Fraud criminalization model in cyber space

Mahdi Nazari[1]
Reza Sobhkhiz[2]

Type of article: research article
Received:17/01/2022 Accepted: 30/07/2022
NAJA Strategic Studies Quarterly/Vol.8/NO.1(serial27)/Spring 2023*103-126
DOR: 20.1001.1.25381946./ssj.2022.99833

Abstract
The crime of cyber fraud is one of the most important crimes against people's property and property that takes place in the cyber space. Despite its many advantages, this space has caused many crimes to migrate to it due to features such as the possibility of learning different identities, anonymity and, as a result, the ease of committing crimes. The main purpose of this article is to explain effective methods in detecting cyber fraud and how to detect it. This research is applied in terms of type and purpose and mixed in terms of method. The statistical population in the qualitative section includes 100 experts in cyberspace, judges and related judicial authorities, and expert professors in this field, and in the quantitative section, it includes 253 experts related to the subject in both theoretical and experimental fields. The data collection tool in the qualitative part is a semi-structured interview and in the quantitative part, a researcher-made questionnaire. The validity of the interview and questionnaire is content validity, and the reliability of the questionnaire is by spss software, 87/. Was calculated. According to the results of the research, individual dimensions with a factor load of 823/. In the first place, social with a coefficient of 809/. In the second place and an infrastructure with a factor load of 711/. It is in the third place. In examining the methods used, "Using IP trap to obtain personal information" with a factor load of 863/. It is in the first place. In the study of the current methods and methods of criminals, "phishing and pharming of the login page of financial exchange sites to steal information" with a factor load of 842/. It is in the first place and in the examination of the challenges, "criminals use several complex methods to hide their identity at the same time" with a factor load of 869/. They are in the first place.
Keywords: phishing, fraud, cyber space, challenges, crime.

1. Assistant Professor of Shooting Department, Faculty of Basic Sciences, Amin University of Management Sciences, Tehran, Iran (corresponding author), m. nazari2013@yahoo. com
2. Assistant Professor of FATA Scientific Department, Faculty of Information and Knowledge Sciences and Technologies, Amin University of Sciences, Tehran, Iran, reza123onlymorning@gmail. com

الگوی جرم‌یابی کلاهبرداری در فضای سایبر

مهدی نظری[۱]
رضا صبح‌خیز[۲]

نوع مقاله: مقاله پژوهشی
تاریخ دریافت: ۱۴۰۰/۱۰/۲۷ تاریخ پذیرش: ۱۴۰۱/۰۵/۰۸
فصلنامه مطالعات راهبردی ناجا/سال هشتم/ شماره ۱ (پیاپی ۲۷)-بهار ۱۴۰۲*۱۰۳-۱۲۶
DOR: 20.1001.1.25381946./SSJ.2022.99833

چکیده

جرم کلاهبرداری سایبری یکی از مهم‌ترین جرایم برضدّ اموال و مالکیت مردم می‌باشد که در فضای سایبری صورت می‌گیرد. این فضا با وجود مزایای فراوانش، به‌دلیل ویژگی‌هایی مانند امکان تحصیل هویت‌های گوناگون، گمنامی و درنتیجه، سهولت انجام جرایم، موجب مهاجرت بسیاری از جرایم به آن شده‌است. هدف اصلی این مقاله، تبیین شیوه‌های موثر در کشف جرم کلاهبرداری سایبری و نحوه جرم‌یابی آن است. این تحقیق از نظر نوع و هدف، کاربردی و از نظر روش، آمیخته است. جامعه آماری در بخش کیفی شامل خبرگان فضای سایبر، قضات و مراجع قضایی مرتبط و اساتید صاحب‌نظر در این حوزه به تعداد ۱۰۰ نفر و در بخش کمی شامل ۲۵۳ نفر از خبرگان مرتبط با موضوع در هر دو حوزه نظری و تجربی هستند. ابزار گردآوری داده‌ها در بخش کیفی، مصاحبه نیمه‌ساختاریافته و در بخش کمی، پرسش‌نامه محقق‌ساخته است. روایی مصاحبه و پرسش‌نامه از نوع روایی محتوایی است و پایایی پرسش‌نامه توسط نرم‌افزار spss، ۸۷/. محاسبه گردید. طبق نتایج تحقیق، ابعاد فردی با بار عاملی ۸۲۳/. در رتبه اول، اجتماعی با ضریب ۸۰۹/. در رتبه دوم و زیرساختی با بار عاملی ۷۱۱/. در رتبه سوم قرار دارد. در بررسی روش‌های مورد استفاده، "استفاده از تله IP برای به‌دست‌آوردن اطلاعات فرد" با بار عاملی ۸۶۳/. در رتبه اول قرار دارد. در بررسی شگردها و شیوه‌های کنونی مجرمین، "فیشنگ و فارمینگ صفحه ورود به سایت‌های تبادلات مالی جهت سرقت اطلاعات" با بار عاملی ۸۴۲/. در رتبه اول است و در بررسی چالش‌ها نیز "استفاده مجرمان از چندین روش پیچیده جهت اختفای هویت به‌صورت هم‌زمان" با بار عاملی ۸۶۹/. در رتبه اول قرار دارند.

واژگان کلیدی: فیشینگ، کلاهبرداری، فضای سایبر، چالش‌ها، جرم.

---

۱. استادیار گروه تیراندازی، دانشکده علوم پایه، دانشگاه علوم انتظامی امین، تهران، ایران(نویسنده مسئول)، m.nazari2013@yahoo.com
۲. استادیار گروه علمی فتا، دانشکده علوم و فنون اطلاعات و آگاهی، دانشگاه علوم انتظامی امین، تهران، ایران، reza123onlymorning@gmail. com

مقدمه

به‌عقیده بسیاری از صاحب‌نظران، جهان در آستانه یک انقلاب اجتماعی نوین قرار دارد و فناوری اطلاعات، دستاورد تلاش‌های علمی بشر و تجلی آرمان‌های ذهنی انسان است. در دهه گذشته، با گسترش فناوری اطلاعات، فضای مجازی به‌طورچشمگیری گسترش یافته است(پورنقدی، ۱۳۹۳: ۹). این فضا ـ که دریچه نوینی در ارتباطات بشری محسوب می‌شود ـ تعاملات منحصر به خود را دارا بوده و متناسب با ویژگی‌ها، دارای مزایا و معایب خاص خود است. یکی از نگرانی‌های نوخاسته و فزاینده معاصر این است که جریان‌های جهانی پول، اطلاعات و افراد و به‌ویژه فراهم‌آمدن بستر جدیدی به نام فضای مجازی و نیز ابزارهای لازم برای بهره‌گیری از این فضا شرایط و فرصت‌های مناسبی را برای گسترش شکل جدیدی از بزه‌کاری فراهم نموده‌است؛ ازاین‌رو، اهمیت سیاست‌ها، برنامه‌ها و تدابیر مبارزه با جرایم سایبری، با توجه به اقدامات متنوع نظام عدالت کیفری در مبارزه با جرم، امری غیرقابل‌انکار است.

امروزه، موضوع جرم‌یابی و مبارزه با جرایم در حوزه سایبری، به یکی از موضوعات مهم دولت‌ها تبدیل شده‌است؛ چراکه با توجه به امر جهانی‌شدن، شاید بتوان ادعا کرد که بارزترین جرم بین‌المللی، جرم سایبری است؛ بر این اساس، میزان کارآمدی دولت‌ها در این زمینه، یکی از ملاک‌های بسیار مهم موفقیت آنها در "حکمرانی خوب" تلقی می‌شود(مقیمی، ۱۳۹۵: ۱۲). تحول اشکال بزه‌کاری و افزایش رفتارهای مجرمانه در فضای سایبر، به‌ویژه کلاهبرداری سایبری، ضرورت مقابله و رویارویی با این پدیده مجرمانه را در سطوح ملی و فراملی، بیش از پیش مطرح ساخته است. درحقیقت، باید گفت که این جرم از لحاظ موازین جرم‌شناختی، سریع‌ترین، گسترده‌ترین، شایع‌ترین و آسان‌ترین جرمی است که می‌تواند در فضای ملی و بین‌المللی به وقوع بپیوندد و ازاین‌رو، به نظر می‌رسد که از جمله مهم‌ترین دغدغه‌های جهان در عصر حاضر از نظر حقوقی، جرم‌شناسی و امنیتی، بحث جرم سایبری است.

یکی از جرایم شایع در فضای مجازی، انواع کلاهبرداری‌های مالی است که قربانیان فراوانی را طعمه خود می‌نماید و جهان روزانه شاهد افزایش شیوه‌ها و

شگردهای ارتکاب این جرم در فضای سایبر است. این جرم فقط برضدّ اشخاص حقیقی ارتکاب نمی‌یابد بلکه اغلب برضدّ سیستم‌های رایانه‌ای و نرم‌افزارهای آن است و بنابراین، شرط فریب قربانی در آن، تا مرز حذف‌شدن تضعیف می‌شود. موضوع جرم کلاهبرداری سایبری نیز فراتر از مال یا وسیله تحصیل مال است و شامل خدمات و امتیازات مالی و حتی داده‌های رایانه‌ای دارای ارزش مالی نیز می‌باشد. کلاهبرداری سایبری جرمی است که در آن، رایانه دارای نقشی اساسی است و به همین دلیل، نیازمند جرم‌انگاری خاص می‌باشد. این درحالی است که با وجود جرم‌انگاری در این خصوص، هنوز کاستی‌ها و ابهاماتی در زمینه جرم انگاری و همچنین فراتر از آن، در زمینه کاهش و پیشگیری از جرم وجود دارد. در ایران، مقوله پی‌جویی و کشف علمی این جرم، دارای سابقه منسجم علمی و دانشگاهی نیست و نیاز به این مسئله بسیار شایان‌توجه است. سهل‌الوصول‌بودن ارتکاب جرم در فضای سایبر و خصوصیات و ویژگی‌های آن، باعث شکل‌گیری نهضتی بین‌المللی در مبارزه با جرایم سایبری شده‌است؛ اما آنچه که محور اصلی این تحقیق را تشکیل می‌دهد، بحث تدابیر(در سطح کلان) و فنون، راهکارها و روش‌های(در سطح خُرد) مقابله‌ای و جرم‌یابی است که برای مقابله و جرم‌یابی کلاهبرداری سایبری اتخاذ گردیده‌است؛ بنابراین، تحقیق حاضر برای پاسخ به سوال اساسی "الگوی جرم‌یابی کلاهبرداری در فضای سایبر" نگاشته شده‌است. درباره جرم‌یابی کلاهبرداری در فضای سایبر، مشکلات عدیده‌ای وجود دارد که برخی از آنها عبارتند از:

۱. بالابودن رقم سیاه بزه‌کاری درکلاهبرداری سایبری؛
۲. عدم آگاهی و شناخت کامل بزه‌دیدگان و قربانیان کلاهبرداری از این جرم؛
۳. فقدان امکانات کافی در مبارزه با کلاهبرداری سایبری؛
۴. پرهیز از گزارش وقوع کلاهبرداری سایبری به‌علت ترس از لطمه به اعتبار شرکت؛
۵. سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان آن؛
۶. بحث ملی و فراملی بودن کلاهبرداری سایبری.

از این رو، تحقیق حاضر درصدد است تا بااستفاده از نظریات و الگوهای جرم‌یابی و نظرات خبرگان و کارشناسان امر، نسبت‌به تبیین نقاط قوت و ضعف اقدامات جرم‌یابی مبتنی‌بر طراحی الگویی مطلوب اقدام نماید تا از این طریق، بتوان انسجام لازم را در مجموعه اقدامات و برنامه‌های جرم‌یابی از جرایم فضای سایبر، به‌خصوص کلاهبرداری سایبری انجام داده و گامی مهم و اساسی در انجام هرچه بهتر مأموریت‌های محوله در حوزه مبارزه با جرایم سایبری، به‌ویژه کلاهبرداری سایبری برداشت. بر این اساس، سوالات فرعی تحقیق حاضر، به این ترتیب مطرح گردیده‌است:

۱. ابعاد و مولفه‌های جرم کلاهبرداری سایبری کدامند؟
۲. روش‌های مورد استفاده برای جرم‌یابی کلاهبرداری سایبری چیست؟
۳. روش‌های ارتکاب کلاهبرداری در فضای سایبر کدامند؟
۴. الگوهای موجود در جرم‌یابی کلاهبرداری چیست؟
۵. چالش‌های جرم‌یابی کلاهبرداری در فضای سایبر کدامند؟

پیشینه تحقیق

هرچند از تصویب قانون جرایم رایانه‌ای مدت زیادی نمی‌گذرد، با این حال، در برخی از منابع و متون، مطالبی مرتبط با موضوع این تحقیق مورد بررسی قرار گرفته‌است که به شرح ذیل ارائه می‌گردد:

جدول ۱. پیشینه تحقیق

پژوهشگران	موضوع تحقیق	یافته‌های تحقیق
محسنی، فرید؛ صوفی زمرد، محسن	پلیس و چالش‌های اجرایی تأمین امنیت سایبری	هرچند سیاست‌های تقنینی در حوزه امنیت فضای مجازی تا حدودی به جرایم و مجازات‌ها پرداخته‌است اما نیازمند مداخله سیاست‌گذاری و برنامه‌ریزی مجدد می‌باشد. موانع عقیدتی و ایدئولوژیک، ضعف سیاست‌گذاری و زیرساخت‌ها، عدم‌دسترسی، عدم‌مشارکت بخش خصوصی در تأمین امنیت و... از چالش‌های اجرایی می‌باشد.
حاجی ده آبادی، احمد؛ سلیمی، احسان	اصول جرم‌انگاری	این مقاله جرم‌انگاری بی‌ضابطه و گسترده در قوانین کیفری را موجبات بروز آثار و تبعات سوء تورم کیفری دانسته و

پژوهشگران	موضوع تحقیق	یافته‌های تحقیق
	درفضای سایبر(بارویکرد انتقادی به قانون جرایم رایانه‌ای)	جرم‌انگاری در فضای سایبری را هنگامی صحیح و قابل‌پذیرش می‌داند که بر مبنای اصولی چون ضرورت و مشروعیت انجام شود و از تناسب دقیقی بین رفتار مجرمانه و نوع مجازات برخوردار باشد.
رجبی، ابراهیم	جرم‌شناختی فضای اینترنت	به نظر مولف، آگاهی از پیامدهای استفاده از اینترنت و درنظرگرفتن راهبردهای مناسب برای استفاده درست و پیش‌گیری از اثرات احتمالی منفی آن، اهمیتی اساسی دارد. بر اساس یافته‌های این تحقیق، اینترنت علاوه‌بر دستاوردهای مثبت و انکارناپذیر، دارای پیامدهای نامطلوبی از جمله اعتیاد اینترنتی، انحرافات جنسی، و سلطه فرهنگی است که باید موردتوجه والدین و برنامه‌ریزان قرار گیرد.
رضوی، محمد	جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها	در این مقاله، به چالش‌های نوین جرایم سایبری در حوزه پیشگیری و کشف جرم پرداخته شده‌است و آموزش‌های تخصصی و جامع درخصوص رایانه و اینترنت را پیشنهاد می‌نماید.
وروایی، اکبر؛ میرزکی، سید شمس الدین	بررسی عوامل موثر بر کشف جرم کلاهبرداری رایانه‌ای	این مقاله مبارزه با جرایم سایبری، به‌خصوص کلاهبرداری رایانه‌ای را نیازمند تدابیر و راهکارهای نوینی دانسته‌است و توانمندی کارآگاهان و تجهیزات سازمانی و ارتقای دانش فنی مأموران پی‌جویی را بر عملکرد بهتر مأموران در کشف جرم کلاهبرداری رایانه‌ای موثر دانسته‌است.

مفاهیم تحقیق

جرم‌یابی[1]

جرم‌یابی را رشته حرفه‌ای و علمی مدیریت تشخیص، تعیین، تمایز(تفرد) و ارزیابی ادله مادی با استفاده از علوم فیزیکی و طبیعی در موضوعات علوم حقوقی تعریف کرده‌است(موذن زادگان و حمیدزاده، ۱۳۹۲: ۱۰۰). در تعریفی دیگر، جرم‌یابی را علمی که درباره کاربرد علوم مادی در کشف جرایم و شناسایی مجرمان و اثبات جرم بحث کرده و به سه شاخه کشف علمی جرایم، پزشکی قانونی و روان‌شناسی تقسیم می‌شود، دانسته‌اند.

فضای سایبر(فضای مجازی)

واژه سایبردر زبان فارسی، به‌معنای مجازی ترجمه شده‌است و از لغت یونانی کیبرنتس[2] به‌معنی سکاندار یا راهنما مشتق شده‌است(کمالی‌زاده و همکاران، ۱۳۹۴: ۲۱). نخستین‌بار اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ به کار برده شد. در۱۹۸۴ نیز یک نویسنده علمی ـ تخیلی به نام ویلیام گیبسون، واژه سایبر را به اسپیس چسباند تا شبکه‌های رایانه‌ای دنیای برخط را نشان دهد و از آن زمان، فضای سایبر مترادف با دنیای رایانه‌ها و شبکه اینترنت قرار گرفت. بر این اساس، می‌توان فضای سایبر را مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی نامید.

جرایم سایبری

جرایم سایبری شامل جرم‌هایی است که در محیط سایبر به وجود می‌آیند. درخصوص جرایم فضای سایبری از ابتدای دهه ۷۰ تا امروز، تعریف مورد توافقی که بتواند تمام ویژگی‌های یک تعریف جامع و مانع را شامل شود، ارائه نشده‌است(نجفی علمی، ۱۳۹۳: ۲۳). این اصطلاح، بیشتر زمانی مورد استفاده قرار می‌گیرد که فعالیت‌های تبهکارانه با استفاده از ابزارها، نرم‌افزارهای

1. Criminalistics
1. Kyber Netes

کاربردی و شبکه‌های رایانه‌ای به‌عنوان ابزار یا هدف انجام شده باشد. جرایم سایبری به دو صورت تعریف می‌شود: ۱. جرایم سایبری محض ؛ ۲. جرایم سایبری انتقالی(توسعه یافته).

"جرایم سایبری محض" جرمی است که فقط مختص فضای سایبر بوده و قبلا از جرایم سنتی به شمار نمی‌رفته‌است و تنها با شکل‌گیری فضای سایبر می‌تواند اتفاق بیفتد؛ همانند ساپوتاژ(تخریب داده)؛ به این معنی که باید داده وجود داشته باشد تا تخریب انجام شود. اما "جرایم سایبری انتقالی(توسعه یافته)" جرایمی هستند که قبلا در فضای واقعی به‌عنوان جرم تعریف شده‌اند و در حال حاضر، این جرایم به فضای سایبر انتقال یافته‌اند؛ همانند سرقت و کلاهبرداری که در فضای واقعی نیز جرم است و امروزه، در فضای سایبر نیز اتفاق می‌افتد(نجفی علمی، همان: ۲۴).

جرم‌یابی سایبری

جرم‌یابی سایبری علمی است در راستای یافتن یا کشف جرم و نگهداری از شواهد و یا مدارک دیجیتالی که در فضای سایبر ارتکاب یافته‌است و موثق و قابل‌ارائه به دادگاه است. گسترش فرصت‌های فعالیت مجرمانه در فضای سایبر و نگرانی جامعه از این جرایم، منجر به ایجاد و گسترش جرم‌شناسی و جرم‌یابی سایبری به‌عنوان یک رشته مستقل مرتبط با چارچوب جرم‌شناسی شده‌است که می‌توان آن را دانشی نوپا دانست که پیشرفت و گسترش آن نیازمند همکاری و همت دست‌اندرکاران علوم پلیسی، قضایی و... می‌باشد(نظری منظم، ۱۳۹۹: ۲۸).

کلاهبرداری سایبری

کمیته تخصصی شورای اروپا در زمینه جرایم رایانه‌ای، واردکردن، تغییر، محو یا موقوف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای یا دیگر مداخلات در پردازش داده‌ها که بر نتیجه پردازش داده‌ها اثر بگذارد و موجب ضررهای اقتصادی یا هر تصرفی در اموال شخصی دیگر به قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یا دیگری شود(راه‌حل جایگزین: با قصد محروم‌کردن

غیرقانونی آن شخص از اموالش) را کلاهبرداری سایبری تعریف نموده‌است(نجفی علمی، همان: ۲۸).

جرم‌یابی کلاهبرداری سایبری

منظور از جرم‌یابی کلاهبرداری سایبری در این تحقیق، کلیه امور فنی، علمی، عملی و... است که در راستای یافتن یا کشف جرم کلاهبرداری سایبری و نگهداری از شواهد و یا مدارک دیجیتالی که بر روی رایانه یا شبکه فرد مظنون وجود دارد، صورت می‌پذیرد؛ به‌طوری‌که این نوع شواهد و مدارک قانونی موثق و قابل ارائه به دادگاه بوده و نتیجه اقدامات مذکور نیز منجر به کشف جرایم سایبری و یا کاهش احتمال وقوع آن گردد(نظری منظم، همان: ۲۹).

روش‌شناسی تحقیق

هدف از انجام تحقیق حاضر، دستیابی به مجموعه راهکارهایی برای تقویت جرم‌یابی کلاهبرداری در فضای سایبر می‌باشد؛ بدین‌لحاظ، این تحقیق از نظر هدف، کاربردی و از لحاظ ماهیت و روش، توصیفی ـ اکتشافی است و از جهت نوع داده‌ها، آمیخته(کمی و کیفی) است. این تحقیق در پی آن است که از طریق بررسی و جستجو، ابعاد و ماهیت اقدامات و نیز نقاط قوت و ضعف اقدامات در راستای مبارزه با جرم کلاهبرداری سایبری را احصا نموده و مورد بررسی قرار دهد؛ بنابراین، تحقیق حاضر از نوع اکتشافی است؛ ضمن اینکه، از نظر روش گردآوری داده‌ها، این تحقیق، توصیفی از نوع پیمایشی است.

جامعه آماری بخش کیفی تحقیق، شامل خبرگان فضای سایبر، قضات و مراجع قضایی مرتبط و اساتید صاحب‌نظر در این حوزه به تعداد ۱۰۰ نفر می‌باشند و جامعه آماری بخش کمی نیز ۲۵۳ نفر شامل خبرگان مرتبط با موضوع در هر دو حوزه نظری و تجربی هستند.

حجم نمونه و روش نمونه‌گیری

الف. مرحله اول(کیفی): تا اشباع نظری محقق با قضات، مراجع قضایی، فرماندهان، روسا و مدیران عالی منتخب، مصاحبه نیمه‌ساختاریافته صورت پذیرفت؛ بنابراین، در این مرحله، نمونه‌گیری هدفمند بوده‌است.

ب. مرحله دوم(کمی): حجم نمونه با استفاده از فرمول کوکران مشخص که با توجه به جامعه ۲۸۵ نفری، تعداد ۱۴۳ نفر درنظرگرفته شده‌است.

روش نمونه‌گیری در مرحله مصاحبه، نمونه‌گیری هدفمند بود و خبرگانی که در هر دو بعد جرم‌یابی فضای سایبر و مفاهیم حقوقی مرتبط با حوزه فضای سایبر، از تجربه و تخصص لازم برخوردار بوده‌اند، انتخاب شدند. در مرحله دوم نیز برای انتخاب نمونه‌ها(به‌نحوی‌که معرف جامعه آماری باشند) از روش نمونه‌گیری طبقه‌ای به‌صورت تصادفی استفاده گردیده‌است.

روش گردآوری اطلاعات

در گام اول، پس از جمع‌آوری داده‌های نظری، برای دستیابی به نتایج اولیه از طریق مصاحبه نیمه‌ساختاریافته با خبرگان موضوع تا اشباع نظری محقق، مصاحبه صورت پذیرفت. در گام دوم، با جمع‌بندی داده‌های نظری و مصاحبه‌های انجام‌شده، پرسش‌نامه لازم تدوین گردید و بین حجم نمونه آماری انتخاب‌شده توزیع شد. ابزار گردآوری داده‌ها در این تحقیق، در گام اول، مصاحبه نیمه‌ساختاریافته و در گام دوم، پرسش‌نامه محقق‌ساخته بر مبنای نظریه‌های علمی مرتبط و مصاحبه با خبرگان است.

شیوه اجرا و واحد تحلیل

در این پژوهش، از روش توصیفی در تحلیل الگوی جرم‌یابی کلاهبرداری سایبری استفاده شد. در روش استنباطی، بااستفاده از نرم‌افزارهای آماری Spss، لیزرل و تحلیل عاملی اکتشافی، تجزیه‌وتحلیل لازم در زمینه نقش عوامل تأثیرگذار در جرم‌یابی کلاهبرداری در فضای سایبر صورت پذیرفت. قلمرو زمانی تحقیق سال ۹۶-۹۵ بود و روایی پژوهش از نوع روایی محتوایی و از طریق مصاحبه با خبرگان مورد تأیید قرار گرفته است و پایایی نیز از طریق آلفای کرونباخ و نرم‌افزارspss، ۸۷/. محاسبه شده‌است.

یافته‌های تحقیق

در این بخش، اطلاعات حاصل از پرسش‌نامه وارد نرم‌افزار SPSS22 شده و تجزیه‌وتحلیل داده‌ها در دو بخش توصیفی و استنباطی ارائه شده‌است. در بخش توصیفی، از شاخص گرایش به مرکز میانگین و شاخص‌های فراوانی، درصد و فراوانی تجمعی استفاده شده‌است. این بخش شامل توصیف جمعیت نمونه، توصیف سوالات، شاخص‌ها و ابعاد است. درقسمت استنباطی این فصل، ابتدا طبیعی‌بودن توزیع داده‌ها بررسی شده و سپس از آزمون‌های پارامتریک استفاده گردید(فرض صفر در این آزمون، طبیعی‌بودن توزیع داده‌هاست). در قسمت دوم، تصادفی‌بودن توزیع داده‌ها ارائه شده‌است. درصورتی‌که سطح معناداری در این آزمون، کمتر از ۰۵/. باشد، می‌توان با اطمینان ۹۵درصد بیان کرد که توزیع داده‌ها تصادفی است. در قسمت آخر نیز با استفاده از آزمون‌های آماری متناسب نظیر kmo، بارتلت، واریمکس و بار عاملی داده‌ها، به سوالات تحقیق پاسخ داده شد.

اطلاعات جمعیت‌شناختی

جدول۲. اطلاعات جمعیت‌شناختی(بخش کیفی)

متغیر	طبقه	فراوانی	درصد	درصد فراوانی تجمعی
سازمان	پلیس	۱۱	۶۱	۶۱
	دستگاه قضایی	۵	۲۸	۸۹
	سایر دستگاه‌ها	۲	۱۱	۱۰۰
میزان تحصیلات	کاردانی و پایین‌تر	۲	۱۱/۱	۱۱/۱
	کارشناسی	۱۲	۶۶/۷	۷۷/۸
	کارشناسی‌ارشد و بالاتر	۴	۲۲/۲	۱۰۰
سن	۳۰ سال و کمتر	۲	۱۱/۱	۱۱/۱
	۳۱ تا ۴۰ سال	۹	۵۰	۶۱/۱
	۴۱ سال و بالاتر	۷	۳۸/۹	۱۰۰
سابقه فعالیت	۱۰ سال و کمتر	۲	۱۱/۱	۱۱/۱
	۱۱ تا ۱۵ سال	۵	۲۷/۸	۳۸/۹
	۱۶ الی ۲۰ سال	۸	۴۴/۴	۸۳/۳
	۲۱ سال و بالاتر	۳	۱۶/۷	۱۰۰

همان‌گونه که در جدول شماره ۲ قابل‌مشاهده است، در بررسی توصیفی ویژگی‌های جمعیت‌شناختی مربوط به سازمان محل فعالیت پاسخ‌دهندگان به مصاحبه، ۶۱ درصد از پاسخ‌دهندگان جزو پلیس، ۲۸ درصد دستگاه قضایی و ۱۱ درصد نیز جزو سایر دستگاه‌ها می‌باشند. در بررسی توصیفی ویژگی‌های جمعیت‌شناختی مربوط به میزان تحصیلات پاسخ‌دهندگان، ۶۶/۷ درصد دارای مدرک تحصیلی کارشناسی، ۲۲/۲ درصد کارشناسی‌ارشد و بالاتر و ۱۱/۱ درصد نیز کاردانی و پایین‌تر می‌باشند و درمجموع، ۹۰ درصد مشارکت‌کنندگان کارشناسی و بالاتر هستند. در بررسی توصیفی ویژگی‌های جمعیت‌شناختی مربوط به سن پاسخ‌دهندگان، ۵۰ درصد پاسخ‌دهندگان دارای سن ۳۱ الی ۴۰ سال، ۳۸/۹ درصد دارای سن ۴۱ سال و بالاتر و ۱۱/۱ درصد نیز دارای سن ۳۰ سال و پایین‌تر می‌باشند. در بررسی توصیفی ویژگی‌های جمعیت‌شناختی مربوط به سابقه فعالیت پاسخ‌دهندگان، ۴۴/۴ درصد پاسخ‌دهندگان دارای سابقه ۱۶ الی ۲۰ سال، ۲۷/۸ درصد دارای سابقه ۱۱ الی ۱۵ سال، ۱۶/۷ درصد نیز دارای سابقه ۲۱ سال و بالاتر و ۱۱/۱ درصد دارای سابقه ۱۰ سال و کمتر می‌باشند و حدود ۹۰ درصد سابقه بالاتر از ده سال دارند و این نشان‌دهنده آن است که افراد شرکت‌کننده در این تحقیق، از تجربه لازم و خبرگی در این حوزه برخوردار می‌باشند.

جدول۳. اطلاعات جمعیت نمونه(بخش کمی)

متغیر	گروه	فراوانی	درصد
تحصیلات	کاردانی و پایین‌تر	۱۳	۹
	کارشناسی	۷۱	۴۹/۶
	کارشناسی‌ارشد و بالاتر	۵۹	۴۱/۴
سن	تا ۳۰ سال	۲۱	۱۴/۶
	۳۱ تا ۴۰ سال	۵۸	۴۰/۵۵
	۴۱ سال تا ۵۰ سال	۴۰	۲۷/۹
	۵۱ سال و بالاتر	۲۴	۱۶/۹
سابقه فعالیت	تا ۱۰ سال	۵۹	۴۱/۲
	۱۱ تا ۱۵ سال	۴۲	۲۹/۳
	۱۶ تا ۲۰ سال	۳۰	۲۰/۹
	۲۱ سال و بالاتر	۱۲	۸/۶

همان‌گونه که در جدول شماره ۳ قابل‌مشاهده است، در بررسی توصیفی ویژگی‌های جمعیت‌شناختی پاسخ‌دهندگان به پرسش‌نامه تنظیمی(حاصل از مرحله کیفی)، در متغیر تحصیلات ۴۹/۶ درصد دارای مدرک کارشناسی، ۴۱/۴ درصد دارای مدرک کارشناسی‌ارشد و دکتری و ۹ درصد دارای مدرک کاردانی و پایین‌تر هستند. در بررسی سن پاسخ‌دهندگان، ۴۰/۵۵ درصد دارای سن ۳۱ الی ۴۰ سال، ۲۷/۹ درصد دارای سن ۴۱ الی ۵۰ سال، ۱۶/۹ درصد دارای سن ۵۱ سال و بالاتر و ۱۴/۶ درصد دارای سن تا ۳۰ سال هستند. درخصوص سابقه فعالیت، ۴۱/۲ درصد دارای سابقه تا ۱۰ سال، ۲۹/۳ درصد دارای سابقه ۱۱ تا ۱۵ سال، ۲۰/۹ درصد دارای سابقه ۱۶ تا ۲۰ سال و ۸/۶ درصد نیز دارای سابقه ۲۱ سال و بالاتر هستند.

جدول ۴. رتبه‌بندی ابعاد و مولفه‌های جرم کلاهبرداری سایبری

عنوان	مقدار آزمون KMO	سطح معناداری	ابعاد	مولفه‌ها	مقدار بار عاملی	رتبه
ابعاد	./۷۵۸	./۰۰۰	فردی	اقتصادی	./۸۲۳	۱
				مهارت افراد		
				مشکلات روحی و روانی		
			اجتماعی	احساس بی‌عدالتی	./۸۰۹	۲
				فقر فرهنگی		
				روابط اجتماعی ناسالم		
				آگاه‌سازی شهروندان		
			زیرساختی	مشکلات امنیتی سامانه‌های بانکی و پولی	./۷۱۱	۳
				سامانه‌های جرم‌یابی پلیس		

با توجه به مقدار آزمون kmo که ۷۵۸/. و بارتلت که ۹۵۲/۷۴ و سطح معناداری ۰۰۰/. می‌توان با اطمینان ۹۵ درصد بیان کرد که ابعاد و مولفه‌های شناسایی‌شده، معتبر بوده و این ابعاد و مولفه‌ها ۷۸/. درصد از واریانس کل را تبیین می‌کند و رتبه‌بندی این ابعاد نشان داد که ابعاد فردی با بار عاملی ۸۲۳/.

در رتبه اول، اجتماعی با ضریب ۸۰۹/. در رتبه دوم و زیرساختی با بار عاملی ۷۱۱/. در رتبه سوم قرار دارد.

روش‌های مورد استفاده برای جرم‌یابی کلاهبرداری سایبری

جدول ۵. اعتبارسنجی رتبه‌بندی اقدامات

مقدار آزمون KMO	مقدار آزمون بارتلت	سطح معناداری	درجه آزادی	مقدار واریمکس
۸۱۷/.	۱۹۶۰/۰۹	۰۰۰/.	۱۳	۷۱/.

با توجه به مقدار آزمون kmo که ۸۱۷/. و بارتلت که ۱۹۶۰/۰۹ و سطح معناداری ۰۰۰/. می‌توان با اطمینان ۹۵ درصد بیان کرد که رتبه‌بندی اقدامات شناسایی‌شده، معتبر بوده و روش‌های موردنظر ۷۱/. درصد از واریانس کل را تبیین می‌کند که برای رتبه‌بندی این روش‌ها باید به جدول بعد و مقدار ضریب بارعاملی مراجعه کرد:

جدول ۶. رتبه‌بندی روش‌های مورد استفاده

روش‌های مورد استفاده	مقدار بار عاملی	رتبه
استفاده از تله IP برای به‌دست‌آوردن اطلاعات فرد	۸۶۳/.	۱
گشت‌زنی سایبری	۸۵۲/.	۲
مهندسی اجتماعی و رصد فعالیت‌های سایبری فرد متهم	۸۴۲/.	۳
استفاده از منابع و مخبرین و گزارش‌های مردمی	۸۴۲/.	۴
بهره‌برداری از امکانات سازمان‌های سرویس‌دهنده و زیرساخت	۸۲۲/.	۵
استعلام از بانک‌ها و موسسات مالی	۸۰۳/.	۶
استفاده از هوشمندسازی و هوش‌مصنوعی و یادگیری ماشینی برای رصد مستمر	۷۹۹/.	۷
رصد صفحات اجتماعی و پروفایل فرد	۷۸۲/.	۸
بررسی پست‌ها و تحلیل مطالب پست	۷۷۴/.	۹
نفوذ به دایرکت متهمین	۷۴۹/.	۱۰
بررسی پست‌الکترونیک فرد	۷۲۲/.	۱۱
تحلیل شبکه ارتباطی	۷۱۴/.	۱۲
ردیابی شماره‌های تماس وستیر ردیابی‌های فنی	۷۰۹/.	۱۳
بهره‌گیری از سامانه‌های هوشمند کشف جرم	۷۰۱/.	۱۴

در بررسی روش‌های مورد استفاده، ۱۴ روش اصلی شناسایی شده‌است که در بررسی دقیق‌تر مشخص می‌شود " استفاده از تله IP برای به‌دست‌آوردن اطلاعات فرد " با بار عاملی ۸۶۳/. در رتبه اول، " گشت زنی سایبری " با بار عاملی ۸۵۲/. در رتبه دوم و " مهندسی اجتماعی و رصد فعالیت‌های سایبری فرد متهم " و " استفاده از منابع و مخبرین و گزارش‌های مردمی " با بار عاملی ۸۴۲/. در رتبه سوم قرار دارند.

شگردها و شیوه‌های مجرمان برای کلاهبرداری در فضای سایبر طی پنج سال گذشته

جدول ۷. اعتبارسنجی رتبه‌بندی شگردهای مجرمان

مقدار آزمون KMO	مقدار آزمون بارتلت	سطح معناداری	درجه آزادی	مقدار واریمکس
/۷۹۶	۲۱۰۶/۳۱	/۰۰۰	۱۳	/۷۸

با توجه به مقدار آزمون kmo که ۷۹۶/. و بارتلت که ۲۱۰۶/۳۱ و سطح معناداری ۰۰۰/. می‌توان با اطمینان ۹۵ درصد بیان کرد که رتبه‌بندی شگردهای مجرمان معتبر بوده و روش‌های موردنظر ۷۸/. درصد از واریانس کل را تبیین می‌کند که برای رتبه‌بندی این شگردها باید به جدول بعد و مقدار ضریب بار عاملی مراجعه کرد:

جدول ۸. رتبه‌بندی روش‌های مورد استفاده

شگردهای مجرمین	مقدار بار عاملی	رتبه
فیشنگ و فارمینگ صفحه ورود به سایت‌های تبادلات مالی جهت سرقت اطلاعات	/۸۴۲	۱
فریب تلفنی و پیامکی	/۸۳۲	۲
روش اسکیمر	/۸۲۵	۳
فروش کالاهای بی‌کیفیت و اخذ وجه اینترنتی بدون تحویل کالا در بازارهای آنلاین	/۸۲۵	۴
قمار و شرطبندی	/۸۱۲	۵
اخاذی از طریق گروکشی تصاویر، فیلم و اطلاعات خصوصی افراد و ...	/۸۰۶	۶
ارسال پیامک برنده‌شدن در لاتاری	/۷۸۵	۷
دوستیابی	/۷۸۲	۸
کلاهبرداری پنجره‌ای	/۷۷۵	۹

شگردهای مجرمین	مقدار بار عاملی	رتبه
استفاده از بد افزارها	/۷۶۳	۱۰
کلاهبرداری‌های برخط از طریق چت و پست‌الکترونیک	/۷۵۲	۱۱
بهره‌برداری از کسب‌وکارهای نوین در فضای مجازی	/۷۲۶	۱۲
شنود سامانه‌های مخابراتی	/۷۱۵	۱۳

در بررسی شگرها و شیوه‌های کنونی مجرمین، ۱۴ شگرد شناسایی شده‌است و در بررسی دقیق‌تر مشخص شد که "فیشنگ و فارمینگ صفحه ورود به سایت‌های تبادلات مالی جهت سرقت اطلاعات" با بار عاملی ۸۴۲/. در رتبه اول، "فریب تلفنی و پیامکی" با بار عاملی ۸۳۲/. در رتبه دوم و "روش اسکیمر" و "فروش کالاهای بی‌کیفیت و اخذ وجه اینترنتی بدون تحویل کالا در بازارهای برخط" با بار عاملی ۸۲۵/. در رتبه سوم قرار دارند.

مهم‌ترین چالش‌ها در جرم‌یابی کلاهبرداری در فضای سایبر

جدول ۹. اعتبارسنجی رتبه‌بندی چالش‌های شناسایی‌شده

مقدار آزمون KMO	مقدار آزمون بارتلت	سطح معناداری	درجه آزادی	مقدار واریمکس
/۷۵۲	۲۲۶/۵۸	/۰۰۰	۱۳	/۷۳

با توجه به مقدار آزمون kmo که ۷۵۲/. و بارتلت که ۲۲۶/۵۸ و سطح معناداری ۰۰۰/. می‌توان با اطمینان ۹۵ درصد بیان کرد که رتبه‌بندی چالش‌های شناسایی‌شده معتبر بوده و روش‌های مورد نظر ۷۳/. درصد از واریانس کل را تبیین می‌کند که برای رتبه‌بندی این چالش‌ها باید به جدول بعد و مقدار ضریب بارعاملی مراجعه کرد:

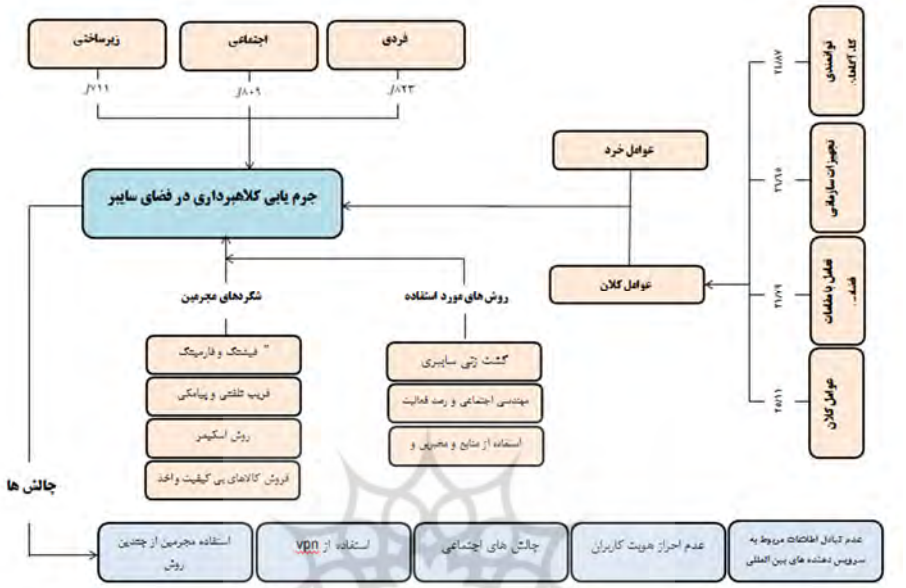
جدول ۱۰. رتبه‌بندی چالش‌های شناسایی‌شده

روش مورد استفاده	مقدار بار عاملی	رتبه
استفاده مجرمان از چندین روش پیچیده جهت اختفای هویت به‌صورت هم‌زمان	/۸۶۹	۱
استفاده از VPN(رد زنی IP را دو چندان می‌کند)	/۸۵۲	۲
چالش‌های اجتماعی(پذیرفته‌شدن برخی رفتارهای ناهنجار در جامعه)	/۸۴۱	۳
عدم احراز هویت کاربران	/۸۲۹	۴
عدم‌تبادل اطلاعات مربوط به سرویس‌دهنده‌های بین‌المللی	/۸۱۶	۵
استفاده از پول‌های مجازی غیرقابل‌ردگیری	/۸۰۸	۶
چالش‌های قضایی(کم‌سن بودن مجرمان و ...)	/۷۸۶	۷
فراگیرشدن استفاده از پیام‌های رمزنگاری‌شده در پیام‌رسان‌ها	/۷۸۲	۸
ضعف دانش و آگاهی امنیتی کاربران	/۷۸۰	۹
توسعه روزافزون فضای سایبر بدون‌توجه به امنیت	/۷۵۶	۱۰
رشد کسب‌وکارهای غیرمجاز و بی‌ضابطه	/۷۴۶	۱۱
عدم‌انسجام و هماهنگی متولیان حوزه سایبر کشور	/۷۳۲	۱۲
اینترنت اشیا و اینترنت آزاد	/۷۲۹	۱۳
فراملی‌بودن برخی از کلاهبرداری‌ها	/۷۱۶	۱۴

در بررسی چالش‌ها، ۱۴ چالش شناسایی شده‌است و در بررسی دقیق‌تر شد که "استفاده مجرمان از چندین روش پیچیده جهت اختفای هویت به‌صورت هم‌زمان" با بار عاملی ۸۶۹/. در رتبه اول، "استفاده از VPN(رد زنی IP را دو چندان می‌کند)" با بار عاملی ۸۵۲/. در رتبه دوم و "چالش‌های اجتماعی(پذیرفته شدن برخی رفتارهای ناهنجار در جامعه)" با بار عاملی ۸۴۱/. در رتبه سوم قرار دارند.

الگوی تحلیلی تحقیق

الگوی تحلیلی تحقیق در نمودار شماره ۱ ارائه شده‌است:



نمودار ۱. الگوی تحلیلی تحقیق

بحث و نتیجه‌گیری

نتایج تحقیق حاضر، در سه بعد زیر قابل بررسی است:

الف. ابعاد و مولفه‌ها

طبق نتایج تحقیق، سه بعد فردی، اجتماعی و زیرساختی، بیشترین اثرگذاری را در جرم‌یابی کلاهبرداری سایبری دارا می‌باشند. در ابعاد "فردی" سه عامل اقتصادی، مهارت افراد و مشکلات روحی، بیشترین نقش را دارا هستند. در ابعاد "اجتماعی" احساس بی‌عدالتی، فقر فرهنگی، روابط اجتماعی ناسالم و آگاه‌سازی شهروندان، بیشتر از سایر عوامل موردتوجه قرار گرفته‌اند. در قسمت "زیرساختی" امنیت سامانه‌ها و سامانه‌های جرم‌یابی بیشترین نقش را برعهده دارند. نتایج این بخش با نتایج به‌دست‌آمده در تحقیقات شومیکر و کاتکلین(۲۰۱۶)، یاسمی نژاد(۱۳۹۲) و شیرمحمدی(۱۳۹۶) هم‌راستا می‌باشد.

ب. روش‌های مورد استفاده

نتایج تحقیق نشان می‌دهد که استفاده از تله IP برای به‌دست‌آوردن اطلاعات فرد، گشت‌زنی سایبری، مهندسی اجتماعی و رصد فعالیت‌های سایبری فرد متهم، استفاده از منابع و مخبرین و گزارش‌های مردمی، بهره‌برداری از امکانات سازمان‌های سرویس‌دهنده و زیرساخت، استعلام از بانک‌ها و موسسات مالی، استفاده از هوشمندسازی و هوش مصنوعی و یادگیری ماشینی برای رصد مستمر، رصد صفحات اجتماعی و پروفایل فرد، بررسی پست‌ها و تحلیل مطالب پست نفوذ به دایرکت متهمان، بررسی ایمیل‌های فرد، تحلیل شبکه ارتباطی، ردیابی شماره‌های تماس وستیر ردیابی‌های فنی و نیز بهره‌گیری از سامانه‌های هوشمند کشف جرم می‌تواند برای جرم‌یابی کلاهبرداری در فضای سایبر مورد استفاده قرار گیرد. نتایج این بخش، هم‌سو با نتایج تحقیقات توانبخش(۱۳۹۶) و تراب‌زاده(۱۳۸۸) می‌باشد.

ج. شگردها و شیوه‌های کنونی مجرمان

کلاهبرداران سایبری مانند همتایان کلاسیک خود، طیف وسیعی از انگیزه‌ها را در سر می‌پرورانند؛ زیرا اکنون نیز همان انگیزه‌های سنتی که همواره با بشر همراه بوده‌است، در پوششی نوین در فضای سایبر رخنمایی می‌کند. در بررسی شگردها و شیوه‌های کنونی مجرمان در تحقیق حاضر، ۱۴ شگرد شناسایی شده‌است که مهم‌ترین آنها به قرار زیر است: فیشنگ و فارمینگ صفحه ورود به سایت‌های تبادلات مالی جهت سرقت اطلاعات، فریب تلفنی و پیامکی، روش اسکیمر، فروش کالاهای بی‌کیفیت و اخذ وجه اینترنتی بدون تحویل کالا در بازارهای آنلاین، قمار و شرط‌بندی، اخاذی از طریق گروکشی تصاویر، فیلم و اطلاعات خصوصی افراد و ارسال پیامک برنده‌شدن در لاتاری، دوستیابی، کلاهبرداری پنجره‌ای، استفاده از بدافزارها، کلاهبرداری‌های برخط از طریق چت و ایمیل، بهره‌برداری از کسب‌وکارهای نوین در فضای مجازی و شنود سامانه‌های مخابراتی. این نتایج هم‌سو با نتایج دیانتی(۱۳۸۷)، سیمون(۲۰۱۴) و توانبخش(۱۳۹۶) می‌باشد.

پیشنهادهای کاربردی

به‌منظور افزایش درصد موفقیت در جرم‌یابی کلاهبرداری سایبری، تأمین برخی تجهیزات از ضروریات غیرقابل‌انکار تلقی می‌شود که مهم‌ترین آنها به شرح زیر است:

۱. سخت‌افزارهای پی‌جویی و کشف جرایم رایانه‌ای، سخت‌افزارهای جلوگیری از نگارش داده‌ها، سخت‌افزارهای تصویربرداری از دیسک‌ها و نرم‌افزارهای جلوگیری از نگارش داده‌ها؛

۲.نرم‌افزارهای پی‌جویی جرایم رایانه‌ای، نرم‌افزارهای جلوگیری از نگارش داده‌ها نظیر پی.دی.بلاک[1]، نرم‌افزارهای جستجوی داده‌ها، نرم‌افزارهای تصویربرداری از داده‌ها، نرم‌افزارهای تصویربرداری لحظه‌ای و کپی‌کردن فایل، نرم‌افزارهای جمع‌آوری و تجزیه‌وتحلیل داده‌ها.

۳. احداث آزمایشگاه جنایی رایانه‌ای[2]: انجام تحقیقات درحوزه فناوری‌های نوین بسیار وابسته به آزمایشگاه‌های تخصصی است. کشف علمی جرایم با اتکا به روش‌های نوین علمی و درآزمایشگاه‌ها از قابلیت ارزیابی و ممیزی برخوردار می‌باشند و ضابطین در این آزمایشگاه‌ها به‌صورت علمی به‌دنبال کشف جرایم هستند. همچنین، با توجه به نیازهای تحقیقاتی و جرایم رایانه‌ای، این آزمایشگاه‌ها می‌توانند نیاز ضابطین قضایی را در رابطه با بررسی جرایم رایانه‌ای برآورده سازند؛ آزمایشگاه‌هایی نظیر آزمایشگاه بررسی تصاویر و فیلم، آزمایشگاه بررسی اصوات، آزمایشگاه بررسی جرایم مربوط به ذخیره‌سازی دیجیتالی، آزمایشگاه بررسی جرایم مربوط به دستگاه‌های سیار، ذخیره‌سازی ادله، آماده‌سازی کیت‌های بررسی جرایم دیجیتال و آزمایشگاه موبایل[3].

۴.آزمایشگاه شناسایی جرایم تصویری: داده‌های تصویری ادله بیسار غنی و متقاعدکننده‌ای را ارائه می‌دهند و خوشبختانه دستکاری داده‌های تصویری، دشوار، هزینه‌بر و وقت‌گیر است و ازاین‌رو، به‌ندرت صورت

1.PD Block
2. Computer Forensics Lab
3. http//7Safe. com/training

می‌پذیرد؛ اما توانایی شناسایی آنها درتحقیقات، از اهمیت به‌سزایی برخوردار است. بررسی جرایم تصویری توانمندی‌هایی را جهت تعیین صحت و سقم از طریق شناسایی الگو، انطباق محتوای ادله با نمونه‌های شناخته‌شده ارائه می‌دهد. توانایی در جهت ارتقای تصویر به‌منظور تعیین درستی نوع تشخیص بسیار مهم است. نقش حمایتی در بررسی جرایم بصری، توانایی در اندازه‌گیری اجزای خاصی از تصویر است؛ از جمله ارتفاع، پهنا یا عمق که درواقع، اجزای فیزیکی را به‌صورت تصویری مشخص می‌کند.

۵.آزمایشگاه بررسی جرایم صوتی: داده‌های صوتی از دیگر منابع اطلاعاتی غنی به شمار می‌روند. الگوهای سمعی با نمونه‌های شناخته‌شده منطبق می‌شوند تا بدین‌ترتیب، منبع، هویت، موقعیت، زمان یا سایر ادله جهت انجام تحقیقات شناسایی شوند. جهت نیل به این هدف، لازم است که آزمایشگاه، صداها و فرکانس‌ها را تفکیک کرده و با نمونه‌های شناخته‌شده مقایسه کند. به‌علاوه، شناسایی صداهای دستکاری‌شده جهت تأیید انسجام ادله جمع‌آوری‌شده بسیار مهم است.

۶.آزمایشگاه بررسی جرایم مربوط به ذخیره‌سازی دیجیتالی: معمول‌ترین و مهم‌ترین شکل ذخیره‌سازی دیجیتالی "هارددیسک" است که بخش اصلی ذخیره‌سازی را در بسیاری از سامانه‌های دیجیتال تشکیل می‌دهد. داده‌های هارددیسک باید به‌لحاظ منطقی، الکترونیکی و حتی فیزیکی، بازیابی شوند و لازم است که جهت حصول اطمینان از اینکه لایه دربرگیرنده بیت‌های اطلاعاتی آسیب نبیند، مراقبت فیزیکی صورت گیرد. در این آزمایشگاه، تجهیزات حساس الکترونیکی مورد استفاده قرار می‌گیرد ولازم است که فیلترهای گردوغبار و ذرات نصب شوند(محرمی، ۱۳۹۳: ۶۴).

۷.آزمایشگاه بررسی وسایل و دستگاه‌های سیار: وسایل سیار تقریبا در تمامی جوامع مدرن موجود است. این ابزارها، برنامه‌ها، تماس‌ها، پیام‌ها، تصاویر، موارد سمعی و بصری و ... را ذخیره می‌کنند؛ به‌نحوی‌که همواره بتوانیم

در ارتباط باقی بمانیم. چنین ارتباطی اطلاعات غنی را تأمین می‌کند؛ اطلاعاتی که فعالیت‌ها، روابط و تاحدی قصد و نیت ما را به تفصیل شرح می‌دهد؛ به‌طورکلی، تاریخچه‌ای از زندگی دیجیتال ما را نشان می‌دهد. اهمیت ایجاد این آزمایشگاه، به‌دلیل وجودتنوع وگوناگونی وسایل سیار در بازار است.

درحقیقت، جرایم سایبری ـ به‌ویژه جرایم کلاهبرداری سایبری که ماهیتی فراملی داشته و از لحاظ ارتکاب در بعد حقوق کیفری، ماهیتی کاملا نوین دارند ــ حقوق اطلاعاتی کیفری را در معرض چالش‌های جدیدی قرار داده‌است؛ در جمهوری‌اسلامی‌ایران نیز با توجه به ارتکاب موج گسترده‌ای از کلاهبرداری سایبری با استفاده از فضای سایبری و رواج استفاده از رایانه‌های شخصی و ضرورت استفاده از امکانات شبکه‌ای(اینترنت) وجود قوانین لازم و بستر حقوقی مناسب در این مورد احساس می‌شود؛ بنابراین، با توجه به نیاز مبرم در به‌روزشدن قوانین داخلی و هماهنگی با متخصصان در مواجهه با این جرم، پیشنهادات کاربردی زیر ارائه می‌گردد:

۱. آینده نگری و افزایش مجازات جرایم سایبری به‌ویژه کلاهبرداری سایبری در قوانین؛
۲. آموزش نیروها و کادر قضایی متخصص در زمینه پی‌جویی و تحقیقات کشف جرم کلاهبرداری سایبری؛
۳. تدوین قوانین و مقررات سخت مربوط به امنیت اطلاعات برای صاحبان اطلاعات قابل طبقه‌بندی و مهم؛
۴. گسترش فرهنگ همکاری و تعاون با پلیس در زمینه کشف، شناسایی و تعقیب جرایم سایبری؛
۵. تهیه، تأمین و به‌روزرسانی تجهیزات تخصصی و عمومی موردنیاز در رابطه با پی‌جویی جرایم سایبری؛
۶. ارتقای سطح علمی در دانشکده‌های علوم‌انتظامی از طریق تدریس واحدهای درسی موردنیاز با موضوع جرایم سایبری و اینترنتی؛

۷. همکاری با مجامع علمی و دانشگاهی دنیا و تبادل افکار، تجربیات و اطلاعات در زمینه موردبحث؛
۸. همکاری و تعامل با کارشناسان حقوقی به‌منظور آشنایی کارآگاهان و افسران تحقیق با مبانی حقوقی جرم کلاهبرداری سایبری؛
۹. ارائه آموزش‌های کافی برای استفاده‌کنندگان از این فناوری به‌صورت حضوری و غیرحضوری به‌شکل انتشار کتاب و نشریات و ارتقای سطح امنیت رایانه و آشنایی با خطرات و شیوه‌های نفوذ مجرمان به سامانه‌های رایانه؛
۱۰. تدوین سیاست کیفری خاص جرایم تجارت الکترونیکی تدوین؛
۱۱. تدوین آیین دادرسی ویژه محیط‌های سایبری؛
۱۲. تشکیل گروه واکنش سریع سایبری با تمام شرایط و امکانات لازم؛
۱۳. ترویج راهکارهای پیشگیری فنی و امنیت شبکه؛
۱۴. توسعه امنیت فناوری اطلاعات با آموزش و آگاه‌سازی عمومی؛
۱۵. توسعه امنیت فناوری اطلاعات در سطح سازمان‌ها، شرکت‌ها و موسسات.

فهرست منابع

منابع فارسی

- انصاری، ولی اله(۱۳۹۱)، کشف علمی جرائم، تهران، سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها
- رضوی، محمد(۱۳۸۶)، "جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها"، فصلنامه دانش انتظامی، سال نهم، شماره ۱، صص۱۴۰ ـ ۱۲۰
- زندی، محمدرضا(۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل
- سلیمی، صادق؛ بخشی‌زاده اهری، امین(۱۳۹۳)، تحلیل ماده به ماده قانون آیین دادرسی کیفری ۱۳۹۲ در مقایسه با قوانین سابق، تهران، انتشارات جاودانه جنگل
- صبح خیز، رضا(۱۳۹۴)، "بررسی تطبیقی جرایم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران"، پایان‌نامه برای دریافت درجه کارشناسی‌ارشد حقوق بین‌الملل، دانشگاه آزاد اسلامی، واحد مراغه
- کمالی زاده، سلمان؛ شاه محمدی، غلامرضا(۱۳۹۵)، "ارزیابی روش‌های شناسایی وب‌سایت فیشینگ"، فصلنامه پژوهش‌های اطلاعاتی و جنایی، سال یازدهم، شماره ۱، صص ۴۶ ـ ۳۲
- مارسلا، آلبرت جی؛ مننـدز، داگلاس (۱۳۹۲)، سایبر فارنزیک، ترجمه امیر توکلی، تهران، انتشارات حدیث کوثر
- مقیمی، مهدی(۱۳۹۵)، "جرایم سایبری در اسناد بین‌الملل"، پایان‌نامه برای دریافت درجه دکتری، تهران، دانشگاه شهید بهشتی، دانشکده حقوق
- نتزگر، مایکل؛ موراسی، جرمی(۱۳۹۴)، تحقیقات در جرایم با فناوری پیشرفته، ترجمه مهدی جاوید، تهران، دانشگاه علوم انتظامی امین، معاونت پژوهش و فناوری
- نظری منظم، مهدی(۱۳۹۹)، "الگوی جرم‌یابی کلاهبرداری در فضای سایبر"، پایان‌نامه برای دریافت درجه دکتری، تهران، دانشگاه علوم انتظامی امین، دانشکده فرماندهی و ستاد
- هادیانفر، کمال(۱۳۹۴)، "جرم فیشینگ"، قابل‌دسترسی در:
www. cyberpolice. ir/news/ ۷۵۸۲۱