



Универзитет у Нишу
ПРАВНИ ФАКУЛТЕТ

Бр. 01-1687/1

17/06/2024. године

На основу члана 36. Правилника о мастер академским студијама права Служба за наставу и студентска питања даје следеће

О Б А В Е Ш Т Е Њ Е

1. Обавештава се јавност да су завршни мастер рад и Извештај Комисије за оцену и одбрану мастер рада под називом „Видеоснимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета”, кандидата Момчиловић Милице, број досјеа М033/23-УП, студента мастер академских студија права на Правном факултету у Нишу, примљени дана 17/06/2024. године и да се налазе у Библиотеци и на сајту Факултета.

2. Извештај и мастер рад доступни су, у року од 5 (пет) дана од дана истицања овог обавештења на огласну таблу Факултета, заинтересованим лицима у времену од 08,00 до 15,00 сати сваког радног дана.

3. Извештај Комисије за оцену и одбрану мастер рада су саставни део овог обавештења.

4. Ово обавештење истаћи на сајт и доставити Библиотеци.

СЛУЖБА ЗА НАСТАВУ И
СТУДЕНТСКА ПИТАЊА



**Катедри за кривичноправне науке
Правног факултета Универзитета у Нишу**

На седници Катедре за кривичноправне науке која је одржана дана 26.04.2024. на основу члана 34. Правилника о мастер студијама Правног факултета у Нишу предложена је, а одлуком декана бр.01-1129 од 29.04.2024. године, формирана Комисија за оцену и јавну одбрану мастер рада под називом: „**Видеоснимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета**“, кандидаткиње Милице Момчиловић, број индекса М002/20-УП. Комисија, након детаљног прегледа мастер рада подноси следећи:

ИЗВЕШТАЈ

Мастер рад под називом: „**Видеоснимци генерисани уз помоћ вештачке интелигенције (дипфејк) као облик сајбер криминалитета**“, кандидаткиње Милице Момчиловић написан је на 89 страница компјутерски обрађеног текста, без прореда. Кандидаткиња је цитирање вршила у фуснотама (укупно 257). Литерарну подлогу рада чини 62 иностраних и домаћих извора књига, библиографских јединица (уџбеника, приручника, коментара закона и статистичких података) и други бројни научни и стручни радови објављени у часописима, уз осталу истраживачку грађу – 26 законских и подзаконских аката, као и електронски извори.

Структурално рад је подељен на десет делова: 1) Појам и одлике рачунарског криминалитета, 2) Улога вештачке интелигенције у сајбер криминалитету, 3) Појам и подела дипфејка, 4) Злоупотреба дипфејк технологије, 5) Позитивна примена дипфејк технологије, 6) Откривање, могућа решења и будућност дипфејка, 7) Нормативно правни оквир дипфејк технологије, 8) Нормативни оквир дипфејка у појединим државама, 9) Нормативни оквир дипфејка у Републици Србији, 10) Надлежност и поступање органа у области високотехолошког криминалитета, укључујући и увод, закључна разматрања, попис коришћене литературе, сажетак и кључне речи на српском и енглеском језику и биографију студенткиње.

У уводу (стр. 1-2) кандидаткиња је изложила предмет свог рада указујући да је криминал појава која је стара колико и само друштво, да је као феномен својствен свим народима те да као такав никада не може бити у потпуности елиминисан, како у стварном тако ни у виртуелном свету. Упркос чињеници да су технолошки проналасци одиграли можда пресудну улогу у еволуцији нашег друштва, истиче да је потребно размотрити суштинске ефекте нових технологија као и њихову улогу и значај у будућности рачунарског криминалитета.

У првом делу мастер рада под називом „Појам и одлике рачунарског криминалитета“ (стр. 3-14) кандидаткиња је указала на изазове ове појаве, поставила ширу и ужу дефиницију рачунарског криминалитета и описала заједничке карактеристике дефиниција овог појма које су најчешће у терминолошкој употреби. Посебну пажњу је посветила и карактеристикама рачунарског криминалитета, разликама између прве, друге и треће генерације рачунарског криминалитета као и

особинама овог феномена попут високог степена анонимности, екстериторијалног карактера и тежње за профитом. Акцент је стављен на растућу зависност од дигиталних система нарочито током пандемије вируса „КОВИД-19“ али и на тенденцију повећања претњи у сфери сајбер безбедности. Наиме, усавршавање технологије отворило је нове могућности за сајбер криминалце чиме су побољшани изгледи за извршење најразноврснијих кривичних дела. Истовремено, дата им је прилика да буду учесници у појавама попут друштвеног инжењеринга, ширења дезинформација и лажних вести. Кандидаткиња је потом обрадила појавне облике рачунарског криминалитета, међу којима су компјутерске крађе, компјутерске преваре, неовлашћено прибављање информација уз помоћ компјутера, уцењивачки софтвер, рачунарска саботажа и компјутерски тероризам, а потом и савремене у које је уврстила пиратерију, сајбер прогањање, дечју порнографију и дипфејк.

У другом делу рада под називом „Улога вештачке интелигенције у сајбер криминалитету“ (стр. 14-18) кандидаткиња је описала зачетке вештачке интелигенције, предности и очекивања од ове технологије у савременом добу. Потом је дефинисала ову подобласт рачунарства и указала на позитивну примену коју има или може имати у разним сферама живота попут медицине, пољопривреде или екологије. Са становишта криминалитета, одредила је негативне стране ове технологије и начине на који сајбер криминалци могу да профитирају од њеног коришћења. Указано је на етичке принципе вештачке интелигенције постављене од стране великих интернет платформи као и на појаву дипфејк технологије која је почела да се користи у многим индустријама као и њеној вези са сајбер криминалитетом.

У трећем делу рада под називом „Појам и подела дипфејка“ (стр. 18-30) одређен је појам и дефиниција дипфејка. Потом је одређен поступак настајања дипфејк садржаја, прво путем дубоких неуронских мрежа (ДНМ) односно аутокодера, а потом и процес стварања таквог садржаја путем ГАН технологије. Закључује да се време потребно за креирање једног дипфејк материјала константно смањује, те да је постало могуће направити уверљиви, лажни дипфејк видео помоћу само једне слике као извора. Даље, извршена је подела дипфејка на фото, аудио, видео, и аудио-видео дипфејк при чему је кандидаткиња детаљнио обрадила сваки појединачно. Наведени су начини и процеси на који сваки од ових садржаја настаје као и приступ који просечан корисник интернета може користити како би створио један дипфејк материјал.

Четврти део рада под називом „Злоупотреба дипфејк технологије“ (стр. 30-44) односи се на неке од начина на које се дипфејк може злоупотребити како од сајбер криминалаца тако и од малициозних појединаца. У овом делу кандидаткиња под опасном употребом дипфејка наводи стварање и коришћење ове технологије у циљу дезинформисања, креирања и ширења лажних вести, манипулацију доказима у судским и другим поступцима, малверзације у сфери пословања, раду приватних и јавних институција. Истиче да су као нарочито опасне појаве оне када се дипфејк садржај користи у циљу преваре или крађе идентитета а као посебно друштвено опасну појаву издваја дипфејк порнографију. Дефинисан је феномен лажних вести и онлајн дезинформација поткрепљен примерима. Као посебан проблем истиче везу новинарста и дипфејка као и потребу да се пронађу механизми који би појединцу помогли да изгради ставове који су базирани на поузданим информацијама. Потом је анализирано како дипфејк садржај може утицати на грађанске и кривичне поступке односно на опасност од појаве манипулисаних доказа у судници, а додатно је указано и на начине на које би се судови могли заштитити од оваквих појава. У области пословања,