Journal of Social Order

Vol 15. No.1, Spring 2023

Organizational Strategic Environment Recognition in Internet Fraud (with a Law Enforcement-Social Approach)

Received: 16, January, 2023
Accepted: 20, March, 2023
Article type: Research Article
PP: 89-124
DOI:
10.22034/entezam.2023.1273117.2503

Mustafa Negahban
PhD Candidate in Criminalistics, Amin Police University, Tehran, Iran. Email: Mostafanegahban1354@gmail.com

Lotfali Bakhtiari
Professor in Strategic Management and Future Research, Amin Police University, Tehran, Iran (Corresponding Author). Email: a.bakhti51@gmail.com

Hossein Vafaadar
Associate Professor, Department of Criminalistics, Amin Police University, Tehran, Iran. Email: vafadar.hosein@yahoo.com

Yousef Mohammadi Moghaddam
Professor, Department of Management, Amin Police University, Tehran, Iran. Email: you-mohammad@yahoo.com

This article is a PhD dissertation entitled "Criminalistics Strategies for Scam" at Amin Police University.

Abstract

Background and objectives: The environment is surrounded by many factors affecting human actions and behavior. The fraud, which is an environmental phenomenon, is affected by destructive environmental factors. Therefore, the increasing development of technology has led to new ways that the offenders use. So criminalization also requires a specific dynamics to make its methods of continuous change. Investigating the context of the formation of internet fraud mass plays an important role in this change and dynamics. This study sought to understand the strategic organizational environment in the criminalization of Internet fraud (with a law enforcement-social approach).

Methodology: The type of research is applied and the research method is descriptive-analytical and the statistical population of the research was 85 commanders, managers and professors of the police, and the sample size was specified by 70 people using the Morgan table. The method of data collection was a library and field, and the collection tool was a note-taking (both physical and internet) and a researcher-made questionnaire whose content and face validity were confirmed by experts and its reliability was obtained using Cronbach's alpha coefficient test (0.87). The data analysis was performed using Friedman's ranking test.

Findings: In the component of organizational opportunities, the indicators of the existence of national, regional and international databases; the existence of legal, legal capacities, upstream opportunistic documents; and the existence of resources and secretaries to help collect information to accelerate the reduction of Internet fraud are ranked first to third. In the component of organizational threats, the increasing development indicators of internet fraud in real and virtual space; the existence of an economic, social and cultural context and many motivations to commit the crime of internet fraud; the lack of experienced judges and specialized prosecutions for Internet fraud crimes came first to third.

Results: Considering organizational opportunities and threats (such as the use of artificial intelligence capabilities, providing interactive training between judicial and law enforcement, establishing a comprehensive information system and adopting legal approach), the success of the police in the crime of internet fraud will increase.

Keywords: Strategic environment recognition, Crime, Scam, Internet fraud, Criminalistics, Offender identification.

Citation(APA): Negahban, Mustafa; Bakhtiari, Lotfali; Vafaadar, Hossein; Mohammadi Moghaddam, Yousef. (2023). "Organizational Strategic Environment Recognition in Internet Fraud (with a Law Enforcement-Social Approach)", *Journal of Social Order*, 15(1), pp. 89-124.
Doi: 10.22034/entezam.2023.1273117.2503

نشریه علمی انتظام اجتماعی

سال پانزدهم/ شماره اول/بهار ۱۴۰۲

محیط‌شناسی راهبردی سازمانی در جرم یابی کلاه‌برداری اینترنتی (با رویکرد انتظامی ــ اجتماعی)

دریافت: ۱۴۰۱/۱۰/۲۶

پذیرش: ۱۴۰۱/۱۲/۱۹

نوع مقاله: مقاله پژوهشی

صص: ۸۹-۱۲۴

شناسه دیجیتال(DOI):

10.22034/entezam.2023.1273117.2503

مصطفی نگهبان

دانشجوی دکتری رشته جرم¬یابی دانشگاه جامع علوم انتظامی امین، تهران ایران. رایانامه:

mostafanegahban1354@gmail.com

لطفعلی بختیاری

استاد گروه مدیریت راهبردی و آینده¬پژوهی، دانشگاه جامع علوم انتظامی امین. تهران. ایران. (نویسندهٔ مسئول). رایانامه:

a.bakhti51@gmail.com

حسین وفادار

دانشیار گروه کشف جرائم دانشگاه جامع علوم انتظامی امین، تهران، ایران. رایانامه:

vafadar.hosein@yahoo.com

یوسف محمدی‌مقدم

استاد گروه مدیریت دانشگاه جامع علوم انتظامی امین، تهران، ایران. رایانامه:

you-mohammad@yahoo.com

این مقاله، مستخرج از رسالهٔ دکتری با عنوان «راهبردهای جرم‌یابی کلاه‌برداری» رشته جرم‌یابی دانشگاه جامع علوم انتظامی امین است.

چکیده

زمینه و هدف: محیط با عوامل زیادی که بر اعمال و رفتار انسان تأثیر می‌گذارد احاطه شده است. کلاه‌برداری که پدیده‌ای محیطی است تحت تأثیر عوامل محیطی مخرب می‌باشد؛ لذا توسعهٔ روزافزون فناوری، شیوه‌های نوینی را پیش می‌کشد که بزهکاران از آن‌ها بهره می‌برند؛ پس جرم‌یابی نیز مستلزم پویایی خاصی است تا شیوه‌های آن تغییر مستمر داشته باشد. بررسی بسترهای شکل‌گیری جرم کلاه‌برداری اینترنتی در این تغییر و پویایی نقش بسزایی دارد. این پژوهش به دنبال شناخت محیط‌شناسی راهبردی سازمانی در جرم‌یابی کلاه‌برداری اینترنتی (با رویکرد انتظامی ـ اجتماعی) بود.

روش: نوع تحقیق، کاربردی و روش پژوهش، توصیفی ـ تحلیلی و جامعهٔ آماری تحقیق تعداد ۸۵ نفر از فرماندهان و مدیران و استادان حوزهٔ جرم‌یابی پلیس بوده‌اند و حجم نمونه به تعداد ۷۰ نفر و با استفاده از جدول مورگان تعیین شد. روش گردآوری داده‌ها، کتابخانه‌ای و میدانی بوده و ابزار گردآوری نیز فیش (اعم از فیزیکی و اینترنتی) و پرسش‌نامهٔ محقق‌ساخته بود که روایی محتوایی و صوری آن به‌وسیلهٔ خبرگان و صاحب‌نظران و پایایی آن با آزمون ضریب آلفای کرونباخ (۰/۸۷) به‌دست آمد. تجزیه‌وتحلیل داده‌ها با استفاده از آزمون رتبه‌ای فریدمن انجام شد.

یافته‌ها: در مؤلفهٔ فرصت‌های سازمانی، شاخص‌های وجود بانک‌های اطلاعاتی ملی ـ منطقه‌ای و بین‌المللی؛ وجود ظرفیت‌های قانونی، حقوقی، اسناد فرصت‌ساز بالادستی؛ و وجود منابع و مخبرین در جهت کمک به جمع‌آوری اطلاعات در تسریع کاهش جرم کلاه‌برداری اینترنتی به‌ترتیب در جایگاه اول تا سوم قرار گرفته‌اند. در مؤلفهٔ تهدیدهای سازمانی، شاخص‌های توسعهٔ روزافزون کلاه‌برداری اینترنتی در فضای حقیقی و مجازی؛ وجود بسترهای اقتصادی، اجتماعی و فرهنگی و انگیزه‌های زیاد برای ارتکاب جرم کلاه‌برداری اینترنتی؛ کمبود قضات باتجربه و دادسراهای تخصصی ویژه جرائم کلاه‌برداری اینترنتی، به‌ترتیب در جایگاه اول تا سوم قرار گرفت.

نتیجه‌گیری: با مدنظر قراردادن فرصت‌ها و تهدیدهای سازمانی (از قبیل استفاده از قابلیت‌های هوش مصنوعی، ارائه آموزش تعاملی میان مراجع قضایی و انتظامی، ایجاد سامانهٔ اطلاع‌رسانی جامع و اتخاذ رویکرد تقنینی مانع) موفقیت پلیس در جرم‌یابی کلاه‌برداری اینترنتی بیشتر خواهد شد.

کلیدواژه‌ها: محیط‌شناسی راهبرد، جرمیابی، کلاه‌برداری، کلاه‌برداری اینترنتی، کشف جرم، شناسایی مجرم.

استناد(APA): نگهبان، مصطفی؛ بختیاری، لطفعلی؛ وفادار، حسین؛ محمدی‌مقدم، یوسف. (۱۴۰۲). « محیط‌شناسی راهبردی سازمانی در جرم یابی کلاه‌برداری اینترنتی (با رویکرد انتظامی ـ اجتماعی)». *نشریه علمی انتظام اجتماعی*، ۱۵(۱)، صص ۸۹-۱۲۴.

شناسه دیجیتال: 10.22034/entezam.2023.1273117.2503

مقدمه

«کلاه برداری» جرمی مستمر و ادامه دار است که حتی گریبان دنیای متمدن و شبکه‌ای امروزی را هم گرفته و هر سال خسارت فراوان و جبران‌ناپذیری به تجار، بازرگانان و بنگاهای مالی و بانکی تحمیل می‌کند و غالباً روابط عادی و دادوستدهای معمول بین مردم را نیز تحت شعاع قرار می‌دهد و موجب کاهش اعتماد بین افراد در معاملات و امور تجاری نسبت به یکدیگر شده و در این مورد فراجا را به عنوان متولی برقراری نظم و امنیّت در فضای حقیقی و مجازی با چالش جدیدی روبه‌رو ساخته است. براساس آمار موجود، وقوع جرم کلاه‌برداری در ده سال گذشته به‌طور متوسط حدود ۶۲/۵ درصد رشد داشته است؛ یعنی در سال ۱۳۹۰ تعداد وقوع جرم به میزان ۳۷۴۰۰ فقره بوده و در سال ۱۴۰۰ این میزان وقوع به تعداد ۵۹۸۱۳ فقره افزایش یافته است (معاونت مبارزه با جعل و کلاهبرداربرداری پلیس آگاهی فراجا مصاحبه شخصی، ۱۴۰۱).

تعداد شکایات کلاه برداری اینترنتی در سال های اخیر سیر صعودی داشته و نشان‌دهندهٔ آن است که هر سال افراد بیشتری نسبت به سال قبل مورد کلاه‌برداری اینترنتی قرار گرفته‌اند؛ به‌طوری‌که ۵۸ درصد خسارات مالی ناشی از جرائم فضای مجازی درنتیجهٔ کلاه‌برداری‌های اینترنتی است (طالبیان،۱۴۰۰، ۲۴). اگرچه امروزه کارشناسان بر این باورند که برای جلوگیری از شیوع بیشتر این جرم علاوه بر تحمیل مجازات مشدد در قانون، لازم است دستگاه های قضایی و انتظامی کشور به افراد مجرّبی مجهز شود که به اصول و قواعد جرم‌یابی نوین مسلط بوده و با سیستم پیشرفتهٔ جرم‌یابی آشنایی کامل داشته باشند تا هیچ جرم نامکشوفی باقی نماند اما با رشد فنّاوری‌های اطلاعاتی و ارتباطی و فنّاوری‌های مرتبط با آن و روبه‌رو شدن جوامع با عصر جدیدی از زندگی به نام دوران سایبری یا عصر اطلاعات و شکل‌گیری دهکدهٔ جهانی به‌واسطهٔ درنوردیدن مرزهای فیزیکی و جغرافیایی، جنبه‌های جدیدی از جرائم به‌ویژه جرائم مالی شکل گرفته و بالطبع جرم کلاه برداری اینترنتی نیز از این قاعده مستثنا نبوده است؛ بنابراین، با توجه به

پیچیدگی‌های مسیر کشف جرم کلاه‌برداری اینترنتی و لزوم تسریع کشف و دستگیری کلاه‌برداران و تأثیر آن در کاهش میزان وقوع این جرم، لازم است در حیطهٔ جرم‌یابی کلاه‌برداری اینترنتی، محیط‌شناسی راهبردی مناسب صورت گیرد، که این امر مستلزم شناخت عوامل محیطی راهبردی مؤثر بر جرم‌یابی کلاه‌برداری اینترنتی است.

از سویی دیگر، سازمان‌ها و به‌تبع آن نیروی انتظامی برای تحقق مطلوبیت‌ها (اهداف و ارزش‌ها) پدید آمده‌اند و برای آن تلاش می‌کنند. رسیدن به قله مطلوبیت‌های موردنظر (موفقیت و اثربخشی سازمان) مستلزم طی مسیر یا مسیرهای ویژه‌ای می‌باشد. روشن است که این مسیرها و شیوه‌ها و طی‌کردن آن‌ها باید متناسب با شرایط محیطی و ویژگی‌های درونی سازمان و البته در راستای تحقق مطلوبیت‌های سازمان به‌گونه‌ای انتخاب و تهیه شود که حداکثر توفیق (بهره‌وری) را به ارمغان آورد. می‌توان گفت راهبرد چنین چیزی را برای ما میسر می‌سازد. راهبرد به زبان ساده مشخص می‌سازد که کجا هستیم؛ به کجا می‌خواهیم برویم؛ و از چه راهی می‌خواهیم برویم. از این طریق، مبنایی برای هم‌سو کردن توجهات و تلاش‌های مختلف و بسیج و تخصیص مناسب منابع موجود به‌منظور تحقق مطلوبیت‌های موردنظر فراهم می‌آورد. درواقع راهبرد، طرح کلی عملیات و تدابیر لازم برای نیل به مطلوبیت‌های اساسی سازمان از طریق تعیین اهداف، اتخاذ شیوهٔ کار و تخصیص منابع مختلف و مشخص است؛ اما اگر راهبرد نداشته باشیم هدف و جهتمان مشخص نیست و دچار تشتت و پراکندگی خواهیم شد، که معنی شکست و زوال سازمان خواهد بود. برای پرهیز از چنین وضعیت نامطلوبی لزوماً باید محیط‌شناسی راهبردی مناسب و مدبرانه داشته باشیم و بر آن اساس عمل نماییم؛ به‌گونه‌ای که نقش و رسالت مهم سازمان به نحو احسن تحقق یابد. همچنین داشتن الگوی تصمیم‌گیری و اجرای هدفمند منطقی و دارای ثبات رویه و در یک کلام برخورداری از راهبرد، لازمهٔ موفقیت هر حوزه‌ای به‌خصوص حوزهٔ جرم‌یابی کلاه‌برداری اینترنتی است. در غیر این صورت، عملکرد این حوزه که سهم بسزایی در فرایند کیفری (از مرحلهٔ جمع‌آوری ادلّه تا مرحلهٔ محکومیت) دارد

از بازدهی مناسبی برخوردار نبوده و نتیجهٔ چندان مطلوبی به همراه نخواهد داشت؛ بنابراین با توجه به پیچیدگی‌های مسیر کشف جرم کلاه‌برداری اینترنتی و لزوم تسریع کشف و دستگیری کلاه‌برداران و تأثیر آن در کاهش میزان وقوع این جرم، لازم است در حیطهٔ جرم‌یابی کلاه‌برداری اینترنتی محیط‌شناسی راهبردی مناسب صورت گیرد، که این امر مستلزم شناخت عوامل راهبردی مؤثر بر جرم‌یابی کلاه‌برداری است.

لذا این پژوهش در نظر دارد تا نخست با اِشراف به چیستی کلاه‌برداری و شیوه‌های انجام آن به‌ویژه در بسترهای مجازی و اینترنتی، شناختی نسبتاً جامع نسبت از نحوهٔ عملکرد مجرمین به‌دست دهد و در ادامه نیز باتوجه به این شیوه‌های کلاه‌برداری اینترنتی به بررسی زمینه‌های شکل‌گیری این جرم بپردازد؛ زمینه‌هایی که می‌تواند تا حد زیادی به کشف جرم پیش‌گفته کمک کنند و همچنین زمینه‌ساز جلوگیری از وقوع آن‌ها باشند. در آخر نیز با شناخت و تجزیه‌وتحلیل محیطی دربارهٔ موضوع به بررسی مهم‌ترین فرصت‌ها و تهدیدهای سازمانی در جرم‌یابی کلاه‌برداری اینترنتی بپردازد. هدف اصلی پژوهشگر در انجام این تحقیق، محیط‌شناسی راهبردهای جرم‌یابی کلاه‌برداری اینترنتی با تأکید بر فرصت‌ها و تهدیدها (با رویکرد انتظامی ــ اجتماعی) است. مقالهٔ پیش رو به دنبال پاسخ به این سؤال است که محیط‌شناسی راهبردهای جرم‌یابی کلاه‌برداری اینترنتی با تأکید بر فرصت‌ها و تهدیدها (با رویکرد انتظامی ـ اجتماعی) چگونه می‌باشد؟

پیشینه و مبانی نظری

کریمی (۱۴۰۰)، در پژوهشی با عنوان «راهبردهای جرم‌یابی جرائم سازمان‌یافته مواد مخدر» راهبردهایی نظیر تقویت ساختار پلیس مبارزه با مواد مخدر متناسب با جغرافیای جرم، راهبرد افزایش بودجه عملیاتی، راهبرد اِشراف اطلاعاتی با استفاده از سامانه‌های سنجش از راه دور، توسعهٔ شبکه‌های داخلی منابع و مخبرین برای نقاط کشت، راهبرد تقویت دیپلماسی پلیسی و مرزی، راهبرد ارتقای اثربخش‌کردن و مبارزه حقیقی با مواد مخدر، طرح‌ریزی

عملیات‌های برون‌مرزی برای شناسایی و انهدام لابراتوارهای تولید مواد روان‌گردان، راهبردهای ایجاد مجتمع‌های ویژه قضایی مبارزه با مواد مخدر، تقویت آموزش و اقدامات پیشگیرانه را ازجمله مهم‌ترین راهبردهای این حوزه می‌داند.

رسولی و همکاران (۱۴۰۰)، در پژوهشی با عنوان «نقش پلیس اطلاعات-محور در جرم‌یابی کلاه‌برداری تلفنی به شیوهٔ کارت به کارت» به این نتیجه رسیده‌اند که به‌کارگیری هدفمند بانک‌های اطلاعاتی، اجرای دقیق آموزش‌های ارائه‌شده به مأمورین پلیس، تعامل بیشتر با مراجع قضایی و ایجاد بانک‌های اطلاعاتی جدید موردنیاز توسط پلیس اطلاعات‌محور، در جرم‌یابی کلاه‌برداری به شیوهٔ کارت به کارت نقش دارند. طبق پژوهش ایشان امکان دسترسی توسط پلیس آگاهی، فتا و پیشگیری در سراسر کشور جهت به اشتراک گذاشتن و مشاهدهٔ اطلاعات پرونده‌های متشکله کلاه‌برداری تلفنی، ازجمله پیشنهادهایی در راستای جرم‌یابی کلاه‌برداری به شیوهٔ کارت به کارت است.

مرتضوی و همکاران (۱۴۰۰)، در مقاله‌ای با عنوان «شناسایی عوامل راهبردی مؤثر بر جرم‌یابی با رویکرد آینده‌پژوهی» به این نتیجه رسیده‌اند که هفده عامل به‌عنوان عوامل راهبردی بر جرم‌یابی مؤثر هستند؛ ازجمله: بهره‌برداری از کار تیمی، تجزیه‌وتحلیل اطلاعات جرائم، وجود بانک‌های اطلاعاتی مجرمان سابقه‌دار و حوزه‌های فعالیتی آن، داشتن تجهیزات فنی و آزمایشگاهی مجهز برای استخراج ادلّه جرم و... که می‌بایست به‌منظور موفقیت هر چه بیشتر مورد توجه قرار گیرند.

دباغ و همکاران (۱۴۰۰)، در پژوهشی با عنوان «طراحی الگوی راهبردی زیست‌بوم نوآوری در حوزهٔ سلامت» به این نتیجه رسیده‌اند که عواملی همچون تأسیس دانشگاه و مؤسسات پژوهش‌محور، کوتاه کردن روند اخذ مجوزهای لازم، حمایت دولت از تحقیق و توسعه، مشوق‌های مادی و معنوی، افزایش سرمایه‌گذاری ریسک‌پذیر، به‌عنوان عوامل راهبردی بر نوآوری حوزهٔ سلامت مؤثر هستند.

نظری منظم (۱۳۹۹)، در پژوهشی با عنوان «ارائه الگوی جرم‌یابی کلاه‌برداری در فضای سایبر» به این نتیجه رسیده‌اند که تعامل پلیس با مقامات قضایی، آشنایی مقامات قضایی با مبانی فنی و حقوقی، تجهیزات مدرن، علم و آگاهی از علوم رایانه‌ای توسط کارآگاهان سایبری در کشف جرم کلاه‌برداری سایبری تأثیر دارد.

بارانی و همکاران (۱۳۹۹)، در پژوهشی با عنوان «نقش اقدامات پلیس در پیشگیری از جرائم کلاه‌برداری در حوزهٔ کسب‌وکار» به این نتیجه رسیده‌اند که چهار شاخص ۱- افزایش تلاش (زحمت) موردنظر برای دستیابی به هدف؛ ۲- افزایش خطرات موردنظر برای ارتکاب جرم؛ ۳- کاهش دستاوردهای مورد انتظار از جرم یا همان سود حاصله؛ و ۴- حذف معاذیر یا ازبین‌بردن عواملی که باعث تحریک یا تشویق فرد در ارتکاب جرم می‌شود، نقش مهمی در پیشگیری از جرم کلاه‌برداری دارند.

طالبیان و کریمی (۱۳۹۹)، در پژوهشی با عنوان «بررسی الگوهای جرم‌یابی» به این نتیجه رسیده‌اند که رشتهٔ جرم‌یابی به‌عنوان یک دانش پلیسی و یکی از شاخه‌های مطالعاتی علوم جنایی، قطعاً دارای اصول و قواعدی بوده که بر آن استقرار داشته، اما مسلماً از ابتدا از سبک و اسلوب سازمان‌یافته‌ای برخوردار نبوده و متأسفانه در این حوزه در مقایسه با علوم دیگر و با وجود تنوع در فرایندهای فنی مؤثر در آن، محققان با فقدان اصول و نظریه‌های تئوریک مواجه هستند. اکنون پس از گذشت سالیان متمادی، جرم‌یابی به‌تازگی از یک نقشهٔ راه برخوردار شده که بدون تردید با رعایت و اجرای اصول آن، کشف علمی جرم به صورتی ساختارمند و محکمه‌پسند صورت خواهد گرفت.

حسینی (۱۳۹۹)، در پژوهشی با عنوان «نقش فناوری‌های علمی و پلیسی در کشف جرم» به این نتیجه رسیده است که ابزارها و روش‌های مختلفی برای کشف جرم و دستگیری مجرم وجود دارد که در به‌سرانجام‌رسیدن تحقیقات کمک شایانی می‌نمایند که عبارت‌اند از: نقش اثرانگشت در دستگیری جنایت‌کاران، عوامل بو، صوت و رنگ در تشخیص جنایت‌کاران، آزمایشگاه‌های کشف جرم پلیس، تشخیص هویت با استفاده از DNA، نانو تکنولوژی،

بازجویی‌های مدرن و... که به‌وسیلهٔ آن‌ها کشف جرائم سرعت پیدا می‌کند و روند انجام کارها تسهیل پیدا می‌کند. بر این اساس استفاده از فناوری‌های نوین و علوم و فنون مدرن توسط پلیس می‌تواند در کشف جرائم سرعت بخشیده و قضات را در صدور احکام واقعی و حقیقی کمک کرده و جامعه را به سمت عدالت‌خواهی و عدالت‌محوری پیش ببرد.

نظری منظم و همکاران (۱۳۹۸)، در پژوهشی با عنوان «بررسی عوامل مؤثر بر جرم‌یابی کلاه‌برداری در فضای سایبر» به این نتیجه رسیده‌اند که همکاری پلیس با مقامات قضایی، تجهیزات مدرن، علم و آگاهی از علوم رایانه‌ای توسط کارآگاهان سایبری و... در کشف جرم کلاه‌برداری اینترنتی تأثیر دارد.

اکشولا و آدتا[1] (۲۰۱۳)، در پژوهشی با عنوان «ماهیت، علل و پیامدهای جرائم سایبری در ایالات زاریا کادونا، نیجریه» به این نتیجه می‌رسند که با شناخت ماهیت و اثرات جرائم سایبری، همیشه چالش‌های جدید و غیرمنتظره‌ای برای در امان ماندن از جنایتکاران و تروریست‌های سایبری وجود دارد؛ اما این مهم فقط با همکاری افراد و دولت ممکن است. آن‌ها عقیده دارند بزهکاران جرائم سایبری دور از نظر نیستند؛ آن‌ها برادران، دوستان، همکاران، اقوام و همسایگان بزه‌دیدگان هستند که می‌توانند تحت شرایط مناسب با ارتباطات درست و مثبت، جهت‌گیری، آموزش و توانمندسازی مورد بازداری قرار گیرند.

اسرت [2] (۲۰۲۰)، در پژوهشی با عنوان «علل بزه‌دیدگی از جرائم اینترنتی» به این نتیجه رسیده‌اند نوجوانان بیشترین قربانیان جرائم اینترنتی هستند. نگرش خودکنترلی پایین، رفتارهای روان‌پریشانه، رفتار تقلیدگرایانه، نابرابری اجتماعی، استفاده بیشتر از تلفن همراه و اینترنت را به‌عنوان عمده‌ترین دلایل مزاحمت‌های اینترنتی بیان نموده که در این مورد افراد مسن جامعه مسئول کلاه‌برداری آنلاین هستند. دلایل کلاه‌برداری آنلاین هم آسیب‌پذیری، حرص و آز، اعتماد، ساده‌لوحی، احساسات شدید، دسترسی به اینترنت از خانه، ناآگاهی

1- Okeshola & Adeta
2- Osrat

و گزارش‌نکردن جرائم اینترنتی اعلام کرده‌اند. در پایان هم راهبردهای پیگیری، هشدار، تحریم و مجازات و برنامه‌های آموزشی را به‌عنوان راهکار موضوع پیشنهاد نموده‌اند.

پراباکاران[1] (۲۰۱۸)، در پژوهشی با عنوان «بررسی تحلیل تکنیک‌های کشف جرم استفاده از داده‌کاوی و یادگیری ماشین» به این نتیجه رسیده‌اند که حجم بسیار زیاد داده‌های مربوط به جرم‌ها و مجرمین از یک‌سو و وجود روابط معنایی پیچیده و نامحسوس میان این اطلاعات از دیگر سو، جرم‌شناسی را به یکی از مهم‌ترین حوزه‌های کاربردی داده‌کاوی مبدل نموده است؛ که در این مورد تحقیقات جنایی یک برنامهٔ جالب برای پردازش ویژگی‌های جرم برای کمک به جامعه در جهت بهتر زندگی‌کردن دارد.

در طرح تحقیقاتی که با موضوع «بررسی کلاه‌برداری سایبری از بانک‌های خصوصی و دولتی هند» و با حمایت دانشکده علوم و فناوری اطلاعات دانشگاه ایالتی پنسیلوانیا توسط کومار آشوین و همکاران[2] (۲۰۱۳) انجام شده به این نتیجه رسیده است: تأثیر استفاده از تکنولوژی در بخش خدمات مالی برای توسعه امور امری فوق‌العاده مؤثر بوده است؛ اما وابستگی شدید در تجهیزات الکترونیکی و دیجیتال به یک تهدید جدی برای ایمنی و قابلیت اطمینان از عملیات مالی تبدیل شده است. با روند رو به رشد انجام معاملات به‌صورت آنلاین و در فضای سایبر، تعدادی از فن‌آوری‌های بانکی مورد سوءاستفاده قرار گرفته و هر روز بیشتر مردم تحت تأثیر قرار می‌گیرند. پرداخت آنلاین، دستگاه‌های خودپرداز، کارت‌های الکترونیکی و کلاه‌برداری سایبری در معامله‌های بانک‌ها با اتخاذ تدابیر مناسب در بروز خسارات فراوان به خود و مشتریان نقش داشته‌اند.

لا اوت، آنتونیوس[3] (۲۰۱۵)، در پژوهش خود با عنوان «بررسی جرم کلاه‌برداری از کارت‌های اعتباری در حقوق جزای اندونزی» هدف از تحقیق

1- Prabakaran , Mitra
2- kumar , Ashvine & et al
3- la ott, & Antonius

خـــود را تعیـــین ترتیبـــات قـــانونی در رســـیدگی بـــه جـــرم مـــذکور، اســـتفاده از جرم‌انگـاری کـلاه‌بـرداری کـارت‌هـای اعتبـاری از طریـق افـزایش مجـازات را خواسـتار شده و یکپـارچگی و برخـورد قـانونی و قضـایی بـا کـلاه‌بـرداری از طریـق تحـریم‌هـای کیفری را خواستار شده‌اند.

ســـیمون[1] و همکـــاران (۲۰۱۳)، در پـــژوهش خـــود بـــا عنـــوان «راهکـــار اصـــلی تشـخیص کـلاه‌بـرداری سـایبری بـا اسـتفاده از تکنیـک پیشـرفته ضـد فیشـینگ» معتقدنـــد در اجـــرای سیاســـت معـــاملات بـــدون پرداخـــت پـــول نقـــد کشـــورهای درحـال‌توسـعه بـه‌تـدریج دوران گـذار از پـول نقـد بـه یـک اقتصـاد الکترونیکـی را مبنـای کـار قـرار مـی‌دادنـد هـم‌اکنـون اقـدام بـه گسـترش اعمـال مجرمانـه و بهـره‌بـرداری از نقـاط ضـعف ممکـن در سیسـتم‌هـای پرداخـت الکترونیکـی از طریـق ارتکـاب کـلاه‌بـرداری نمـوده‌انـد. در ایـن مقالـه رویکـرد ارتقاءیافتـه در تشـخیص حملات فیشـینگ در جلـوگیری از خـروج غیرمجـاز و انتقـال آنلایـن پـول ارائـه شـده اسـت. ایـن تحقیـق بـا اسـتفاده از روش تحلیـل محتـوا، بیومتریـک و بـا اسـتفاده از احـراز هویـت از طریـق اثرانگشـت اقـدام بـه ارائـه یـک مـدل نمـوده اسـت. در ایـن مقاله، اثربخشی مدل ارائه‌شـده بـا انجـام چنـد آزمـایش بـه اثبـات رسـیده و بـه نتـایج خوب و قابل‌توجهی منجر شده است.

یوپینـگ و همکـاران[2] (۲۰۰۴) در پـژوهش خـود بـا عنـوان «بررسـی روش‌هـای تشـخیص کـلاه‌بـرداری سـایبری» بـه ایـن نتیجـه رسـیده‌انـد، افـزایش چشـمگیر کلاه‌بـرداری سـایبری، منجـر بـه ازدسـت‌دادن میلیاردهـا دلار در هـر سـال در سراسـر جهان می‌شود. بـه همـین علـت، تکنیـک‌هـای مـدرن در کشـف کـلاه‌بـرداری بـه‌طـور مستمر تکامل یافتـه و کـاربری بـرای بسـیاری از زمینـه‌هـای کسـب‌وکـار پیـدا نمـوده اسـت. تشـخیص کـلاه‌بـرداری نیازمنـد نظـارت بـر رفتـار کـاربران بـه‌منظـور بـرآورد، شناسـایی و یـا جلـوگیری از رفتـار نـامطلوب آنـان اسـت. در ایـن تحقیـق رفتـار نامطلوب یـک اصـطلاح گسـترده اسـت ازجملـه تقلـب، نفـوذ، و حسـاب فـرد متخلـف، در ایـن مقالـه یـک نظرسـنجی از تکنیـک‌هـای مـورد اسـتفاده در تشـخیص

1- Simon & et al
2- Yuping, Hong & et al

کـلاه‌بـرداری از کـارت اعتبـاری، ارتباطـات راه دور و تشـخیص نفـوذ بـه کـامپیوتر صـورت گرفتـه اسـت. هـدف از ایـن مقالـه ارائـه یـک بررسـی جـامع از تکنیـک‌هـای متفاوت و متنوع در تشخیص کلاه‌برداری سایبری است.

جمع‌بندی پیشینه‌های تحقیق

پیشـینهٔ تحقیـق حـاکی از آن اسـت کـه وجـه مشـترک همـهٔ فعالیـت‌هـای علمـی انجـام‌شـده در حـوزهٔ راهبردهـای جـرم‌یـابی، نگـاه کلـی بـه موضـوع اسـت؛ در ایـن فراینـد، تحقیـق علمـی قابـل‌تـوجهی کـه محـیط‌شناسـی راهبـردی در جـرم‌یـابی کـلاه‌بـرداری اینترنتـی را بـه‌صـورت ویـژه مـورد توجـه قـرار داده باشـد، یافـت نشـد؛ بنابراین، با اذعـان بـه اینکـه پیشـینهٔ تحقیـق، اهمیـت موضـوع راهبردهـای جـرم‌یـابی کلاه‌بـرداری رایانـه‌ای را در مأموریـت‌هـای جـرم یابـان نشـان مـی‌دهـد، بایـد گفـت از خلأهـای موجـود در ایـن زمینـه و لـزوم نگـاه تخصصـی بـه مبحـث محـیط‌شناسـی راهبردی در جرم‌یابی کلاه‌برداری رایانه‌ای حکایت دارد.

شایان ذکـر اسـت پیشـرفت‌هـای روزافـزون تکنولـوژی جوامـع را نـاگزیر مـی‌سـازد تـا همـواره از پویـایی لازم بـرای کشـف جـرائم و پیشـگیری از وقـوع آن‌هـا برخـوردار باشند و از همـین رو، ایـن پـژوهش در راسـتای پـژوهش‌هـایی اسـت کـه سـابقاً انجـام شده و بـه فراخـور طبیعـت تکنولـوژی نیـاز بـه مطالعـات آتـی و همسـویی بـا جریـان موجود منتفی نیست.

جرم‌یـابی و بسـتر شناسـی آن حـوزه‌ای گسـترده اسـت کـه مطالعـات جـامعی در رابطه با آن‌ها در علم حقـوق جـزا انجـام شـده و نظریـه‌هـای متعـددی شـکل گرفتـه است و در این پژوهش با در نظـر داشـتن ایـن دو مفهـوم بـه بهـره‌گیـری از آن‌هـا در رابطه با کلاه‌برداری اینترنتی پرداخته‌ایم.

مفهـوم محـیط‌شناسـی راهبـردی بـه صـورت‌هـای گونـاگونی تعریـف شـده اسـت؛ ازجملـه اینکـه محـیط‌شناسـی نـوع خاصـی از شـناخت اسـت کـه بـا هـدف ارائـه

تحلیل‌های مرتبط با دستیابی به اهداف جام سازمان، شرکت یا دولت انجام می‌پذیرد. (مک‌دوئل[1]، ۲۰۰۸، ۳۴).

محیط‌شناسی راهبردی فرایند و محصول توسعهٔ فهم و دانش عمیق از محیط به‌منظور پشتیبانی تصمیم‌سازی‌های راهبردی است. مقصود از محیط‌شناسی راهبردی، دستیابی به دانشی کارکردی یا هشدار پیش‌آگاهانه به تصمیم‌سازان است. مفهوم کلیدی در این جمله، دانش کارکردی است .درواقع دانش محیط‌شناسی طراحی شده تا به عمل کمک کند و در غیر این صورت دانشی مرده خواهد بود (کوییگین[2]، ۲۰۰۷، ۴۵).

صاحب‌نظران علم جزا، تعاریف متعددی از جرم‌یابی ارائه داده‌اند؛ ازجمله این تعاریف کاربردی می‌توان به این موارد اشاره کرد: گلدوزیان در کتاب *بایسته‌های حقوق جزای عمومی* تشریح می‌کند که علوم جرم‌یابی شامل مجموعه علوم و دانش‌های فنی است که برای کشف جرائم و تشخیص هویت و دستگیری مجرمین مورد استفاده قرار می‌گیرد (گلدوزیان، ۱۳۸۸، ۴۹).

همچنین هیئت جرم‌یابی آمریکا، جرم‌یابی را رشته حرفه‌ای و علمی مدیریت تشخیص، تعیین، تمایز و ارزیابی ادله مادی با استفاده از علوم فیزیکی و طبیعی در موضوعات علوم حقوقی تعریف کرده است (مؤذن‌زادگان و حمیدزاده، ۱۳۹۲، ۱۰۰). به‌هرحال، با لحاظ نمودن همه تعاریف و مفاهیم پیش‌گفته، می‌توان جرم‌یابی را علمی دانست که با مطالعهٔ پدیده‌های مجرمانه، شناسایی مجرمان، حفظ آثار، جمع‌آوری دلایل و مدارک ارتکاب جرم و نحوهٔ ارتکاب بزهکاری و نیز چگونگی تشخیص هویت و اثبات جرم در جهت مساعدت به نظام عدالت کیفری می‌پردازد تا درنهایت نظام کیفری بتواند واکنشی متناسب با کنش‌های مجرمانه در جهت تأمین اهداف شخصی و اجتماعی جرم‌انگاری رفتارها داشته باشد.

1- Mc Dowell
2- Quiggin

«کلاه‌برداری» فعالیتی است که در محیط اجتماعی روی می‌دهد و پیامدهای جدی برای اقتصاد، شرکت‌ها و افراد به همراه دارد. این مسئله آلودگی‌ای فرصت‌طلبانه است که در صورت پیوند میان طمع و امکان فریب رخ می‌دهد. یک تعریف آکادمیک و عام که از کلاه‌برداری وجود دارد آن است که گفته شده: در کلاه‌برداری، کلاه‌برداران برای دور کردن قربانی بی‌گناه از دارایی و حق قانونی خود از راه فریب برای نفع شخصی تمرکز دارد. این فریب شامل واژه‌ها یا رفتارهای گمراه‌کننده یا غفلت و پنهان‌کردن حقایق است که زیان حقوقی را به همراه دارد (سیلورستون و شیتز[1]، ۱۳۹۱، ۶۵). کلاه‌برداری در حقوق موضوعه به دو دستهٔ سنتی و نوین یا رایانه‌ای تقسیم می‌شود؛ در کلاه‌برداری اینترنتی با اینکه نتیجه آن که عبارت از بردن مال دیگری است با کلاه‌برداری سنتی برابر است اما عملیات فریبکارانه در بستر اینترنتی انجام می‌شود و نیاز به حضور فیزیکی فرد کلاه‌بردار وجود ندارد. بر طبق مادهٔ ۱۳ قانون جرائم رایانه‌ای، «هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی یا ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یک‌صد میلیون ریال یا هر دو مجازات محکوم خواهد شد.» در بیان تفاوت میان کلاه‌برداری سنتی و اینترنتی می‌توان این‌گونه گفت که کلاه‌برداری رایانه‌ای آن‌گونه که در اسناد بین‌المللی و در قوانین داخلی یعنی مادهٔ ۱۳ قانون جرائم رایانه‌ای بدان اشاره شده است با تکیه بر فناوری برتر صورت می‌گیرد و به‌عبارت‌دیگر استفاده غیرمجاز از سیستم‌های رایانه‌ای و مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم، به‌منظور تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری، کلاه‌برداری رایانه‌ای محسوب می‌شود، درحالی‌که در کلاه‌برداری سنتی استفاده غیرمجاز از سیستم رایانه‌ای و مخابراتی و همچنین

1- Silverston & Sheets

ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم لازم نیست بلکه ارتکاب هر نوع عمل متقلبانه توأم با سوءنیت که منجر به بردن مال دیگری شود کلاه‌برداری خواهد بود.

محیط‌شناسی راهبردی در خصوص جرم‌یابی کلاه‌برداری اینترنتی مستلزم آن است که جرم‌یابان احاطه کامل به شیوه‌های انجام کلاه‌برداری توسط بزهکاران داشته باشند و با توجه به پیشرفت تکنولوژی و ارتباطات، این شیوه‌ها همه‌روزه در حال گسترش است. در این پژوهش نخست به معرفی برخی از شایع‌ترین شیوه‌های انجام کلاه‌برداری اینترنتی پرداخته و در ادامه با توجه به این شیوه‌ها اقدام به ارائهٔ شاخص‌های احصاء شده در دو بُعد محیط‌شناسی راهبردی یعنی بُعد فرصت‌ها و تهدیدها که بسترساز جرم‌یابی و کشف و شناسایی مجرمان است، خواهیم پرداخت.

۱- شیوه‌های انجام کلاه‌برداری اینترنتی

اصولاً کلاه‌برداری‌های رایانه‌ای یا اینترنتی به دو گروه عمده و اصلی تقسیم می‌شوند که در این گفتار هر کدام از آن‌ها به تفکیک مورد بررسی قرار می گیرند. باید توجه داشت که با توسعهٔ فناوری دیجیتال نمی‌توان شیوه‌های کلاه‌برداری اینترنتی را منحصر در مجموعه محدودی دانست و با توسعه تکنولوژی شیوه‌های نوینی توسط کلاه‌برداران به کار بسته می‌شود؛ لذا موارد مذکور در ذیل جنبه تمثیلی خواهند داشت. مضاف بر این، برخی از مصادیق کلاه‌برداری رایانه‌ای قابل‌تطبیق با مادهٔ ۱۳ قانون جرائم رایانه‌ای نیست و باید آن‌ها را از مصادیق مادهٔ ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاه‌برداری دانست.

۱-۱. کلاه‌برداری رایانه‌ای ارادی یا اختیاری

این گروه شامل آن دسته از انواع کلاه‌برداری است که طعمه با فریب کلاه‌برداران به چرخه جرم وارد و به‌صورت ارادی و اختیاری مبادرت به همکاری با مجرمان نموده و درنهایت از طریق پرداخت وجه و یا واریز پول، خود را قربانی می‌کند که برای این شیوه از کلاه‌برداری رایانه‌ای، می‌توان

اصطلاح ارادی یا اختیاری را به کار برد. ازجمله شیوه‌هایی که در این دسته قرار می‌گیرند می‌توان به موارد زیر اشاره کرد:

۱-۱-۱. کلاه‌برداری نیجریه‌ای

این نوع کلاه‌برداری یکی از رایج‌ترین و البته قدیمی‌ترین شیوه‌های کلاه‌برداری بوده و همچنان پرطرفدار است. در این روش کلاه‌بردار کارش را با ارسال پیامک و ایمیلی آغاز و ادعا می‌کند که قرار است مبلغ کلانی پول به دستش برسد و چون مبلغ پرداختی برای تکمیل بیمه آن ندارد؛ چنانچه به او کمک کنید ممکن است نیمی از آن را با شما تقسیم کند. اگر طعمه‌ها اغفال شوند، از آن‌ها خواسته می‌شود ابتدا مبلغ کمی را برای کمک به پرداخت هزینه بانکی ارسال کنند. معمولاً این مبلغ کمتر از ده دلار است؛ اما ارسال پول توسط قربانی، آغازی برای کلاه‌برداری بیشتر خواهد بود؛ زیرا کلاه‌بردار هر بار به بهانه‌های مختلف تقاضای مبلغی می‌نماید و قربانی از یک‌سو به‌دلیل از دست دادن پول خود و برای جبران آن و از سوی دیگر به‌واسطهٔ طمع برای رسیدن به نیمی از پول‌های خیالی، بازی را ادامه و متأسفانه هر بار مبلغ بیشتری را از دست می‌دهد و چون این نوع کلاه‌برداری ابتدا از سوی اتباع کشور نیجریه رخ داد به آن کلاه‌برداری نیجریه‌ای می‌گویند .از سویی هم این روش به نام‌های زهر نیجریایی و کلاه‌برداری ۴۱۹ نیز معرفی می‌شود؛ زیرا این عمل در مادهٔ ۴۱۹ قانون مجازات نیجریه، جرم شناخته شده است.

۱-۱-۲. کلاه‌برداری از طریق ایمیل جعلی

در این روش، مجرمان اینترنتی با نفوذ به نشانی پست الکترونیکی چنین افرادی، از دادوستد آن‌ها با شرکت‌های بین‌المللی باخبر و در ادامه، ابتدا پست-الکترونیکی مشابه شرکت با تغییراتی کوچک در یک یا دو حرف ساخته و با کاربر وارد گفت‌وگو می‌شوند. آن‌ها هنگامی که قرار است فرد خریدار پول واریز کند با پست‌الکترونیکی جعلی، شماره‌حساب خود را داده و فرد تاجر نیز که متوجه تغییر کوچک در نشانی پست‌الکترونیکی نمی‌شود، مبلغ مورد معامله را به حساب کلاه‌برداران می‌ریزد. معمولاً طعمه‌های این روش، تجار و بازرگانان

هستند که به‌راحتی و برای لحظه‌ای غفلت، میلیون‌ها و حتی میلیاردها تومان سرمایه‌شان را برای کلاه‌برداران ناپیدا و ناشناس واریز می‌کنند.

۱-۱-۳. کلاه‌برداری از طریق سایت‌های مجازی خریدوفروش

با گسترش روزافزون فضای مجازی و وسیع‌تر شدن پهنهٔ فعالیت‌های آن اغلب افراد، شرکت‌ها و مؤسسات مالی، معاملات و خدمات خریدوفروش کالاهایشان را در این بستر انجام می‌دهند؛ لیکن در این مورد کاربر با خرید وسیله‌ای پول آن را به‌صورت اینترنتی واریز می‌کند اما هرچه منتظر می‌ماند وسیله موردنظر به دستش نمی‌رسد یا در مواردی پیش آمده که وسیلهٔ دیگری با کیفیّت پایین به مشتری فروخته می‌شود و پس از تحویل پول، دیگر از فروشنده خبری نمی‌شود.

۱-۲. کلاه‌برداری رایانه‌ای عدوانی یا اجباری

در این گروه، کلاه‌بردار به‌صورت عدوانی و یا اجباری، طعمه را قربانی می کند؛ بدین‌صورت که شرایطی متناسب با نیاز افراد در بستر فضای مجازی فراهم و پس از کشاندن طعمه به مهلکه جرم، او را خلع سلاح کرده و تقریباً شرایطی شبیه سرقت برای خود مهیا و مال قربانی را به‌طور عدوانی برداشت می‌کند. برای این روش از کلاه‌برداری نیز می‌توان از اصطلاح عدوانی و یا اجباری استفاده کرد. ازجمله شیوه‌هایی که در این دسته قرار می‌گیرند می‌توان به موارد زیر اشاره کرد:

۱-۲-۱. کلاه‌برداری از طریق فیشینگ

فیشینگ از شاخص‌ترین شگردهای کلاه‌برداری رایانه‌ای است که در آن کلاه‌برداران به رمز عبور و نام کاربری کارت‌های اعتباری افراد دسترسی پیدا می‌کنند. این روش از ساده‌ترین و محبوب‌ترین روش‌های کلاه‌برداری موجود در جهان است. فیشینگ در معنای لغوی یعنی «رسید قبض» ولی در اصطلاح عامه سیاه‌پوستان آمریکا به معنای نقاب، ماسک و یا گونه‌ای از تغییر چهره که صورت اصلی قابل‌تشخیص نباشد. در تعریف دیگر، فیشینگ را اصطلاحاً نوعی سرقت آنلاین از طریق رمزگیری معرفی و آن را مخفف صید رمز عبور از طریق

طعمه‌گذاری می‌دانند. رمزگیری یا فیشینگ به‌عنوان یک جرم، شامل مهارت های فریبنده مختلف از طریق فن‌آوری و مهندسی اجتماعی است که از جعل هویت و بازی کردن در نقش دیگران برای دستیابی به اطلاعات محرمانه و سپس سرقت پول افراد استفاده می‌کند. این اطلاعات می‌تواند شامل نام کاربری، رمز عبور، اطلاعات کارت‌های اعتباری، کد ملی، رمز عبور کارت‌های بانکی، تاریخ‌های تولد و آدرس‌های ضروری و مهم باشد (غروی، ۱۳۹۵، ۴۳).

در حال حاضر، «فیشینگ» جرمی است که رتبهٔ نخست جرائم اینترنتی کشور را به خود اختصاص داده و هر مجرم اینترنتی حتی هکرهای شانزده‌ساله نیز آن را مرتکب می‌شوند. مجرمانی که از این روش استفاده می‌کنند، ابتدا با ساختن صفحه‌ای جعلی مشابه صفحه اصلی بانک‌ها؛ شماره کارت، رمز دوم و کد ۲ CVV را به‌دست آورده و در فرصتی مناسب اقدام به برداشت از حساب کاربر می‌کنند.

۱-۲-۲. کلاه‌برداری با روش اسمیشینگ

یکی از شکل‌های فیشینگ، کلاه‌برداری اسمیشینگ است که با استفاده از پیامک صورت می‌گیرد و از شخص درخواست می‌شود تا با شماره خاصی تماس بگیرد و یا به سایتی وارد شود. این روش همانند روش کلاه‌برداری فیشینگ با ایمیل است؛ با این تفاوت که کلاه‌برداران از پیامک استفاده می کنند. در این روش ممکن است کلاه‌برداران خود را از طرف بانک معرفی و اعلام کنند که حساب طعمه مسدود شده و باید وارد لینک مشخصی شود و اطلاعات حساب خود را وارد کند تا اصلاح صورت پذیرد .یا کلاه‌بردار از طریق تلفن همراه و با ارسال پیامک به افراد اعلام می‌کند که مشکل درمانی خاصی داشته و به کمک نیاز دارد و بدین‌صورت با چرب‌زبانی خاصی اعتماد مخاطب را به خود جلب می‌کند.

۱-۲-۳. کلاه‌برداری از طریق ویشینگ

شکل دیگری از کلاه‌برداری‌های اینترنتی، ویشینگ نام دارد که بی‌شباهت با اسمیشینگ نیست. در این شکل قربانی یک ایمیل و یا پیامک صوتی دریافت

می‌کند و سپس همان فرایندها تکرار می‌شود. کلاه‌برداران از این روش در حال حاضر کمتر استفاده می‌کنند؛ اما در سال‌های اخیر با توجه به افزایش خریدوفروش‌های اینترنتی، بسیاری از کلاه‌برداران اقدام به تأسیس فروشگاه های مجازی نموده و یا از لوگو (نشان‌واره) و صفحه اصلی فروشگاه و سایت‌های مجازی استفاده و اهداف مجرمانه خود را دنبال می‌کنند؛ بنابراین باید توجه داشت که برای جلوگیری از کلاه‌برداری‌های اینترنتی خصوصاً انواع فیشینگ، از وب‌سایت‌هایی خرید شود که دارای نماد اعتماد الکترونیکی کسب‌وکارهای اینترنتی هستند. این نماد نشانه‌ای است که از طرف مرکز توسعهٔ تجارت الکترونیک وابسته به وزارت صنعت، معدن و تجارت به‌عنوان تأییدیه به فروشگاه‌های اینترنتی داده می‌شود.

۱-۲-۴. کلاه‌برداری با اسکیمر

در این روش، مجرمان با قرار دادن مدارهای مغناطیسی در دستگاه‌های کارت‌خوان فروشگاه‌ها به نام اسکیمر، اطلاعات بانکی مشتریان را ذخیره و با تخلیه اطلاعات ازجمله رمز دوم، کارت بانکی جعلی ساخته و حساب مشتری را خالی می‌کنند. اسکیمر یک قطعه بسیار کوچک است که سارقان آن را بر روی دستگاه‌های خودپرداز نصب می‌کنند تا با کپی‌برداری اطلاعات بانکی موجود در نوار مغناطیسی مشکی‌رنگ کارت‌ها بپردازند و گاهی اوقات با نصب دوربین بسیار کوچکی، واردکردن رمز توسط مشتری را ضبط می‌کنند و در برخی از مواقع با سؤال از مشتری، رمز را پرسیده و پس از خروج وی، رمز را یادداشت و سپس با تهیهٔ کپی از کارت مذکور، اقدام به برداشت و سرقت وجوه می‌نمایند؛ بنابراین، اسکیمینگ یعنی کپی‌کردن غیرقانونی داده‌های نوار مغناطیسی کارت بانکی روی یک کارت دیگر که از طریق دستگاه اسکیمر انجام می‌شود و اسکیمر ها دستگاه‌های الکترونیکی کوچکی هستند که انواع مختلفی داشته و آن‌قدر ظریف و باریک‌اند که بدون دیده شدن روی شکاف‌های ورودی کارت عابر بانک قرار می‌گیرند و به‌راحتی اطلاعات روی نوار مغناطیسی کارت بانکی را خوانده و در حافظهٔ خود ذخیره می‌کنند.

۱-۲-۵. کلاه‌برداری با کارت تبریک

در این نوع کلاه‌برداری در اعیاد و مناسبت‌های مختلف، کارت‌های تبریکی از طریق ایمیل برای افراد ارسال و معمولاً از آن‌ها خواسته می‌شود تا روی آن کلیک کرده و باز کنند. در بسیاری از موارد پس از کلیک کردن، نرم‌افزار مخربی روی سیستم کاربر نصب و اطلاعات دستگاه و گاه داده‌های موجود در آن، به‌صورت خودکار و بدون اعلام کاربر برای کلاه‌بردار ارسال می‌شود.

۱-۲-۶. کلاه‌برداری آنلاین اقتصادی

در این روش که یکی از انواع کلاه‌برداری اینترنتی است، مجرمان طعمه خود را قانع می‌کنند که با انجام پیشنهادهای آن‌ها به‌راحتی صاحب منبع کسب درآمد می‌شوند. با این کار طعمه ممکن است به بهانه آموزش کار در منزل و ایده‌های رؤیایی، فریب‌خورده و وجوهی را برای آن‌ها منتقل سازد. کلاه‌برداری اینترنتی از طریق بیت‌کوین، بی‌شک یکی از ابداعات محبوب چند سال اخیر ارز دیجیتال به‌ویژه بیت‌کوین می‌باشد که علاقه‌مندان بسیاری را برای خرید‌وفروش به سمت خود جذب نموده است. متأسفانه سود جویان اینترنتی از این علاقه سوءاستفاده نموده و اعمالی مثل استخراج غیرقانونی بیت‌کوین از طریق رایانه شخصی کاربران، ارسال دعوت‌نامه‌های جعلی برای سرمایه‌گذاری، مبادلات ارزی جعلی، تزریق بدافزارها از طریق سرویس‌های مبتنی به بیت‌کوین و... انجام می‌دهند.

۱-۲-۷. کلاه‌برداری از طریق سایت‌های شرط‌بندی

شرط‌بندی که در سال‌های دور در قهوه‌خانه‌ها انجام می‌شد، امروز به سایت های اینترنتی راه‌یافته و کلاه‌برداران سالانه میلیاردها تومان از این طریق به جیب می‌زنند. در این روش به‌دلیل اینکه از هر فرد بین ده تا صد هزار توان کلاه‌برداری می‌شود افراد به خاطر مبلغ پایین و ترس از جرم شرط‌بندی از شکایت صرف‌نظر می‌کنند.

۲. شیوه‌های پیشگیری از کلاه‌برداری با رویکرد انتظامی اجتماعی

از دهه‌های گذشته حرکت‌های رو به افزایش بسیاری در راستای تبدیل پیشگیری از جرم به‌عنوان یکی از شیوه‌های اصلی سیاست جنایی به‌وجود آمده و گونه‌های مختلف آن به‌عنوان یکی از اصلی‌ترین شیوه‌های پیشگیری و پاسخ به پدیدهٔ مجرمانه مورد توجه صاحب‌نظران عدالت کیفری و سیاست جنایی قرار گرفته است (علیوردی‌نیا، ۱۳۹۳، ۳۹). از سویی این شیوه‌ها نمی‌توانند ایستا باشند و پیشرفت جوامع ملازمه با پویایی شیوه‌های پیشگیرانهٔ جنایی دارد؛ نهادهای دخیل در پاسخ به پدیدهٔ مجرمانه به‌عنوان محرک‌های اصلی حفظ نظم و امنیّت جامعه، مدام با ایجاد تغییر در روش‌های فعالیتی و مدیریتی خود، هماهنگ با این تغییرات گام برداشته و در رساندن جامعه به توسعه‌یافتگی اجتماعی نقش ایفا نمایند (صالحی و رضایی، ۱۳۹۹، ۶۶).

یافته‌های این پژوهش نشان می‌دهد که در بحث جرم‌یابی کلاه‌برداری اینترنتی می‌توان در سطوح مختلف شیوه‌های گوناگونی را در نظر گرفت که در ادامه به آن‌ها اشاره می‌شود.

۲-۱. افزایش آگاهی جمعی و ارائهٔ آموزش به عموم

فقدان اقدامات متقابل سخت‌گیرانه و جو فرهنگی ـ اجتماعی دلیل اصلی افزایش جرائم سایبری است (کاوالیر[1]، ۲۰۲۱، ۴۲) قربانیان کلاه‌برداری اینترنتی عمدتاً اشخاص حقیقی جامعه هستند و بعضاً شاهد کلاه‌برداری از اشخاص حقوقی نیز هستیم. آگاهی اشخاصی که مستعد مورد هدف قرار گرفتن توسط کلاه‌برداران هستند می‌تواند تا حد زیادی زمینهٔ بروز این جرم را کاهش دهد. مهم‌ترین دلیل قربانی شدن این افراد را می‌توان در عدم آگاهی آن‌ها نسبت به شیوهٔ استفاده از فضای مجازی خلاصه کرد. از طرف دیگر بزهکارانی که اقدام به کلاه‌برداری می‌کنند نیز عمدتاً از اقشار ضعیف جامعه هستند که ارائه آموزش لازم و تثبیت اخلاق‌مداری در میان آن‌ها از دوران مدرسه می‌تواند نقش عمده‌ای در کاهش نرخ بزهکاری داشته باشد. طیف

1- Cavaliere

وسیعی از مجرمان و بزه‌دیدگان جرائم اینترنتی را افراد کم سن و سال، خصوصاً نوجوانان تشکیل می‌دهند. در دسترس نبودن شغل برای جوانان تحصیل‌کرده مشکل بزرگی است که باید برطرف شود. این مسئله نشان می دهد که چگونه تعادل بین ابزارهای نهادینه شده و اهداف فرهنگی باعث کاهش جرم و انحراف در جامعه می‌شود (آیودل اویدجی و بادموس[1]، ۲۰۲۲، ۳۴) از همین رو، ازجمله تدابیر مؤثر در پیشگیری کلاه‌برداری اینترنتی، ارائه آموزش کافی و اطلاع‌رسانی به‌موقع است. آگاه ساختن افراد و ارائه آموزش‌های لازم در سنین کودکی و نوجوانی می‌تواند نقش شایان‌توجهی در مقابله با کلاه‌برداری اینترنتی داشته باشد (انصاری، ۱۳۹۸، ۱۴۲)؛ لذا به همین ترتیب نسبت به کشف جرم و شناسایی مجرمان نخستین راهکار، ارائه آموزش به اشخاص عادی در خصوص شیوه‌های کلاه‌برداری مجرمان و اهمیت گزارش‌دهی اشخاص به مراجع انتظامی و قضایی است؛ هرچند خود شخص بزه‌دیده نباشند.

۲-۲. اتخاذ رویکرد تقنینی مانع

در خصوص انواع کلاه‌برداری آنچه امروزه شایع شده این است که حجم کلاه‌برداری‌های اینترنتی بسیار بیشتر از کلاه‌برداری‌های سنتی است؛ اما مجازاتی که قانون‌گذار در مادۀ ۱ قانون تشدید مجازات مرتکبین اختلاس، ارتشاء و کلاه‌برداری برای کلاه‌برداری سنتی در نظر گرفته است سنگین‌تر از مجازات مذکور در مادۀ ۱۳ قانون جرائم رایانه‌ای برای کلاه‌برداری اینترنتی است که این امر نمی‌تواند مانعیت لازم را برای بازداری بزهکاران داشته باشد و به همین سبب رویکرد قانون‌گذار نیاز به بازنگری اساسی دارد تا مجازات کلاه‌برداری اینترنتی با توجه به گستردگی آن در سال‌های اخیر متناسب با حجم جرائمی باشد که ممکن است اتفاق بیفتد.

موفقیت تحقیق در مورد هر جرمی تا حد زیادی با توانایی نفوذ نه‌تنها در قانون کیفری، بلکه ماهیت جنایی آن نیز تعیین می‌شود (استولوف[2]، ۲۰۱۸، ۱۸) از سویی شیوه‌های متعددی که کلاه‌برداران برای بردن وجوه نقد اشخاص

1- Ayodele & Badmos
2- Stulov

اتخاذ می‌کنند بسیار متنوع است و شاهد انجام کلاه‌برداری در حوزه‌های بازار واقعی اقتصاد و بازارهای مالی ازجمله بازار پول، سرمایه، بیمه و... هستیم که هر یک از این حوزه‌ها مقررات خاص خود را می‌طلبد؛ لذا وضع مقرره در هر حوزه نیاز به در نظر گرفتن ترتیبات جامع برای کشف جرم و شناسایی مجرمان دارد. قانون‌گذار ایران، تعریف کلاه‌برداری اینترنتی را از شکل سنتی گرفته است، درصورتی‌که در دیگر کشورها به دلیل وجود تفاوت بین کلاه‌برداری اینترنتی با نوع سنتی آن و همچنین کیفیات مجزا و متفاوت در شکل‌گیری این دو جرم، کلاه‌برداری اینترنتی را جرمی با تعریف و ماهیت جداگانه از کلاه‌برداری می‌دانند (بای، ۱۳۹۰، ۳۰۴).

۲-۳. ارائه آموزش تعاملی به مراجع انتظامی و قضایی

در چند سال گذشته عزم جزم قوّهٔ قضائیه در مقابله و مجازات مجرمین در فضای سایبر به‌وضوح نشان داده شده است اما نیاز امروز دادسرای جرائم رایانه ای تربیت قضات متخصص در امور رایانه‌ای می‌باشد؛ چراکه ضعف سیستم قضا در مباحث مذکور منجر به جمع‌آوری و ارائه ادلّه ضعیف به دادگاه و تضییع حقوق مجرمین و متهمین خواهد شد (نظری منظم، ۱۳۹۸، ۲۴۴). رویکرد پلیسی اطلاعات محور موجب فعال شدن مراکز تجزیه‌وتحلیل اخبار و اطلاعات و تعیین راهکارها و شیوه‌های عملیاتی و تاکتیکی حول محور جرم، عوامل جرم زا و مجرمان و تعیین نیازهای تخصصی‌شده و هزینهٔ جرم و کنترل مجرمین را کاهش داده و افزایش کیفیّت و اثربخشی اقدامات پلیس همچنین رضایت مردم در اثر افزایش احساس امنیّت و سرعت جرم‌یابی جرائم را به دنبال خواهد داشت (رسولی، ۱۴۰۰، ۱۱۸).

۲-۴. استفاده از قابلیت‌های هوش مصنوعی

امروزه پیشرفت‌های تکنولوژی کار را به جایی رسانده است که ماشین می تواند بدون هدایت انسان دستورهایی که به او داده شده است را انجام دهد و از اقداماتی که به‌تنهایی انجام می‌دهد نیز کسب تجربه کند و در اقدامات آتی

خـود اعمـال کنـد؛ ایـن مفهـوم بـا عنـوان یـادگیری ماشـین در حـوزه‌هـای مختلـف ازجمله، پزشکی، مهندسی، مدیریت و... به کار می‌رود.

کلاهبـرداری نیـز بـا توجـه بـه اینکـه بخـش عمـده‌ای از آن در فضـای سـایبر انجام می‌شـود و بـه‌راحتـی در دسـترس هـوش مصـنوعی قـرار مـی‌گیـرد، مـی‌توانـد مورد کشـف و شناسـایی قـرار گیـرد و بـه همـین جهـت اسـتفاده از قابلیـت‌هـای آن مـی‌توانـد گـامی مـؤثر در جهـت کشـف کـلاه‌بـرداری‌هـای اینترنتـی و همچنـین مجرمـانی کـه مرتکـب ایـن دسـت جـرائم مـی‌شـوند، باشـد. بـا در نظـر گـرفتن ایـن نکتـه کـه جـرائم کـلاه‌بـرداری اینترنتـی عمـدتاً توسـط گـروه‌هـا و بانـدهای بـزرگ صورت می‌گیرد و کمتر موردی مشاهده مـی‌شـود کـه تنهـا یـک شـخص پشـت ایـن دست اعمال مجرمانه باشد.

۲-۵. ایجاد سامانۀ جامع اطلاع‌رسانی

در جامعـه‌ای کـه اشـخاص عـادی قربـانی بزهکـاران مـالی مـی‌شـوند، بهتـرین شیوه برای آگاهی مراجـع انتظـامی و قضـایی اطـلاع‌رسـانی توسـط همـین اشخاصـی است کـه از آن‌هـا کـلاه‌بـرداری انجـام مـی‌شـود، هرچنـد رقمـی کـه از یـک شـخص برده می‌شود کوچک باشد؛ چراکه کـلاه‌بـرداران عمـدتاً اقـدام بـه کـلاه‌بـرداری مبـالغ کوچـک از تعـداد زیـادی از اشـخاص مـی‌کننـد. بـه همـین جهـت در نظـر گـرفتن سامانه‌ای بـرای اشـخاص عـادی کـه چنانچـه از وقـوع جرمـی اطـلاع یافتـه‌انـد آن را به آگاهی مراجع انتظامی و قضـایی برسـانند، مـی‌توانـد بسـیار کارآمـد باشـد و انجـام این امر نیاز به آگاهی‌بخشـیدن بـه عمـوم مـردم از وجـود چنـین سـامانه‌ای اسـت تـا چه اشخاصـی کـه خـود مـورد بزهکـاری قـرار گرفتنـد و چـه اشخاصـی کـه از وقـوع بزهکاری علیه دیگران اطلاع می‌یابند اقدام به اطلاع‌رسانی کنند.

در حال حاضر سامانه‌های سوت‌زنـی مختلفـی ایجـاد شـده اسـت تـا عمـوم مـردم وقوع خلاف و بـزه را بـه اطـلاع مراجـع برسـانند امـا عمومـاً ایـن سـامانه‌هـا شـناخته-شده نیستند و یا مردم نسبت بـه آن‌هـا اعتمـاد ندارنـد؛ ازایـن‌رو ایجـاد و بهـره‌گیـری ازاین‌دست سامانه‌ها نیاز به آمـوزش و آگـاهی بخشـی بـه مـردم دارد. همچنـین نیـاز به چنین سامانه‌ای در خصوص وقـوع کـلاه‌بـرداری نیـز وجـود دارد تـا مـردم بتواننـد

وقوع کلاه‌برداری‌های هرچند کوچک برای یک شخص را اطلاع‌رسانی کنند تا اقدامات لازم برای کشف مجرمان و باندهای کلاه‌برداری که با این شیوه‌ها مبالغ کلان به جیب می‌زنند، صورت گیرد.

روش

این پژوهش از نظر نوع، کاربردی و از نظر روش، توصیفی ـ تحلیلی است. جامعهٔ آماری تحقیق، تعداد ۸۵ نفر از فرماندهان و مدیران و استادان حوزهٔ جرم‌یابی پلیس بوده‌اند و حجم نمونه به تعداد ۷۰ است نفر که با استفاده از جدول مورگان تعیین شده‌اند. جهت گردآوری داده‌های کتابخانه‌ای از ابزار فیش‌برداری اعم از فیزیکی و اینترنتی و جهت گردآوری داده‌های میدانی از ابزار پرسش‌نامهٔ محقق‌ساخته که روایی محتوایی و صوری آن به‌وسیلهٔ خبرگان و صاحب‌نظران حوزهٔ جرائم کلاه‌برداری اینترنتی و پایایی آن با استفاده از آزمون ضریب آلفای کرونباخ (۰/۸۷) حاصل شده است. تجزیه‌وتحلیل داده‌ها، بعد از تعیین نرمال‌سنجی پراکندگی داده‌ها با استفاده از آزمون کولموگروف ـ اسمیرنوف برای هر دو مؤلفه فرصت‌ها و تهدیدهای سازمانی با استفاده از آزمون رتبه‌ای فریدمن و بهره‌گیری از نرم‌افزار spss انجام شده است.

یافته‌ها

دموگرافی یا اطلاعات جمعیت‌شناختی یعنی بررسی ویژگی‌های یک جمعیت مشخص در ابعاد متناسب با تحقیق که به‌عنوان مشارکت‌کننده در تحقیق حضور داشتند. ویژگی‌هایی مانند سابقهٔ کار، سنوات خدمت، تحصیلات، درجه و ... طبق جدول ۱ اطلاعات جمعیت‌شناختی مشارکت‌کنندگان و مصاحبه‌شوندگان به شرح ذیل ارائه شده است.

جدول ۱. یافته‌های توصیفی جمعیت‌شناختی

جایگاه شغلی	جایگاه	۱۵	۱۶	۱۷	۱۸	جمع
	فراوانی	۲۸	۲۴	۱۴	۴	۷۰
	درصد	۴۰	۳۴	۲۰	۶	٪۱۰۰
جنسیت	جنسیت	زن			مرد	جمع
	فراوانی	۲			۶۸	۷۰
	درصد	۲/۸۶			۹۷/۱۶	٪۱۰۰
مدرک تحصیلی	مدرک	کارشناسی	کارشناسی ارشد		دکتری	جمع
	فراوانی	۲۵	۳۵		۱۰	۷۰
	درصد	۳۶	۵۰		۱۴	٪۱۰۰
سابقهٔ خدمت	سابقه	۱۱ تا ۱۵ سال	۱۶ تا ۲۰	۲۱ تا ۲۵	بیش از ۲۵	جمع
	فراوانی	۱۰	۲۰	۳۰	۱۰	۷۰
	درصد	۱۴	۲۹	۴۳	۱۴	٪۱۰۰
سابقه مدیریت	سابقه	۲ تا ۵ سال	۶ تا ۱۰	۱۱ تا ۱۵	بیش از ۱۵	جمع
	فراوانی	۴	۲۱	۳۰	۱۵	۷۰
	درصد	۶	۳۰	۴۳	۲۱	٪۱۰۰

داده‌های جدول شماره ۱ بیانگر آن است که اعضای جامعهٔ آماری، دارای جایگاه پانزده به بالا تا سرتیپی بوده‌اند و اکثریت آن‌ها دارای مدرک تحصیلی بالاتر از کارشناسی بوده‌اند. بیشتر آن‌ها دارای مدرک دکتری بوده‌اند. ضمن آنکه سابقهٔ خدمت اکثریت آنان بین ۱۵ تا ۲۵ سال بوده است و جملگی دارای سابقهٔ خدمت و مدیریت درزمینهٔ جرم‌یابی بوده‌اند؛ و با توجه به آنکه در حوزهٔ جرم‌یابی بیشتر آقایان مشغول خدمت هستند، ترکیب جنسیتی جامعهٔ آماری تحقیق شامل ۶۸ نفر مرد و ۲ نفر زن است.

با توجه به اینکه یکی از مفروضات اصلی برای استفاده از آزمون پارامتری تی استودنت، نرمال بودن توزیع داده‌هاست، برای این منظور از آزمون کلموگروف ـ اسمیرنوف استفاده شده است که نتایج این آزمون در جدول ۲ نشان داده شده است.

$\{H_0$: توزیع احتمالی مشاهدات نرمال است H_1: توزیع احتمالی مشاهدات نرمال نیست

جدول ۲. نتایج آزمون نرمال بودن مشاهدات

مؤلفه	سطح معناداری	آماره کلموگروف	نتیجه
فرصت‌ها	۰/۰۹۴	۱/۳۴۸	نرمال
تهدیدها	۰/۰۷۸	۱/۴۹۰	نرمال

بر اساس سطوح معناداری به‌دست‌آمده از آزمون کلموگروف ـ اسمیرنوف مشاهده می‌شود که سطح معناداری برای تمامی مؤلفه‌ها بیشتر از خطای نوع اول ۰/۰۵ به دست آمده‌اند و درنتیجه فرضیهٔ نرمال‌بودن تمامی مشاهدات را در سطح خطای نوع اول ۰/۰۵ می‌پذیریم.

با توجه به نرمال‌بودن پراکندگی داده‌ها در ادامه از آزمون رتبه‌ای فریدمن برای بررسی شاخص‌های به‌دست‌آمده در مؤلفه‌های مورد مطالعه (فرصت‌ها و تهدیدها) در راستای پاسخ به سؤالات تحقیق استفاده شده است.

آزمون فریدمن امتیازات هر سطر فایل داده‌ها را مستقل از سایر سطرهای دیگر رتبه‌بندی می‌نماید و یک میانگین رتبه‌ای برای هر گویه به‌دست می‌دهد.

۱. جدول رتبه‌ای فریدمن برای شاخص‌های مؤلفه فرصت‌های سازمانی در حوزهٔ جرم‌یابی کلاه‌برداری:

رتبه‌بندی گویه های مربوط به سؤال اول تحقیق بر اساس میانگین رتبه‌ای فریدمن که نتیجه اولویت‌بندی نمودن گویه‌ها یا شاخص‌های مربوط به مؤلفه فرصت‌های سازمانی و شاخص‌های آن با موضوع اصلی تحقیق یعنی جرم‌یابی کلاه‌برداری است، به شرح ذیل است:

جدول ۳. میانگین رتبه‌ای و آزمون فریدمن (سؤال ۱)

شاخص‌ها	میانگین رتبه‌ای	اولویت گویه ها
وجود بانک‌های اطلاعاتی ملی ـ منطقه‌ای و بین‌المللی	۵/۶۳	۱
وجود ظرفیت‌های قانونی، حقوقی، اسناد فرصت‌ساز بالادستی	۵/۵۹	۲
وجود منابع و مخبرین در جهت کمک به جمع‌آوری اطلاعات در تسریع کاهش جرم کلاه‌برداری	۴/۵۱	۳
تعامل کارآمد با قوه قضائیه	۴/۴۹	۴
وجود کارشناسان خبره رسمی در حوزهٔ خط، امضاء و اثرانگشت در جهت بررسی علمی تخصصی اسناد و مدارک و ارائه سرنخ‌های لازم برای کشف	۴/۳۹	۵

شاخص‌ها	میانگین رتبه‌ای	اولویت گویه ها
جرم کلاه‌برداری		
وجود ظرفیت‌ها و قابلیت‌های رسانه‌ای کارآمد)شنیداری، دیداری و... به‌منظور بهره‌گیری در همراه سازی، مشارکت و اجرای مأموریت‌های مربوطه	۴/۳۸	۶
بهره‌گیری از ظرفیت سایر سازمان‌های مؤثر (شاک، مفاسد اقتصادی و...)	۳/۹۵	۷
بهره‌گیری از ظرفیت‌های مراکز علمی و دانشگاهی در جهت آسیب‌شناسی جرم کلاه‌برداری اینترنتی و ارائه راهکارهای علمی در پیشگیری و مبارزه با این جرم	۳/۸۲	۸

آزمون فرید من

N	۷۰
Chi – square	۴/۴۵۲
Df	۵
Asymp.sig.	۰/۰۴۴

داده‌های جدول شماره ۳ نشان می‌دهند که اولاً: میانگین‌های رتبه‌ای به‌دست‌آمده اغلب بالاتر از میانگین واقعی سؤالات یعنی (mean =3) می‌باشد که بیانگر آن است که پاسخ پاسخ‌دهندگان به سؤالات متوسط به بالا بوده است یا به‌عبارت‌دیگر آن‌ها را مثبت و مطلوب ارزیابی کرده‌اند؛ ثانیاً: با توجه به سطح معنی‌داری به‌دست‌آمده از آزمون (sig<0/05) بیانگر وجود رابطه حقیقی بین مؤلفه فرصت‌های سازمانی و شاخص‌های آن با موضوع اصلی تحقیق یعنی جرم‌یابی کلاه‌برداری است.

۲. جدول رتبه‌ای فریدمن برای شاخص‌های بعد تهدیدهای سازمانی در حوزهٔ جرم‌یابی کلاه‌برداری:

رتبه‌بندی گویه‌های مربوط به سؤال دوم تحقیق بر اساس میانگین رتبه‌ای فریدمن که نتیجه اولویت‌بندی نمودن گویه‌ها یا شاخص‌های مربوط به مؤلفه تهدیدهای سازمانی و شاخص‌های آن با موضوع اصلی تحقیق یعنی حوزهٔ جرم‌یابی کلاه‌برداری است، به شرح ذیل است:

جدول ۴. میانگین رتبه‌ای و آزمون فریدمن (سؤال ۲)

شاخص‌ها	میانگین رتبه‌ای	اولویت گویه‌ها
توسعهٔ روزافزون کلاه‌برداری در فضای حقیقی و مجازی	۴/۳۴	۱
وجود بسترهای اقتصادی، اجتماعی و فرهنگی و انگیزه‌های زیاد برای ارتکاب جرم کلاه‌برداری	۴/۲۸	۲
کمبود قضات باتجربه و دادسراهای تخصصی ویژه جرم‌یابی کلاه‌برداری	۴/۱۱	۳
وجود خلأهای قانونی در فرایند رسیدگی به جرم کلاه‌برداری	۳/۹۱	۴
نبود سیستم اطلاعات اقتصادی یکپارچه	۳/۸۳	۵
عدم وجود مقررات مدون نحوهٔ فعالیت برخی از مشاغل مانند ساخت و سازهای شرکت‌ها، طلافروشی‌ها و...	۳/۴۹	۶
پیچیدگی، تخصصی بودن و سازمان‌یافتگی جرم کلاه‌برداری اینترنتی که باعث پیچیدگی جرائم، کندی در تکمیل و مستدسازی و درنتیجه فرار مجرم از چنگال عدالت خواهد شد	۳/۳۲	۷
ضعف در همراهی و همکاری سازمان‌های اقتصادی در پیشگیری، کشف و پی‌جویی جرم کلاه‌برداری اینترنتی	۳/۲۶	۸
وجود مجرمین حرفه‌ای و سابقه‌دار که باعث پیچیدگی جرائم و افزایش پرونده‌های زنجیره‌ای و باندی می‌گردد	۳/۱۲	۹
نبود اجماع گفتمانی در سطح نخبگی، تصمیم‌گیری و سیاست‌گذاری در موضوعات کنترلی و مقابله با جرم کلاه‌برداری	۳/۰۵	۱۰

آزمون فرید من

N	۷۰
Chi – square	۱۴/۳۲۴
Df	۳
Asymp.sig.	۰/۰۰۲

داده‌های جدول شماره ۴ نشان می‌دهند که اولاً: میانگین‌های رتبه‌ای به‌دست‌آمده اغلب بالاتر از میانگین واقعی سؤالات یعنی (mean =3) می‌باشد که بیانگر آن است که پاسخ پاسخ‌دهندگان به سؤالات در حد متوسط بوده است یا به‌عبارت‌دیگر آن‌ها را در حد متوسط ارزیابی کرده‌اند. ثانیاً: با توجه به سطح معنی‌داری به‌دست‌آمده از آزمون (sig<0/05) بیانگر وجود رابطه حقیقی

بین مؤلفه تهدیدهای سازمانی و شاخص‌های آن با موضوع اصلی تحقیق یعنی جرم‌یابی کلاه‌برداری است.

بحث و نتیجه‌گیری

امروزه فضای مجازی و اینترنتی در تمامی ابعاد زندگی انسان سایه افکنده است؛ به‌طوری‌که روابط انسان‌ها در این بستر، روزانه رشد و نمو دارد. امنیّت که مهم‌ترین رکن پایداری یک جامعه است در این محیط شکل می‌گیرد و محیط شناسی و مبارزه با جرائم حوزهٔ کلاه‌برداری اینترنتی یکی از ارکان امنیّت محسوب می‌شود؛ لذا ازآنجاکه فضا مجازی از بسترهای علمی و فنی شکل یافته است؛ بنابراین، نیازمند اقدامات علمی و فنی در امنیّت سازی این فضا است؛ که تحقیق حاضر گامی کوتاه اما مهم، اثرگذار و لازم. در محیط‌شناسی راهبردی جرم‌یابی کلاه‌برداری اینترنتی خواهد بود. یافته‌های این پژوهش نشان می‌دهد که توجهات ویژه‌ای باید نسبت به شاخص‌های مورد مطالعه در تحقیق که در ذیل دو مؤلفه فرصت‌ها و تهدیدهای سازمانی مورد مطالعه قرار گرفته است داشته باشیم تا بتوانیم پیش‌بینی، پیش‌گیری و مقابله پیش‌دستانه نسبت به این جرم توسط پلیس در صحنه اجتماعی و در راستای تأمین امنیّت عمومی داشته باشیم؛ و درنتیجه شاهد کاهش نرخ وقوع کلاه‌برداری اینترنتی باشیم. مهم‌ترین و کم‌اهمیت‌ترین شاخص‌های به‌دست‌آمده در ذیل دو مؤلفه پیش‌گفته به شرح زیر می‌باشند:

مؤلفهٔ فرصت‌های سازمانی در حوزهٔ کلاه‌برداری اینترنتی: از بین شاخص‌های به‌دست‌آمده برای این مؤلفه، شاخص‌های وجود بانک‌های اطلاعاتی ملی ـ منطقه‌ای و بین‌المللی (این یافته همسو با یافته‌های تحقیقات رسولی، ۱۴۰۰؛ مرتضوی و هندیانی ۱۴۰۰ و یاوری، ۱۴۰۰ است)؛ وجود ظرفیت‌های قانونی، حقوقی، اسناد فرصت‌ساز بالادستی (این یافته همسو با یافته‌های تحقیق پراباکاران ،۲۰۱۸ می‌باشد.)؛ و وجود منابع و مخبرین در جهت کمک به جمع‌آوری اطلاعات در تسریع کاهش جرم کلاه‌برداری اینترنتی (این یافته همسو با یافته‌های تحقیق کریمی، ۱۴۰۰ است) به ترتیب در جایگاه اول تا

سوم قرار گرفته‌اند؛ و شاخص‌های وجود ظرفیت‌ها و قابلیت‌های رسانه‌ای کارآمد (شنیداری، دیداری و... به‌منظور بهره‌گیری در همراه‌سازی، مشارکت و اجرای مأموریت‌های مربوطه) (این یافته همسو با یافته‌های تحقیقات: کریمی، ۱۴۰۰؛ رسولی ۱۴۰۰ و نظری منظم ۱۳۹۹ است)؛ بهره‌گیری از ظرفیت سایر سازمان‌های مؤثر (شاک، مفاسد اقتصادی و...)؛ و بهره‌گیری از ظرفیت‌های مراکز علمی و دانشگاهی در جهت آسیب‌شناسی جرم کلاه‌برداری اینترنتی و ارائه راهکارهای علمی در پیشگیری و مبارزه با جرم کلاه‌برداری اینترنتی به‌ترتیب در سه جایگاه آخر قرار گرفته‌اند؛ که این مطلب نشان‌دهندهٔ اولویت نگاه جامعه آماری به ظرفیت تعاملی، قانونی و جمع‌آوری پنهان و... در حوزهٔ میدانی به‌عنوان فرصت‌های سازمانی در جهت مبارزه با جرم کلاه‌برداری اینترنتی است چراکه در گام اول نیاز به همکاری و تعامل اطلاعاتی است درصورتی‌که بسترهای حقوقی مناسب فراهم باشد و در غیر این صورت بهره‌گیری از جمع‌آوری پنهان می‌تواند یاری گر باشد و در مرحله دوم نیاز به اقدامات دیگر از قبیل استفاده از ظرفیت‌های رسانه‌ای و تبلیغی، بهره‌گیری از ظرفیت سایر سازمان‌ها و همچنین بهره‌گیری از ظرفیت‌های مراکز علمی و دانشگاهی در جهت آسیب‌شناسی جرم کلاه‌برداری اینترنتی و ارائه راهکارهای علمی در پیشگیری و مبارزه با جرائم کلاه‌برداری اینترنتی است.

مؤلفه تهدیدهای سازمانی در حوزهٔ کلاه‌برداری: از بین شاخص‌های به‌دست‌آمده برای این مؤلفه، شاخص‌های توسعهٔ روزافزون کلاه‌برداری اینترنتی در فضای حقیقی و مجازی (این یافته همسو با یافته‌های تحقیق پراباکاران ، ۲۰۱۸ است.)؛ وجود بسترهای اقتصادی، اجتماعی و فرهنگی و انگیزه‌های زیاد برای ارتکاب جرم کلاه‌برداری اینترنتی (این یافته همسو با یافته‌های تحقیق لاوت، ۲۰۱۵ است.)؛ کمبود قضات باتجربه و دادسراهای تخصصی ویژه جرائم کلاه‌برداری اینترنتی (این یافته همسو با یافته‌های تحقیق نظری منظم، ۱۳۹۹ و لاوت، ۲۰۱۵ است.)، به‌ترتیب در جایگاه اول تا سوم قرار گرفته‌اند؛ و شاخص‌های ضعف در همراهی و همکاری سازمان‌های اقتصادی در پیشگیری، کشف و پی‌جویی جرائم کلاه‌برداری اینترنتی (این یافته همسو با یافته‌های

تحقیق بوپینگ، ۲۰۰۴ می‌باشد.)؛ وجود مجرمین حرفه‌ای و سابقه‌دار که باعث پیچیدگی جرائم و افزایش پرونده‌های زنجیره‌ای و باندی می‌گردد (این یافته همسو با یافته‌های تحقیق یوپینگ، ۲۰۰۴ می‌باشد.)؛ و نبود اجماع گفتمانی در سطح نخبگی، جهت تصمیم‌گیری و سیاست‌گذاری در موضوعات کنترلی و مقابله با جرائم کلاه‌برداری اینترنتی (این یافته همسو با یافته‌های تحقیقات کریمی، ۱۴۰۰؛ رسولی، ۱۴۰۰؛ نظری منظم، ۱۳۹۹ و یاوری، ۱۴۰۰ است.)، به‌ترتیب در سه جایگاه آخر قرار گرفته‌اند؛ که این مطلب در گام اول نشان‌دهندهٔ اولویت نگاه جامعه آماری به بسترهای جدید جرم مانند فضای مجازی و متنوع شدن حوزه‌های وقوع جرم در جامعه و همچنین آسیب‌های درون‌سازمانی مانند کمبود نیروی انسان کیفی یا وجود خلأهای قانونی و ... در حوزهٔ مبارزه با جرائم کلاه‌برداری اینترنتی است و در گام دوم به تهدیداتی از قبیل ضعف در همکاری سازمانی جهت پیشگیری و مبارزه با جرائم کلاه‌برداری اینترنتی، وجود مجرمین حرفه‌ای و سابقه‌دار در جامعه و همچنین نبود اجماع در سطح نخبگی جهت اتخاذ تصمیم و سیاست‌گذاری مؤثر در خصوص کنترل و مقابله با جرائم کلاه‌برداری اینترنتی است.

پیشنهادها

با توجه به یافته‌های تحقیق و نظر به نگاه جامعهٔ آماری تحقیق به اقدامات زودبازده، میدانی و عملیاتی، پیشنهادهای تحقیق به شرح ذیل است:

۱. بستر و ابزارهای فنی لازم جهت بالا بردن قابلیت کشف علمی و اطلاعاتی کلاه‌برداری اینترنتی توسط پلیس در فضای مجازی تقویت شود.

۲. بانک‌های اطلاعات جمعیتی و ارتباطی (مانند بانک مجرمان حرفه‌ای، سابقه‌دار و گروه مجرمانه و...) جهت پیشگیری از وقوع جرم کلاه‌برداری اینترنتی و در صورت وقوع بالا بردن سرعت پلیس در کشف و مقابله با آن تشکیل گردد.

۳. کمبود تجهیزات فنی، تخصصی و آزمایشگاهی نوین و روزآمد در حوزهٔ جرم‌یابی کلاه‌برداری اینترنتی و مجازی پلیس برطرف شود.

۴. جذب، تربیت و آموزش نیروی انسانی متخصص در پلیس متناسب با ساختار سازمانی و رشد و توسعهٔ جرم کلاه‌برداری اینترنتی در سطح جامعه مجازی کشور و همچنین قضات متخصص در حوزهٔ جرائم کلاه‌برداری اینترنتی و مجازی صورت گیرد.

۵. اقدامات لازم جهت توسعهٔ تعامل بین پلیس و سازمان قضایی و دیگر سازمان‌های ذینقش در راستای پیش‌بینی، پیش‌گیری و مقابله با جرم کلاه‌برداری اینترنتی در فضای مجازی انجام گیرد.

۶. جهت به‌روزرسانی و متناسب‌سازی ظرفیت‌های قانونی، حقوقی و دیگر اسناد فرصت ساز بالادستی در راستای پیش‌بینی، پیش‌گیری و مقابله با جرم کلاه‌برداری اینترنتی در فضای مجازی تلاش شود.

۷. با توجه به پیچیدگی و چندلایه بودن فضای مجازی، تلاش جهت ایجاد و ارتقاء منابع و مخبرین در جهت کمک به جمع‌آوری اطلاعات و تسریع در کاهش جرم کلاه‌برداری اینترنتی در فضای مجازی تقویت شود.

۸. اطلاع‌رسانی و آموزش همگانی در سطح جامعه با توجه به توسعهٔ روزافزون کلاه‌برداری اینترنتی در فضای مجازی گسترش داده شود.

سپاسگزاری

نویسندگان در این مجال بر خود فرض می‌دانند از زحمات بی‌دریغ تمام عزیزانی که در به ثمر رسیدن این پژوهش نقش اساسی ایفا کردند و همچنین از مسئولان محترم فصلنامهٔ انتظام اجتماعی کمال تقدیر و تشکر را داشته باشند.

منابع

- انصاری، جلال؛ عطارزاده، سعید و قیومزاده، محمود. (۱۳۹۸). سیاست جنایی ایران و آمریکا در قبال جرائم کلاه‌برداری و سرقت سایبری. فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، ۳ (۱۴)، ۱۳۱- ۱۵۴. قابل بازیابی از: icr.jrl.police.ir/article_92447.html
- بارانی، محمد؛ قنبری، علی و حسن‌زاده، عبدالله. (۱۳۹۸). نقش اقدامات پلیس در پیشگیری از جرایم کلاهبرداری در محیط کسب و کار (مورد مطالعه: استان مازندران). فصلنامهٔ پژوهش‌های دانش انتظامی، ۳(۲۱)، ۱۴۵-۱۷۵. قابل بازیابی از: http://pok.jrl.police.ir/article_93107.html
- بای، حسین‌علی و پورقهرمانی، بابک. (۱۳۸۸). بررسی فقهی حقوقی جرائم رایانه‌ای. قم: انتشارات پژوهشگاه علوم و فرهنگ اسلامی.
- حسینی، سید نواب. (۱۳۹۹). نقش فناوری‌های علمی و پلیسی در کشف جرم. پایان‌نامهٔ کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد دماوند.
- دباغ، افروز؛ بافنده زنده، علیرضا و پاسبانی، محمد. (۱۴۰۰). طراحی الگوی راهبردی زیست بوم نوآوری در حوزهٔ سلامت با استفاده از نظریهٔ داده‌بنیاد. نشریه تصویر سلامت، ۲(۱۲). ۱۱۳-۱۲۶. قابل بازیابی از: https://sid.ir/paper/372540/fa
- رسولی، مهدی؛ یاوری، امیرحسین و عبدالهی، علیرضا. (۱۴۰۰). نقش پلیس اطلاعات محور در جرم‌یابی کلاه‌برداری تلفنی به شیوه کارت به کارت. فصلنامهٔ پژوهش‌های دانش انتظامی، ۳ (۲۳). ۹۳-۱۱۵. قابل بازیابی از: http://www.pok.jrl.police.ir/article_96335.html.
- سیلورستون، هاوارد و شیتز، دیوایا. (۱۳۹۱).کلاه‌برداری و تقلب؛ روش‌ها و شیوه‌های پیشگیری. ترجمهٔ سید حسین موسویون. تهران: انتشارات کارآگاه.

- صالحی، محمدخلیل و رضائی، احمد. (۱۳۹۹). مقایسه الگوی راهبردی برنامه‌ریزی پیشگیری از جرم با الگوهای جزئ نگر. فصلنامهٔ علمی مطالعات بین‌رشته‌ای دانش راهبردی، ۱۰(۳۸). ۳۹-۷۰. قابل بازیابی از: https://smsnds.sndu.ac.ir/article_991.html
- طالبیان، حسین. (۱۴۰۰). پی‌جویی کلاه‌برداری. چاپ یکم. تهران: انتشارات دانشگاه علوم انتظامی امین.
- طالبیان، حسین و کریمی، مجید. (۱۳۹۹). بررسی الگوهای جرم‌یابی. فصلنامهٔ علمی کارآگاه. ۱۴(۵۲). ۶۷-۸۱. قابل بازیابی از: https://doi.org/10.22034/det.2020.95426
- علیوردی‌نیا، اکبر. (۱۳۹۳). مدیریت پیشگیری از جرم در ایران. فصلنامهٔ سیاست‌های راهبردی و کلان.۲(۸). ۳۷-۵۸. قابل بازیابی از: https://www.jmsp.ir/article_7769.html
- غروی، محمد. (۱۳۹۵). پیشگیری عادلانه از جرم در علوم جنایی. چاپ اول، تهران: انتشارات سمت.
- کریمی، مجید. (۱۴۰۰). راهبردهای جرم‌یابی جرائم سازمان‌یافته مواد مخدر. رساله دکتری جهت اخذ دکتری تخصصی جرم‌یابی دانشگاه علوم انتظامی امین.
- گلدوزیان، ایرج. (۱۳۸۸). بایسته‌های حقوق جزای عمومی. چاپ هجدهم. تهران: نشر بنیاد حقوقی میزان.
- مرتضوی، سید مرتضی؛ فضلی، صفر؛ هندیانی، عبدالله؛ توکلی، فخرالدین و کشاورز ترک، محسن. (۱۴۰۰). شناسایی عوامل راهبردی موثر بر جرم‌یابی با رویکرد آینده‌پژوهی. فصلنامهٔ علمی کارآگاه. ۱۵(۵۷). ۱-۲۳. قابل بازیابی از: https://www.sid.ir/paper/966768/fa
- مؤذن‌زادگان، حسن‌علی و حمیدزاده اربابی، نجف. (۱۳۹۲). کاربرد انگشت-نگاری در جرم‌یابی. فصلنامهٔ علمی کارآگاه. ۷(۲۴). ۹۸-۱۱۵. قابل بازیابی از: http://det.jrl.police.ir/article_10444.html

- نظری منظم، مهدی. (۱۳۹۹). ارائه الگوی جرم‌یابی کلاهبرداری در فضای سایبری. رساله دکتری جهت اخذ دکتری تخصصی جرم‌یابی دانشگاه علوم انتظامی امین.

- نظری‌منظم، مهدی؛ مجیدی، عبدالله، هندیانی، عبدالله و وفادار، حسین. (۱۳۹۸). بررسی عوامل مؤثر بر جرم‌یابی کلاه‌برداری در فضای سایبر. نشریه پژوهش‌های دانش انتظامی. ۲(۸۳). ۲۱۷-۲۴۵. قابل بازیابی از:
http://pok.jrl.police.ir/article_92091.html

- Ayodele, O &. Badmos, H. (2022). Social Construction of Internet Fraud as Innovation among Youths in Nigeria. International Journal of Cybersecurity Intelligence and Cybercrime. 5(1), 23-42, Retrievable from:
https://vc.bridgew.edu/ijcic/vol5/iss1/3/

- Cavaliere, L. (2021). The Impact of Internet Fraud on Financial Performance of Banks. Turkish Online Journal of Qualitative Inquiry (TOJQI). 6(12), 8126-8158, Retrievable from:
https://www.tojqi.net/index.php/journal/article/view/3260

- kumar , A & et al. (2013). An Investigation of Banking Cyber Frauds with Indian Private and Public Sector Banks. International Journal of 360o Management. 2(1), 1-11, Retrievable from:
https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=210ab5598d48dd10e7385a747ccab4dfc748d71f

- la ott, K & Antonius, M. (2014). Indonesia's Criminal Sanction Toward Crime Of Credit / Debit Card Fraud. South East Asia Journal of Contemporary Business, Economics and Law. 4 (5), 34-39, Retrievable from:
http://seajbel.com/wp-content/uploads/2014/12/LAW-55-Indonesias-Criminal-Sanction-Toward-Crime-Of-Credit-Debit-Card-Fraud.pdf

- McDowell, D. (2008). Strategic intelligence: a handbook for practitioners, managers, and users. 34, The Scarecrow Press. Retrievable from:
https://sciebook.ir/downloads/strategic-intelligence-a-handbook-for-practit-3376

- Okeshola, B & Adeta, A. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-

Kaduna State, Nigeria. American International Journal of Contemporary Research. 3(9),98-114, Retrievable from: http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf

- Osrat, A. T. M. (2020). Causes of Cybercrime Victimization: A Systematic. Literature Review, International Journal of Research and Review. 5(7). 89-98, Retrievable from: https://www.ijrrjournal.com/IJRR_Vol.7_Issue.5_May2020/IJRR0015.pdf

- Prabakaran, M. (2018). Survey of Analysis of Crime Detection Techniques Using Data Mining and Machine Learning. National Conference on Mathematical Techniques and its Applications (NCMTA 18), Journal of Physics: Conference Series. 1-10, Retrievable from: https://iopscience.iop.org/article/10.1088/1742-6596/1000/1/012046/pdf

- Quiggin, T. (2007). Seeing the Invisible: National Security Intelligence in an Uncertain Age. World Scientific, Retrievable from: https://intlib.ir/download/seeing-the-invisible:-national-security-intelligen-21503/

- Simon,Y & et al. (2013). Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique. (IJACSA) International Journal of Advanced Computer Science and Applications. 4(3), 156-164, Retrievable from: https://thesai.org/Publications/ViewPaper?Volume=4&Issue=3&Code=IJACSA&SerialNo=25

- Stulov, I. (2018). Investigation of Internet Frud in the Prosecution Process. Masters thesis in Tallinn University of Technology, School of Business and Governance, Department of Law ,18. Retrievable from: https://digikogu.taltech.ee/et/Download/b7c7d287-999c-4b8c-81ef-5623b6d99eb1

- Yuping, H & et al. (2004). Survey of fraud detection techniques. IEEE International Conference on Networking, Sensing and Control.Vol. 2, 749-754, Retrievable from: https://ieeexplore.ieee.org/document/1297040