rent-a-Car-а).
3. Омогућује плаћање без провизије и куповину на рате.
4. Једноставно плаћање рачуна и куповина путем Интернета.
5. Diners нуди богати наградни програм за редовно измиривање обавеза.
6. Постоје ванредни попусти у виду месечних и дневних акција.
7. Могуће су додатне картице за чланове породице.
8. Нуди VIP пакете осигурања, поред путног и здравственог осигурања, подразумевају и осигурање од губитка пртљага и кашњења лета, покривање трошкова крађе или губитка платне картице, покривање трошкова замене докумената или кључева који су нестали приликом крађе картице, итд. (Diners Club International Belgrade, 2017.).



Слика 12. Diners картица
(Извор: www.diners.rs, 2017.)

7.1. Историјат Diners платне картице

Настанак ове платне картице се везује за 1950. годину, када је Френк Мек Намара вечерао у једном ресторану, и заборавио да понесе новчаник. Из непријатне ситуације извукла га је чињеница да је, као сталном госту, управник одобрио рачун "на потпис". Због срамног догађаја он оснива Diners Club International (Андрејевић, М., 2011:42.). Прва чланска карта приказана је Сликом 13. Данас, чланство у овом клубу подразумева директно банкарство и услуге плаћања, и у власништву је једне од најпознатијих финансијских корпорација Сједињених Америчких држава – Discover Financial Services, који обезбеђују велики опсег опција за плаћање, разноврсне бенифиције и ексклузивне понуде (у сарадњи са водећим продавцима, ресторанима, сервисним компанијама, итд.) које важе у целом свету.

Слика 13. Прва картица Diners Club-а
(Извор: http://markwenning.co.za/taking-credit/, 2017.)

У пословном свету, Diners картица служи како малим фирмама (са мање од 10 картица), тако и великим корпорацијама (које користе велики број националних или интернационалних картица, или имају обрт новца већи од 10 милиона долара на годишњем нивоу). Мале фирме и организације могу да користе основну картицу[42] (ако пословање подразумева мали проток новца), картицу добитака[43] (уколико постоји напредовање у пословању) или путну картицу[44] (која обезбеђује смањење трошкова путовања). За корпорације, Diners картица служи да обезбеди лагодно пословање широм света, обезбеђујући корисницима низ услуга високог квалитета, безбедности и приступа. Уз ове погодности Diners обезбеђује елиминацију ручног уноса података, обједињавање свих података на једном месту, повећану контролу трошкова и транспарентност са понудом погодности (НБС, 2017:3)

[42] Essential Card, енгл.
[43] Rewards Card, енгл.
[44] Travel Card, енгл.

7.2. Савремена Diners платна картица

Структура савремене, хибридне Diners Club картице, са магнетном траком и чипом приказана је Сликом 16.

Слика 14. Савремена Diners Club картица
(Извор: https://www.dinersclub.pl, 2017.).

Бројеви на картици са Слике 14. означавају следеће:

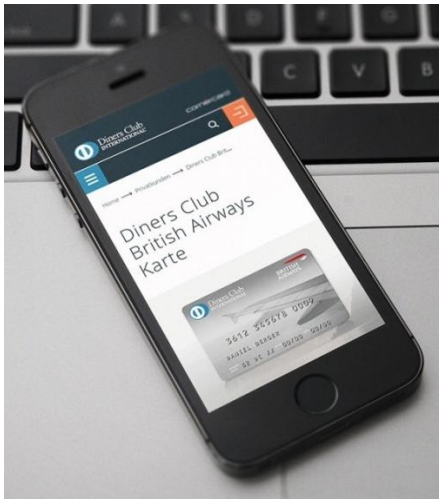
1. Интернационални лого.
2. Микро чип.
3. Број од 14 цифара који увек почиње са 36. Број картице је увек штампан у три блока 4 цифре – 6 цифара – 4 цифре.
4. Име и презиме власника картице.
5. Ознака од када је особа члан клуба.
6. Додатни идентификациони број.
7. Интерни заштитни код.
8. Ознака валидности картице.
9. Истек периода важности картице.
10. Магнетна трака са подацима и заштитним кодом.
11. Трака за потпис у који је утиснут лого клуба.
12. Лого Discovery Networks-а који прихвата картицу у САД и Канади.
13. Лого Puls-а што значи да картицу прихватају АТМ-ови у САД и Канади.

Све погодности које картица нуди истовремено су и њене највеће мане, у смислу безбедности плаћања[45]. У овом случају важе проблеми везани за садржај картице уколико

[45] Diners Club International Belgrade је надлежном суду у Београду поднео захтев за покретање стечајног поступка (од 01.05.2017. године) због злоупотребе и неодговорног управљања. Тренутно се чека одговор главне франшизе Diners Club International, о томе на који начин ће бити измиривани трошкови прекинутог пословања.

се магнетна трака оштети или на неки начин размагнетише. Такође, важе и методе прислушкивања и крађе података са чипа на даљину. Истовремено важе и препоруке, које су наведене у следећем подпоглављу, за пажљиво руковање картицом приликом плаћања, за прекид сумњивих трансакција, плаћање са сопственог рачунара, итд.

Савремена Diners картица постоји и у свом "виртуелном" облику. На Слици 15. приказана је апликација за Diners.



Слика 15. Diners апликација за мобилни телефон дело
(Извор: www.prisluskivanje.net, 2016.)

Прислушкивање мобилног телефона је дозвољено само у неким случајевима (за надзор деце, контролу радника у сопственој фирми, и по налогу суда). Све остало је шпијунажа и представља кривично дело (што то не спречава злонамернике да се баве прислушкивањем). Треба напоменути да постоји могућност надзора над сопственим телефоном јер се на тај начин могу добити подаци о евентуалним локацијама малициозних нападача на сопствени телефон, и тада се извештаји могу слати нпр. мејлом.

Diners картица је погодна за малициозне активности јер је интернационална и хибридна. Кориснику је потребно на кратко узети телефон или му поклонити нови. Софтвер за снимање протока података је лако инсталирати, он ради у позадини и, углавном, га није могуће открити. Програм за праћење је временски лимитиран, а његова цена није велика (prisluskivaci.com, 2017.). Међутим, постоји неколико знакова које корисник, ипак, може приметити и посумњати да му прислушкују телефон:

1. приликом искључивања телефон се искључује са задршком,
2. телефон показује чудну активност као што је нпр. сам укључује позадинско осветљење, активира апликације, и сл.,

3. појављују се позадински шумови као што је нпр. пуцкетање, ехо, електрично пражњење, и сл., а
4. уколико се телефон нађе у близини неког уређаја типа телевизора уређај емитује сметње, итд (Милић, С., 2013.).

Из наведених разлога Diners упозорава своје кориснике на шта да обрате пажњу кад обављају електронску куповину или изводе друге трансакције путем Интернета.

7.3. Електронска куповина и плаћање путем Diners картицом

Могућности куповине и on-line плаћања одлично је решење које свакодневно користи све већи број људи. На жалост, све погодности које чланство у клубу нуди, привлаче и оне особе које желе на лак начин да дођу до привилегија. Да би минимализовао ризик од тога да постане жртва on-line малициозности, корисник треба да познаје следеће принципе:

1. верификацију on-line куповине,
2. избор сигурног места са кога извршава трансакције и
3. надзор над поверљивим подацима са картице током куповине.

Верификација on-line куповине подразумева куповину у радњама које су поуздане и имају репутацију као сигурне за on-line куповину.

За производе који изгледају ‘превише добро да би било истинито’ често важи да је у питању неки вид непоузданости (не мора да буде крађа или малициозност).

Пре него што се корисник картице одлучи за куповину било чега из on-line продавнице, треба да провери мишљења претходних корисника, нпр. на Интернет блоговима, форумима или код интересних група.

Пре него што корисник обави on-line куповину треба, такође, да провери регулативу везану за заштиту трансакција које се одвијају путем web-сајта.

Сигурно место за on-line плаћања значи да корисник не изводи on-line плаћања са рачунара који су лоцирани на јавним местима и, у општем случају, лако доступним локацијама као што су Интернет кафеи, универзитети или библиотеке.

Такође је битно да се обезбеди да рачунар буде стално безбедан, на следећи начин:

1. рачунар треба да има оперативни систем који је ажуриран,
2. треба користити последњу верзију Интернет browser-a,
3. потребна је антивирусна заштита,

4. потребно је користити валидан пакет за заштиту података, као што је нпр. Internet Security који је у стању да детектује малвер или деструктивне фајлове, итд.

Надзор на поверљивим подацима при куповини је трећа препорука клуба. Треба бити посебно пажљив када се неком дају поверљиви подаци као што је, на пример: број картице, датум истека картице, и слично.

Препоручује се да се поверљиви подаци за куповину путем Интернета достављају искључиво преко сајтова, односно страница које се ослањају на ауторизационе центре, на које се власници картица преусмеравају уколико користе плаћање путем Интернета. Ово је једини начин којим се гарантује поверљивост података.

Подаци особе која користи картицу и поверљиви подаци на картици треба увек да буду послати поверљиви, односно да буде коришћен https:// протокол.

Да би ово било изведено потребно је задовољити следеће услове:

1. URL адреса web-сајта који се користи треба да почиње са https://, уместо стандардне адресе која почиње са http://,
2. на дну екрана browser-a или поља за адресу (у зависности од врсте browser-a) треба да стоји симбол закључаног катанца.

Уколико постоји било шта сумњиво током процеса ауторизације код плаћања, потребно је напустити овакву трансакцију и обавестити Diners о овој врсти догађаја. e-mail адреса за обавештавање и телефонски бројеви налазе се на web-сајту.

7.4. Пример злоупотребе Diners платне картице

Као и код других електронских платних картица, и код Diners картице важе проблеми везани за садржај картице уколико се магнетна трака оштети или размагнетише. Такође, могуће је применити и методе прислушкивања или крађе података са чипа на даљину. Савремена Diners картица која се користи на мобилним телефонима као апликација Diners, рањива је као и било који други апликативни софтвер. Кориснику је, за малициозни напад, потребно узети телефон, а софтвер за снимање протока података се лако инсталира и ради као позадински процес. Такође, постоји могућност да се картице ‘заразе’ малициозним софтвером уколико је нападнута једна од локалних картичарских Diners организација. У тексту који следи дат је пример који се десио 2016. године у Јужноафричкој Републици. Детекција напада на Diners картице, натерала је Diners Club

South Africa да 2016. године промени софтвер базиран на алармима односно да дода и надогради софтвер посебним детекторима типа самооубучавајућих модела за препознавање облика.

Стање Diners Club South Africa пре и за време напада

Diners Club детектор упада био је релативно једноставан систем који се показао лошим са растом обима картичарског пословања, па није успео на време да детектује малициозни упад вирусом, на систем електронских Diners картица. Систем, неотпоран на вирусе, показао се нефлексибилним и није радио у реалном времену, што је детекцију упада у Diners Club South Africa одложило тако да није пружио адекватне услуге корисницима са довољно високим степеном заштите података (aiCorporation, 2016.).

Последица и санација система након напада

Diners Club South Africa морао да промени инфраструктуру заштите електронских трансакција својих корисника, а модел који је тада применио Diners Club South Africa постао је дугорочна стратегија Diners Club-а у свету. У постојећи систем заштите прво су уградили RiskNet софтвер који је радио у паралели са њиховим претходним софтвером за заштиту података у периоду од шест месеци. За то време је систем надограђиван тако да препознаје разноврсне облике познатог малициозног софтвера. Прављена је база аларма која је постала интегрисани део RiskNet софтвера.

Садашње стање у Diners Club-у

Коришћењем RiskNet софтвера, Diners Club сада прати потенцијалне нападе као комбинацију аларма које је имала Diners-ова претходна верзија и аларма који су ‘научени’ тако да препознају, односно детектују један од конкретних напада који су детектовани шестомесечним обучавањем овакве структуре. RiskNet сада има базу познатих напада којом брже препознаје познати напад, а непознати садржај се прослеђује администраторима који упоређују садржај са новим малверима (који се појављују у свету) и, уколико га идентификују, додају га у своју базу познатих напада (чиме додатно убрзавају рад система за препознавање малициозног приступа Diners Club мрежи) (aiCorporation, 2016.).

8. ЗАКЉУЧАК

Савремене технологије довеле су до широко распрострањених Интернет активности које су везане не само за приватну и пословну комуникацију него и за трансакције, као што су нпр. обављање банкарских услуга на даљину, плаћање рачуна, примање извештаја и слично. Поред наведеног, све је више активности које су везане за on-line електронско плаћање роба и услуга. Око трећине корисника Интернета истовремено врши и овакве трансакције, односно куповине, што може бити предуслов за малверзације и малициозне активности. Сајбер свет, виртуелно окружење у којем је ово могуће, нуди велики број предности у оваквим ситуацијама. Проблем који се јавља је везан за ситуацију наглог развоја технологије и апликација, као и понуде на тржишту, које не прате одговарајући закони којима би били санкционисани малициозни напади. И поред тога, проток података у сајбер окружењу је огроман.

Велики део електронских трансакција одвија се коришћењем платних картица које се могу сврстати у две групе: са магнетном траком или са чипом (постоје и њихове хибридне варијанте). Због све чешћих злоупотреба електронских платних картица, банке и картичарске организације упозоравају своје кориснике да се придржавају основних упутстава при коришћењу платне картице на банкоматима или POS терминалима. Првенствено, корисници треба да буду свесни да постоји могућност да их неко посматра кад користе картицу, уносе лозинке, идентификационе бројеве, и сл. У том смислу, потребно је да корисник заклања руком тастатуру на банкомату или да прати унос картице у POS терминал. Поред тога, корисник се упућује да прекине сваку сумљиву трансакцију и о томе обавести банку.

Интернет трансакције имају своје предности и мане. Корисник не одлази у банку, подаци су му доступни нон-стоп, може да врши бесплатно плаћање рачуна, обавља куповину, и слично. Могућности напада на персоналне податке корисника, у овим случајевима, се делимично избегавају коришћењем виртуелних тастатура, преусмеравањем на повезане web сајтове или странице, и слично. Код Интернет куповине, корисник се упозорава да води рачуна на који начин и коме прослеђује идентификациони број који чине три цифре на полеђини картице са чипом. Таккође, саветује се да се користе посебни browser-и са заштитним елементима, који су добро видљиви. Поред тога, препоручује се да корисници купују на on-line сајтовима који су познати као безбедни, и да пре тога посете корисничке блогове.

Сајбер безбедност је, захваљујући све већем напретку технике, постала горући проблем садашњости јер постоји велика могућност напада на осетљиве податке и електронске трансакције, а мале су могућности да се виновници кривичних дела извршених у сајбер простору нађу и казне. У том смислу су светске организације, корпорације и институције препознале важност норматива сајбер безбедности. Уједињене нације још 80-их година прошлог века скрећу пажњу на интернационализацију проблема безбедности у сајбер простору, а у периоду од 2001. до 2007. године доносе резолуције и низ директива којима се ова област регулише и допуњава у складу са прогресом технологије и новим типовима напада на податке или трансакције у сајбер простору. Поред Уједињених нација, Савет Европе има низ активности које се односе на борбу против компјутерског криминалитета. Република Србија је, у складу са стратегијама и директивама Европске уније, ратификовала Конвенцију и Протокол о високотехнолошком криминалу, који је имплементиран у домаће законодавство.

У складу са претходно наведеним поглављима, на крају рада дат је приказ студије случаја једног од последњих напада на платну картицу Diners Club-а убацивањем вируса у систем Diners -а у Јужноафричкој Републици и последица које су настале као резултат санације система, upload-а новог софтвера који ради у реалном времену и препознаје велики број постојећих напада. Данас је ова верзија софтвера постала стандард Diners-а за цео свет.

ЛИТЕРАТУРА

1. aiCorporation (2016.) *Diners Club cuts fraud with ai Corporation*. Finextra 05.04.2016. године.
2. Андрејевић, М. (2011.*) Електронско банкарство у Србији*. Пословни факултет. Универзитет Сингидунум. Београд.
3. A paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Stratsbourg, 15-18 November 1976. pp.225-229.
4. Бабовић, С. (2015.) *Кривично дело фалсификовања и злоупотребе платних картица у законодавству Републике Србије и државама Западног балкана*. BIBLID: 0352-3713(2015); 32 (7-9), стр. 62-74.
5. Балтић, У. (2014.) *Платне картице и електронско плаћање.* Пословни факултет. Универзитет Сингидунум. Београд.
6. Barabasi, A.L. & Frangos, J. (2002.) *Linked: The New Science of Networks*. New York: Basic Books.
7. Бараћ, С., Стакић, Б., Хаџић, М. & Иваниш, М. (2007.) *Практикум за банкарство.* Факултет за финансијски менаџмент и осигурање. Универзитет Сингидунум.
8. Bibighaus, D. (2015.) How Power-Laws Re-Write The Rules Of Cyber Warfare. *Journal of Strategic Security*, No 4:8, pp.39-52.
9. Барјактаревић, А. (2012.) *Е-банкинг и сигурност техничких решења за Интернет трансакције.* Електротехнички факултет. Сарајево.
10. Bichoff, V. (2016.) Could you fall pray to a contactless conmann? How thieves can take money from your card as you're walking down the street. Доступно на: http://home.bt.com/lifestyle/money/cards-loans/how-a-simple-trick-with-foil-can-prevent-contactless-card-fraud-11363994986984. Преузето 29.05.2017. године.
11. Buckland, B.S., Shierer, F., Winkler, T.H. (2004.) *Information security forum*. Geneva. pp.9.
12. Bulanan, A. (2014.) Analisah. Доступно на: https://analisah.wordpress.com/2014/02/. Преузето: 29.05.2017. године.
13. Council of Europe, Convention on the Protection of Children Against Aexual Exploatation and Sexual Abuse (2007.), CETS No.: 201, Lanzarote, the 23 October 2007.
14. Council of Europe Computer-related Crime Rrecommendation No. R(89) 9. (1989.).

15. Diners (2017.) Diners Club STANDARD platna kartica. Доступно на: http://www.diners.rs/standard-kartica Преузето 22.05.2017. године.
16. DinersClub (2017.) Diners Club Security Solutions. Доступно на: https://www.dinersclub.pl/en/safety.html. Преузето: 30.05.2017. године.
17. Diners Club International Belgrade (2017.) Premium Club платна картица. Доступно на: http://www.diners.rs/premium-club-kartica, Преузето: 30.05.2017. године.
18. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (2000.) *Official Journal of the European Communities*. L 178, 17.07.2000, pp.1-16.
19. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in electronic communication services or of public communication networks and amending Directive 2002/58/EC. (2006.)
20. Ђорђевић, В. (2009.) *Смарт картица*. Прокупље. Стр. 4-23.
21. Ђукић, Ђ., Бјелица, В. & Ристић, Ж. (2005.) *Банкарство*. Економски факултет. Београд.
22. Glavinić, Đ. (2007.) *Osnovna svojstva kompleksnih mreža i njihova primjena*. Fakultet elektrotehnike i računarstva. Zagreb.
23. Global Cybersecurity Agenda of the International Telecommunication Union (2007.)
24. Hathaway, O. & Crootof, R. (2012.) The law of cyber attack. *California Law Review*. USA.
25. Hollis, D. (2007.) Why Stated Need an International Law for Information Operation. *Lewis & Clark Law Review*, Portland. Vol. 11, pp. 1023-1042.
26. [Internet] (2016.) Прислушкивање мобилног. Доступно на: http://www.prisluskivanje.net/prisluskivanje-mobilnog-telefona/, Преузето: 31.05.2017. године.
27. ISO/IEC 7810:2003 (2003) *Identification card – Physical characteristics*. ICS: 35.240.15 Identification
28. ISACA (2017.) *Business model for information security*.
29. Joint Communications to the European Parlament, the Council, the European Ecconomic and Social Comitee and the Comitee of Regions Cybersecurity Strategy of the European Union. An Open, Save and Secure Cyberspace. (2013.). 7.2.2013. JOIN (2013) 1 final.
30. Јонев, К. (2016.) Сајбер тероризам и употреба сајбер простора у терористичке сврхе. *Безбедност 2/2016*. Стр.206-222.

31. Јонев, К. & Бериша, Х. (2015.) *Сајбер напад – изазов у изучавању стратегије и војне стратегије*. Зборник радова са научног скупа Школе националне одбране, СОРЛОГ. стр.167-176.
32. Koch, C. (2010.) *Bankrecht: Grundlagen der Rechtspraxis* (Hrsg. R. Fischer, T. Klanten), RWS, Koln 2010, 746; Hans-Peter Schwintowski, *Bankrecht*, Carl Heymanns, Koln 2011, 258; Hartmut Strube, *Handbuch des Fachanwalts: Bank– und Kapitalmarktrecht* (Hrsg. P. H. Assies, D. Beule, H. Strube), Carl Heymanns, Koln 2010, 253.
33. Кончар, Ј. (1998.) *Изазови и могућности електронске трговине*. Прометеј. Нови Сад.
34. Конвенција о сајбер криминалу (2001.) Доступно на: http://www.entel.rs/info/software/sajber kriminal-konvencija EZ.pdf. Преузето:30.10.2018. године.
35. Кривични законик (2016.) "Сл. гласник РС", бр. 85/05, 88/05-исправка, 107/05-исправка, 72/09, 121/12, 104/13, 94/16. Члан 243. Злоупотреба и фалсификовање платних картица.
36. Libicki, M.C. (2009.) *Cyberdeterrence and Cyberwar*. Washington DC: RAND.
37. Markoff, J., Sanger, D.E. & Shanker, T. (2010.) In Digital Combat, U.S. Finds No Easy Deterrent. *New York Times* 25. January 2010. World Section.
38. Мијалковић, С. (2011.) *Национална безбедност*. Криминалистичко полицијска академија. Београд.
39. Милић, С. (2013.) Шест знакова да вам прислушкују мобилни. Доступно на: http://www.novosti.rs/vesti/naslovna/tehnologije/aktuelno.236.html:464473-Sest-znakova-da-vam-prisluskuju-mobilni, Преузето 30.05.2017. године.
40. Милосављевић, М., Веиновић, М. & Грубор, Г. (2009.) *Информатика*. Универзитет Сингидунум. Београд.
41. Милошевић, М., Матић, Г., & Миљковић, М. (2018.) Класификација малициозник активности у сајбер простору и организација сајбер безбедности у Републици Србији. *Стручни рад.* стр.540-553.
42. Милошевић, М.М. & Путник, Н.Р. (2017.) Сајбер безбедност и заштита од високотехнолошког криминала у Републици Србији – Стратешки и правни оквир. *Култура полиса* XIV, бр.33, стр.171-191.
43. Мирковић, Д. (2017.) *Криминолошки аспект компјутерског криминалитета.* Правни факултет. Универзитет у Нишу. Стр.1-119.

44. Мушки портал (2012.) Биометријски банкомати који читају длан. Народна банка Србије (2007.) *Водич за платне картице*. стр.2-10.
45. Његуш, А. (2010.) *Пословни информациони системи*. Универзитет Сингидунум. Београд.
46. Pande, J. (2017.) *Introduction to Cyber Security*. Uttarkhand Open University, Haldwani, str.4-143.
47. PCI Data Security Standards 1.1 (2006.)
48. PCI Data Security Standards 1.1 (2006.) – *Revision.*
49. PCI Data Security Standards 2.0 (2010.)
50. PCI Data Security Standards 3.0 (2013.)
51. PCI Data Security Standards 3.2.1 (2018.)
52. PCI Security Standard Council (2006.) PCI security.
53. PCI Security Standard Council (2018.) Payment Card Industry Data Security Standard Requirements and Securiy Assessment Procedures Version 3.2.1. May 2018.
54. Правилник о условима за пружање интернет и осталих услуга преноса података и садржају одобрења. (2008.) Бр. 1-01-110-16/08.
55. Протић, Д. (2013.) Информациона безбедност: стандарди или правила. *Војно дело* 1. стр.133-150.
56. Путник, Н. & Бошковић, М. (2013.) Савремени безбедносни изазови – хактивизам као нови облик друштвеног конфликта. *Култура полиса* X, бр.21. стр.115-132.
57. Путник, Н., Милошевић, М. & Бошковић, М. (2017.) Стратешко планирање сајбер одбране - ка адекватнијем правном оквиру и новој концепцији процене ризика, изазова и претњи. *Војно дело* 7. стр.174-185.
58. Радуновић, В. (2015.) *Сајбер простор: Како осигурати будућност која је већ стигла.* Центар за евроатланске студије. Београд.
59. Recommendation No. R(95) 13 of the Comitee of Ministers to Member States concercing problems of Criminal Procedural Law connected with Information Technology. (1995.)
60. Ризмал, И., Радуновић, В. & Кривокапић, Ђ. (2016.) *Водич кроз информациону безбедност у Републици Србији*. Центар за евроатланске студије. Мисија ОЕБС-а у Србији. Стр.5-75.
61. Rouse, M. (2016.) Information security (infosec). Доступно на: www.searchasecurity.techtarget.com

62. Симић, С. (2018.) Е-платни промет. Електронски платни промет и системи електронског плаћања. Доступно на: http://poslovnainformatika.rs/elektronsko-poslovanje/e-platni-promet/. Преузето: 22.10.2018. године.
63. Simović, V. (2014.) *Zloupotrebe platnih karitica na bankomatima*. Information technology school. Visoka škola strukovnih studija za IT. Comtrade.
64. Спасојевић, Ј. (2013.) *Криптозаштита у комуникационим системима*. Универзитет Singidunum. Београд.
65. Суботић, Н. (2010.) Платне картице. Доступно на: www.asseco-see.rs. Преузето: 25.05.2017. године.
66. Стојановић, И. (2011.) *Електронска куповина и пословање путем Интернета.* Универзитет Сингидунум. Београд.
67. Стојановић, З. (2012.) Коментар Кривичног законика. *Службени гласник.* Београд.
68. Шкорић, М. (2015.) *Картичарство са освртом на ризике електронског пословања.* Универзитет Сингидунум. Београд. стр.1-73.
69. Тренкић, В. (2013.) *Регулатива у е-пословању: Сајбер криминал*.
70. United Nation Manual on the Prevention and Control of Computer-related Crime (1994.)
71. UN resolution on computer crime legislation (1990.)
72. UN resolution A/res/55/63 on combating the criminal missuse of information technologies (2001.).
73. UN resolution A/res/56/121 on combating the criminal missuse of information technologies (2002.).
74. Урош, Т. (2012.) *Електронско банкарство*. Београдска пословна школа. Београд.
75. Урошевић, В., ивановић, З. & Уљанов, С. (2012.) *Мач у world wide web-у*. Eternal mix. Београд
76. Васковић, В. (2007.) *Системи плаћања у електронском пословању.* Београдска пословна школа. Београд.
77. Васковић, В. (2008.) *Електронско пословање и интернет маркетинг*. Београдска пословна школа. Београд.
78. Војводић, М. (2017.) *Стратегија сајбер безбедности ЕУ: отворен безбедан и заштићен сајбер простор*. ПРАВОИКТ.Serbian Law Resource.
79. Вујовић, С. (2005.) *Електронско пословање и електронска интелигенција.* Београдска пословна школа. Београд.

80. Вуковић, И. & Радовић, М. (2014.) Правно-политичко оправдање кривичног дела коришћења платних картица без покрића. *Анали правног факултета у Београду*. Година LXII, 2/2014. стр.68-85.
81. Wood, J. & Dupont, B. (2006.) *Democracy, Society and Governance of Security*. Cambridge University Press. Cambridge.
82. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању. *Сл. гласник*, бр. 94/2017.
83. Закон о изменама и допунама Кривичног законика Републике Србије (2003.) *Службени гласник РС*, бр.39/03.
84. Закон о организацији и надлежности државних органаза борбу против високотехнолошког криминала (2009.) *Сл. гласник РС*, бр. 61/2005 и 104/2009.
85. Закон о полицији (2018.) *Службени гласник РС*, бр. 6/2016 і 24/2018.
86. Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система (2009.) *Службени гласник РС*, бр.19/09.
87. Закон о потврђивању Конвенције о високотехнолошком криминалу (2009.) *Службени гласник РС*, бр.19/09.
88. Закон о слободном приступу информацијама од јавног значаја (2004.) *Службени гласник РС*, бр.120/04, 54/07, 104/09, 36/10.
89. Закон о тајности података (2009.) *Службени гласник РС*, бр.104/09.
90. Закон о заштити података о личности (2009.) *Службени гласник РС*, бр. 97/08, 104/09, 86/12, 107/12.
91. Закон о заштити пословне тајне (2011.) *Службени гласник РС*, бр.72/11.
92. Законик о кривичном поступку (2011.) *Службени гласник РС*, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14.