

Влиянието на автоматизацията и изкуствения интелект върху дигиталната криминалистика

The Impact of Automation and Artificial Intelligence on Digital Forensics

Андрей Вишневский¹

Резюме

В настоящия доклад ще бъде разгледана автоматизацията и изкуствения интелект върху дигиталната криминалистика. Каква е ролята, която оказват технологиите за криминалистиката, какви цели се постигат и какво е общото влияние върху обществото посредством съвременните технологии. В допълнение към това ще се представят възможностите и предизвикателствата, пред които е изправена дигиталната криминалистика.

Ключови думи: Автоматизация, Оптимизация, Изкуствен интелект, Дигитална криминалистика
JEL: L86, O33, K42

Abstract

This report will examine automation and artificial intelligence on digital forensics also known as criminalistics. What is the role of technology in forensics, what goals are being achieved and what is the overall impact on society through modern technology. In addition to this, the opportunities and challenges facing digital forensics will be presented

Keywords: Automation, Optimization, Artificial Intelligence, Digital Forensics

Въведение

Съвременният свят използва решения за специфични проблеми, което помага за качеството на живота на общество, съвременния човек е заобиколен от множество технологии и устройства, създадени с различни цели и за различно използване, но обикновено тези технологии помагат на един човек и/или цяло общество да улесни и подобри живота по един или друг начин. Често тези технологии са свързани с автоматизация, дигитализация и оптимизация на различни процеси и ресурси. Дигитализация, автоматизация и изкуствен интелект намират широки приложения в различни дейности и среди, в търговия и икономиката, в строителство, в производство, медицина, образование, правителствени и неправителствени организации и системи. В сферата на сигурността дигитализацията и автоматизацията също заемат централно място. Много охранителни фирми използват иновативни технологии за защита и сигурност, което е особено полезно за органите на реда, като полицията и различни други служби и агенции за предотвратяване и разкриване на престъпления. В контекста на криминалистиката и на дигитална криминалистика, технологиите съществено улесняват и оптимизират работата на експертите, като по този

¹ Студент-бакалавър, катедра "Информационни технологии и комуникации", УНСС
e-mail: avishnevskiy_21180092@unwe.bg

начин подпомагат дейността на полицията, прокуратурата, военната полиция и други държавни органи, ангажирани със сигурността и поддържането на обществен ред.

Същност на криминалистика и нейните направления

Криминалистиката представлява област в наказателното право, фокусиран върху изучаването на обществени връзки и процеси, свързани с откриването, разследването и превенцията на престъпления. Тази наука използва знания от наказателно право, криминология, химия, биология, медицина, психология, математика, компютърни науки (computer science). Освен връзката с горепосочените науки криминалистиката има и тясна връзка със своите направления. Разновидностите или направления на криминалистика са множество, но ще обърнем по-подробно внимание на част от тях[1].

Направления в криминалистиката

В криминалистиката има множество направления, които още се наричат дялове и според определени класификации те се разделят на сектори, по данните на “Национален институт по криминалистика” при “Министерство на вътрешните работи” на Република България тези сектори са:

- Сектор "Дактилоскопия" – този сектор отговаря за събиране и обработка на веществени доказателства, каквито са пръстови отпечатыци и други важни за идентификация експертизи.
- Сектор "Трасология и балистика"- това е сектор обединяващ две области в криминалистика, „балистика“, която отговаря за изследвания свързани с оръжия и „трасология“, в която се изследват следи от обувки, автомобилни гуми, следи върху дрехи и предмети и други важни способности, които могат да помогнат за разкриването на редица престъпления.
- Сектор "Документни изследвания" и сектор "Идентификационни изследвания"- между тези сектори има достатъчно много прилики, те отговарят за експертизи над фалшиви документи, ценни книжа и банкноти, тяхната цел е противодействие на престъпления свързани с фалшифицирането на предмети.
- Сектор "Компютърни системи и мрежови устройства" – в този сектор се изготвят компютърно-технически експертизи на компютърни информационни системи (настолни компютри, преносими компютри (лаптопи), външни и вътрешни твърди дискове от тип HDD, флаш памети и SSD дискове, SD карти, оптични носители и др.) и компютърни информационни данни, записани и предоставени на носител в това число CD и DVD дискове. Компютърно-криминалистичното изследване е свързано с намиране и установяване на данни, тяхното записване, запазване, анализ и представяне на данните, открити в цифрови веществени доказателства, без да бъдат нарушени или променени. За тази цел в “Национален институт по криминалистика” е изградена съвременна, високотехнологична среда за изготвяне на криминалистични изследвания в областта на цифровите носители на информация. За експерти извършващи тази дейност са осигурени необходимите устройства и технологии, предназначени за лабораторни изследвания на цифрова информация и нейния анализ. Устройствата са проектирани и оптимизирани за работа под високи натоварвания в непрекъснат режим, като осигуряват надеждност и ефективност в процеса на

лабораторни изследвания на цифрова информация. Тези устройства имат вграден електронен блок, който позволява свързването на информационни носители с различни интерфейси и реализира хардуерна защита от запис.

- Сектор "Изследвания на комуникационни устройства" - в този сектор се извършват съдебно-технически експертизи на устройства от комуникационната техника към които се отнасят телефони, факсимилни апарати, мобилни телефони, радио комуникационни устройства, радио средства и други средства с които може да се предава информация, това значително помага за предотвратяване и разкриване на престъпления.
- Сектор "Изследване на електронни устройства"- в този сектор се извършват експертизи на неистински платежни инструменти тоест за фалшиви пластики на банкови карти, за системи за видеонаблюдение, отключване или преодоляване на паролите им с цел извличане на информация и възстановяване на изтрита информация и други експертизи.
- В изброените сектори са показани области на тяхната работа и техните изследвания, всеки от тези сектори е важен и е свързан пряко към автоматизация и дигитализация в криминалистиката, а сектори като : "Изследвания на комуникационни устройства", "Компютърни системи и мрежови устройства" и "Изследвания на комуникационни устройства" те са пряко или косвено се отнасят към направлението наречено "Дигитална криминалистика" [2].

Същност на дигитална криминалистика и ролята ѝ за обществото.

Дигиталната криминалистика е дял или направление на криминалистиката, чието предназначение е събирането и анализ на данни с цел изясняване на обстоятелствата около злонамерени деяния в киберпространството. Такива действия могат да бъдат забелязани, например когато потребител има проблем с работоспособност на дадена система, тоест тя не работи или има неочаквана промяна в данните. От където започва изследването на проблема, за да се разбере при какви обстоятелства и какви събития са довели до инцидента и оценяване на последствията. Такива случаи могат да бъдат различни: минаване по определен линк, достъп до сайт който е фалшифициран с престъпна цел и/или някакъв друг начин, но целта е една и съща, в повечето случаи. Тя е кражба на лична информация или повреда, хардуерна или софтуерна с цел невъзможност за използване на мобилните устройства, които са били "заразени" посредством преминаване по линк или инсталация на някакво приложение от неизвестен източник. Такива престъпления действат предимно върху финансовите източници на пострадалото лице или върху личните му данни, тези престъпления се разследват от различни органи и експерти в това число от експерти от горепосочените сектори на "Национален институт по криминалистика", а начини за противодействие на такива престъпления се създават не само от държавните органи, но и от експерти и специалисти от различни фирми и организации, в това отношение дигиталната криминалистика е тясно свързана с киберсигурността.[3]

Ролята на дигитална криминалистика за обществото е много важна, предимно в контекста на знания и начини за противодействие срещу киберпрестъпления, което ще позволи на потребителите да запазят финансовите си ресурси и личната информация, което е особено важно за мобилно и онлайн банкиране в различните банки и за различни платежни системи.

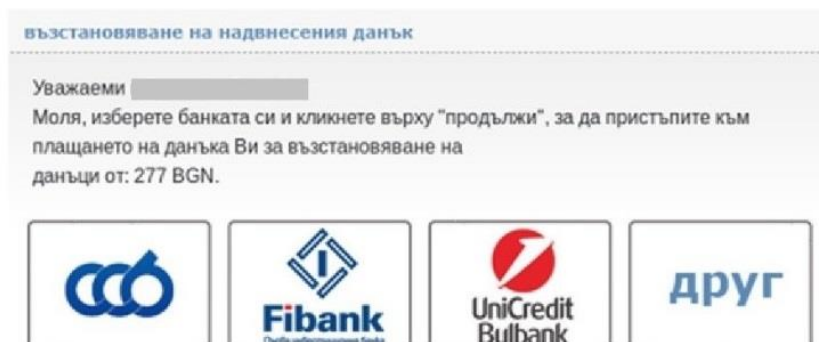
Освен това, от киберпрестъпления направени от така наречени “хакери” и техните хакерски атаки страдат не само обикновени потребители като физическо лице, което ползва определени услуги, но и юридически лица, които често представляват големи фирми и компании, които също търпят загуби на различни ресурси. Те могат да бъдат финансови, ако са откраднати средства от компанията или са повредени техните хардуерни или софтуерни продукти, за които са необходими финансови средства, за решаване и отстраняване на даден проблем, също така загубите могат да бъдат и репутационни, което пряко влияе върху финансовото състояние на компанията. Именно за това ролята на дигиталната криминалистика и киберсигурността е много важна както за цялото общество, така и за отделната единица в нея.

Начините за защита от киберпрестъпления са голямо количество и са разнообразни от софтуерни под формата на антивируси и друг софтуер противодействащ на тях, до хардуерни решения. Ключова роля за обезопасяването на личното си “кибер” пространство са информираността и вниманието на потребителя. Той може да се предпази от киберпрестъпления по отношение към него, когато използва с повишено внимание устройствата си, не тегли приложения от неизвестни източници, внимателно преглежда линковете по които преминава и не споделя никъде и на никого личните си данни, като информация по банковите си карти и сметки, данните под формата на Login, парола и друга важна информация, която може да бъде открадната. Освен това, е добре да се следват препоръки посочени на сайта на Европейски парламент, като част от тези препоръки са:

- Обезопасете мрежата си вкъщи. Не разчитайте на парола по подразбиране за Wi-Fi мрежата: променете я. Ограничаване на броя на свързаните в мрежата устройства и допускате само такива, които са познати на потребителя.
- Подобряване на паролите, с използвайте дълги пароли включващи комбинация от числа, букви и специални символи.
- Постоянно актуализиране на всички системи и приложения, инсталиране на антивирусен софтуер и неговата актуализация.[4]

СПЕШНО! - ВЪЗСТАНОВЯВАНЕ НА НАДВНЕСЕН ДАНЪК

от: "Националната агенция за приходите" user123@xyz.com



Source: Национална агенция за приходите [6]

Фигура 1. Пример за фишинг атака, един от начините за киберпрестъпления.

Горепоказаното изображение е пример за фишинг атака, която идва от измамници, маскирани като надеждни източници, и могат да осуетят достъпа до всички типове чувствителни данни, това е фишинг атака, по имейл. Тя е най-често срещаната форма на фишинг – този тип атака използва тактики като фалшиви хипервръзки(линкове), за да примамва получателите на имейла да споделят личните си данни. Атакуващите често се маскират като голям доставчик на акаунти, като например Microsoft или Google[5]. Друга голяма организация която често е използвана за фишинг атака е Национална агенция за приходите[6].

Искусствен интелект(AI) в Дигитална криминалистика

Искусствен интелект (AI) в дигиталната криминалистика може да бъде много полезен по различни начини и ролята му, също може да бъде разнообразна. Дигиталното съдебно разследване обикновено е сложен и продължителен процес. В зависимост от вида и тежестта на престъплението, от броя на пострадалите и броя на експертите разследващи престъплението, един случай може да отнеме седмици, месеци и дори години. Несравнимата бързина и адаптивност на изкуствения интелект го превръщат в едно от най-ефективните решения за подпомагане на разследванията.

Експертите могат да използват AI по няколко начина. Те могат да използват машинно обучение (ML), обработка на естествен език (NLP) и генеративни модели за разпознаване на модели, предсказуем анализ, търсене на информация или съвместно търсене на решение. Може да подпомага изпълнението на техните рутинни ежедневни задачи или да извършва задълбочен анализ. Извършва се автоматизация, тя е една от най-големите възможности на AI. Тъй като може да работи автономно без човешка намеса. Анализаторите могат да го оставят да се справя с повтаряща се, отнемаша много време работа, докато наблягат върху критични, високоприоритетни отговорности, това също е предимство, защото AI при необходимост може да работи денонощно[7].

Заклучение

Съвременните технологии постоянно се развиват и имат значителна роля в криминалистиката и в това число в нейното направление дигитална криминалистика. Хартени източници на данни се заменят с дигитални ,което драстично улеснява работата с тях и подпомага за оптимизацията. В допълнение към това се развиват технологии, които силно улесняват работата на криминалистите и допринасят за по-лесно и по-качествено предотвратяване и разкриване на престъпленията. За тази цел помагат камери и системи за биометрия ,нови методи за анализ и събиране на доказателства, технологии за защита на информация и данни и други важни заобикалящи ни навсякъде технологични представители. Една от най-новите технологии, която е представена в доклада “ Изкуствен интелект(AI)” , вече оказва значително влияние върху информационните технологии в глобален мащаб, което спомага за по-динамично развиване на автоматизацията в дигиталната криминалистика.

References

- [1]Уча право
<https://uchapravo.com/%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0/>
- [2] Националният институт по криминалистика към Министерство на вътрешните работи
<https://mvr.bg/nik/%D0%94%D0%B5%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D0%B8/%D0%94%D0%B5%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B8-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8/%D0%94%D0%B5%D0%B9%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8/%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80-%D0%B8%D0%B7%D1%81%D0%BB%D0%B5%D0%B4%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B8-%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0>
- [3] DEV.BG
<https://dev.bg/digest/atos-cybersecurity-antoan-hristov-velizar-dimitrov-interview-dc03/>
- [4] Европейски парламент
<https://www.europarl.europa.eu/topics/bg/article/20200327STO76003/kak-da-se-zashchitite-ot-kiberataki>
- [5] Какво е фишинг? | Microsoft Security
<https://www.microsoft.com/bg-bg/security/business/security-101/what-is-phishing>
- [6] Национална агенция за приходите
<https://nra.bg/wps/portal/nra/za-nap/Zashtita-na-lichnite-danni/phishing-kak-da-se-predpazim>
- [7] Как AI подобрява цифровата криминалистика
<https://www.unite.ai/bg/%D0%BA%D0%B0%D0%BA-AI-%D0%BF%D0%BE%D0%B4%D0%BE%D0%B1%D1%80%D1%8F%D0%B2%D0%B0-%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%82%D0%B0-%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0/>