



H.M.AZIMI 0933870152

۱

**Anti-Money Laundering
and Countering Financing of
Terrorism
Laws and Regulations**



H.M.AZIMI 0933870152



**کارگاه آموزشی
قوانین و مقررات مبارزه با
پولشویی و تامین مالی تروریسم**

**سطح تخصصی:
تحلیل و شناسایی موارد مشکوک به پولشویی**

ارائه شده توسط:

حمید محمدعظیمی

شماره: ۰۴/۶۵۰/۱/۱۱۷

تاریخ: ۱۴۰۴/۰۱/۳۱

پیوست: دارد



معاون وزیر رئیس مرکز اطلاعات مالی
و سرورای عالی مقابله و پیشگیری
از جرائم پولشویی و تأمین مالی تروریسم

باسمه تعالی

آنی
بسیار مهم

از: مرکز اطلاعات مالی

به: کلیه اشخاص مشمول موضوع مواد (۵) و (۶) قانون مبارزه با پولشویی

موضوع: دستورالعمل حداقل آموزش های لازم در حوزه مبارزه با پولشویی و

تأمین مالی تروریسم توسط اشخاص مشمول و تعیین صلاحیت مدرسان

H.M.AZIMI 0933870152

۳

پیوست ۱: سرفصل‌های آموزشی

الف) دوره‌های عمومی

عنوان	سوالاتی که مخاطب می‌بایست قادر باشد در پایان دوره به آن پاسخ دهد	مدت *
مقدماتی	- تعریف مفهومی و حقوقی پولشویی چیست؟ - چرا مجرمین مرتکب پولشویی می‌شوند؟ - تفاوت پولشویی با سایر جرائم اقتصادی چیست؟ - آثار و تبعات پولشویی از منظر اقتصادی، سیاسی و اجتماعی چیست؟ - فهرست جرائم و تخلفات مرتبط با نظام مبارزه با پولشویی در حوزه مربوطه شامل چه مواردی است و چه مجازات و ضمانت‌های اجرایی بر آن‌ها مترتب است؟ - نقش حمایتی قانون از فعالیت اقتصادی مشروع چیست؟ - پولشویی در کجا (بازارهای هدف و بسترها) شکل می‌گیرد؟ اشخاص مشمول چه کسانی هستند و چه انواعی دارند؟ - ساختار مبارزه با پولشویی کشور، سازوکارها و ابزارهای مربوطه در سطح حاکمیت و اشخاص مشمول چیست؟ - مخاطرات پولشویی در بخش اقتصادی مربوطه (نحوه شکل‌گیری پولشویی و مبارزه با آن) چیست؟ - نقش و جایگاه آن شخص مشمول در شکل‌گیری پولشویی و همچنین پیشگیری و شناسایی آن چیست؟	۲

H.M.AZIMI 0933870152

۲

عنوان	سوالاتی که مخاطب می‌بایست قادر باشد در پایان دوره به آن پاسخ دهد	مدت
(مفاهیم مذکور در دوره مقدماتی) - مراحل تحقق فرایند پولشویی و تأمین مالی تروریسم چیست؟ - رویکرد کلاسیک مبارزه با جرم چه تفاوت‌هایی با رویکرد مبارزه با پولشویی دارد؟ - شباهت‌ها و تفاوت‌های پولشویی و تأمین مالی تروریسم چیست؟ چه جرائم دیگری با رویکرد نوین در مبارزه تحت رصد هستند؟ - اصول مبارزه با پولشویی چه مواردی هستند؟ کدام یک کلیدی تلقی می‌شوند و چرا؟ - هر یک چگونه اجرای می‌شوند و چه نتیجه‌ای (اعم از پیشگیرانه/پسینی) دارند؟ - رویکرد مبتنی بر ریسک (در ارائه خدمت) چیست و در مقابل چه رویکردی قرار دارد؟ - ساختار پروفایل مشتری باید شامل چه ابعادی باشد؟	- منابع اطلاعاتی (رسمی و غیررسمی) حاکمیتی و خصوصی مورد استفاده در مبارزه با پولشویی چه مواردی هستند؟ هر یک از این منابع در چه مواردی قابل استفاده و در چه مواردی قابل استناد است؟ کارکرد منابع اطلاعاتی غیررسمی و اظهارات مشتری چیست؟ در صورت نبود دسترسی به پایگاه‌های اطلاعات حاکمیتی، اجرای وظایف چگونه خواهد بود؟ - مهم‌ترین منبع اطلاعاتی که شامل اطلاعات پایه، اظهارات و رفتار مشتری و نتایج حاصل از شناسایی مشایق نزد شخص مشمول است، چگونه می‌تواند به مبارزه با پولشویی کمک کند و تا چه حد به‌تنهایی کافی است؟ - آیا جذب منابع در واقع منطقی با امر مبارزه با پولشویی دارد؟ جذب حداکثری و مدیریت منابع به چه نحو باید صورت گیرد که از تحت نظارت خارج نشده و کمترین آسیب را به دنبال باشد؟ حفاظت گفتار در تملک با مشتری، شامل چه مهارت‌هایی است؟ - وظیفه اصلی هر یک از پست‌های سازمانی (اعم از میز ارائه خدمت و باجدهای ستادی) در قبال مشتری (خصوصاً در شناسایی مشتری، شناسایی مشایق و برخورد با اشخاص مظنون و گزارش‌دهی) چیست؟ - به چه طریق می‌توان گزارش‌ها را برای مسئول مبارزه با پولشویی یا مرکز اطلاعات مالی ارسال کرد؟ ارسال گزارش چه نیت با مناسبت برای شخص گزارش‌دهنده دارد؟ - اساس‌ترین معیار برای مشکوک بودن و آماردها فتن پولشویی به طور کلی و به صورت خاص در حوزه تخصصی موضوع فعالیت آن شخص مشمول چیست؟ - مهم‌ترین سازمان‌ها و نهادهای بین‌المللی در مبارزه با پولشویی کدامند و چه نقشی دارند؟ ضوابط اخلاسی آن‌ها تا چه سطح الزام‌آور است؟ - نقش کلی فناوری‌های نوین در ارتقاء پولشویی و مبارزه با آن چیست؟	۶

• مقادیر اعلامی در ستون «مدت» برحسب ساعت می‌باشد.

H.M.A7IMI10933870152

۵

ب) دوره‌های تخصصی **

عنوان	سوالاتی که مخاطب می‌بایست قادر باشد در پایان دوره به آن پاسخ دهد	مدت
تحلیل و شناسایی موارد مشکوک ***	• (مفاهیم مذکور در دوره مقدماتی و پایه) • چه نیازی به تعریف جرم پولشویی به عنوان جرم مستقل وجود دارد؟ • انواع مستندات و مدارک مستبرشناسایی مشتری کدامند؟ پایگاه‌های رسمی مرتبط با هر یک چیست؟ مهم‌ترین نکاتی که در امتحان‌سنجی و جلوگیری از مدارک جعلی باید رعایت کرد چیست؟ • انواع گزارش‌های مورد نیاز مرکز (<i>STR, SAR, ITR</i> معنون و ...) چیست و واحدهای مختلف سازمانی (از جمله واحد دب پولشویی) چه نقشی در هر یک دارند؟ • شاخص‌های مداخلات و عملیات مشکوک در بخش اقتصادی مربوطه شامل چه مواردی است؟ • ردیابی و تحلیل اطلاعات مالی شامل چه مراحل است و هر یک چگونه و با چه ابزارهایی قابل انجام است؟ • انواع رویکردها در تحلیل داده‌ها و شناسایی سیستمی تخلفات (تحلیل فرضیه‌محور و تحلیل اکتشافی) چیست؟ • هوش مصنوعی و انواع الگوریتم‌های یادگیری ماشین (یا مری و بدون مری) چه کمکی به مبارزه با پولشویی می‌کنند؟ مهم‌ترین و کلرآمدترین الگوریتم‌ها در این زمینه کدام‌ها هستند و هر یک چگونه عمل می‌کنند؟ • ربات‌ها چه کمکی به مبارزه با پولشویی می‌کنند؟ پرکاربردترین سامانه‌ها، پلتفرم‌ها و نیز ابزارهای متن‌باز (<i>OPEN-SOURCE</i>) در مبارزه با پولشویی شامل چه مواردی هستند؟ • تفاوت جرم تخلف چیست؟ جرم منشأ در قوانین داخلی چگونه تعریف شده است؟ • صورت‌های مالی شامل • صورت‌های مالی و اظهارنامه مالیاتی، چه اطلاعات مفیدی را در زمینه مبارزه با پولشویی بدست می‌دهد؟ • گردش کار پرونده، حفاظت گفتار و حفظ محرمانگی هویت گزارش دهنده چگونه می‌بایست انجام شود؟	۴

متن	سوالاتی که مخاطب می‌بایست قادر باشد در پایان دوره به آن پاسخ دهد	توان
۴	• مفاهیم مذکور در دوره مقدماتی و پایه) • چه نیازی به تعریف جرم پولشویی به عنوان جرم مستقل وجود دارد؟ • عناصر تشکیل دهنده جرم پولشویی (و جرم مرتبط) و مجازات‌های آن چیست؟ • تفاوت جرم بزه و تخلف چیست؟ جرم منشأ در قوانین داخلی چگونه تعریف شده است؟ جرم سازمان یافته چگونه تعریف می‌شود؟ • شرایط قانونی استناد، توقیف، معادله اموال و دارایی‌ها چیست؟ • انواع مستندات و مدارک معتبرشناسایی مشتری کدامند؟ پایگاه‌های رسمی مرتبط با هر یک چیست؟ مهم‌ترین نکاتی که در اصلالت‌سنجی و جلوگیری از مدارک جعلی باید رعایت کرد چیست؟ • ملاحظات احراز هویت الکترونیکی و امنیتی دیجیتال چیست؟ • مقررات مبارزه با پولشویی و تأمین مالی تروریسم در کشور کدامند؟ • تطبیق قوانین سازمانی با اصول مبارزه با پولشویی چه ابزاری را در بر می‌گیرد و مدیریت ریسک محصولات/خدمات/کانال‌های ارائه خدمت، چگونه و در چه مرحله‌ای می‌بایست انجام شود؟ چه انواع اقداماتی برای مدیریت ریسک لازم است؟ • انواع روش‌های ارزیابی ریسک مشتری (حین ارائه هر خدمت یا دوره‌ای) چیست؟ هر یک چه نقاط قوت و ضعفی دارد و مناسب چه شرایط است؟ • انواع اشخاص (حقیقی/حقوقی) و همچنین از نظر قانونی چه نوعی دارند؟ اشخاص حقوقی از نظر نوع مسئولیت حقوقی مؤسسان و مالکان چه انواعی دارند؟ • شواهد نگهداری سوابق و اطلاعات چیست؟ (شیوه صحیح) • ساختار و تکالیف واحد، انواع مسئول مربوط پولشویی در ادبیات جهانی و ... چیست؟ • شواهد و حدود محرمانگی اطلاعات و حفاظت داده چیست؟ • چه استانداردهایی باید در نظارت و بازرسی رعایت شود؟ انواع روش‌های ممیزی و بازرسی چیست؟ انواع ابزارهای نظارتی و تدابیر کنترلی (تشویقی و تنبیهی) چیست؟ رویکرد ریسک‌محور در نظارت بر عملکرد با چه معیارهایی قابل انجام است؟	تفاوت و تطبیق با مقررات

*** در صورت عدم تفکیک پرسنل مبارزه با پولشویی به دو حوزه مذکور، باید همگی کارکنان، مفاهیم اشاره شده در هر دو دوره تخصصی را آموزش ببینند. این حکم درخصوص مسئول مبارزه با پولشویی نیز صادق است.

*** حتی‌المقدور می‌بایست کارکنان حوزه «تحلیل و شناسایی موارد مشکوک» آموزش‌های لازم برای استفاده از سامانه‌های کشف تقلب و ابزارهای مشابه را گذارنده باشند.

پیوست ۲: سطح آموزش مورد نیاز در هر واحد سازمانی (برای گروه‌های مختلف اشخاص مشمول)						
نوع	شخص مشمول	دستگاه متولی نظارت	گروه ریسک	سطح آموزش مورد نیاز		
				مدیران عالی	واحد م.ب. پولشویی	میز خدمت
موسسه مالی	بانک‌ها و مؤسسات اعتباری غیربانکی	بانک مرکزی ج.ا.ا.	۱	مقدمانی	تخصصی	پایه
	صرافی‌ها	بانک مرکزی ج.ا.ا.	۲	مقدمانی	-	پایه
	صندوق‌های قرض الحسنه (بزرگ)	بانک مرکزی ج.ا.ا.	۱	مقدمانی	تخصصی	پایه
	صندوق‌های قرض الحسنه (کوچک)	بانک مرکزی ج.ا.ا.	۳	مقدمانی	-	پایه
	شرکت‌های لیزینگ	بانک مرکزی ج.ا.ا.	۲	مقدمانی	-	پایه
	پرداختیاران	بانک مرکزی ج.ا.ا.	۲	مقدمانی	-	پایه
	شرکت‌های ارائه دهنده خدمات پرداخت	بانک مرکزی ج.ا.ا.	۱	مقدمانی	تخصصی	پایه
	شرکت‌های مدیریت دارایی مؤسسات اعتباری	بانک مرکزی ج.ا.ا.	۳	مقدمانی	-	
	تعاونی‌های اعتبار	بانک مرکزی ج.ا.ا.	۳	مقدمانی	-	
	شرکت‌های بیمه	بیمه مرکزی ج.ا.ا.	۱	مقدمانی	تخصصی	پایه
	کارگزاران بازار سرمایه	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی	پایه
	بازارگردان	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	مؤسسات رتبه‌بندی	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	مشاوره سرمایه‌گذاری	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	صندوق سرمایه‌گذاری	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	صندوق بازتشتگی	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	شرکت‌های سرمایه‌گذاری	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	شرکت‌های پردازش اطلاعات مالی	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	شرکت‌های تأمین سرمایه	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	
	سبدگردان	سازمان بورس و اوراق بهادار	۳	مقدمانی	-	

نوع	شخص مشمول	دستگاه متولی نظارت	گروه ریسک	سطح آموزش مورد نیاز	
				مدیران عالی	واحد م.ب. پولشویی
مشاغل غیرمالی	فروشندهگان خودرو	اتحادیه‌های صنفی ذریبط	۳	مقدمانی	-
	سرمایه‌گذاران و انبوه‌سازان مسکن و ساختمان	اتحادیه‌های صنفی ذریبط	۳	مقدمانی	-
	مشاورین املاک	اتحادیه‌های صنفی ذریبط	۳	مقدمانی	-
	فروشندهگان طلا، نقره و مسکوکات	اتحادیه‌های صنفی ذریبط	۳	پایه	-
	فروشندهگان فلزات گرانبها و سنگ‌های قیمتی	اتحادیه‌های صنفی ذریبط	۳	پایه	-
	فروشندهگان فرش دستباف نفیس	اتحادیه‌های صنفی ذریبط	۳	مقدمانی	-
	فروشندهگان عتیقه، آثار هنری و صنایع دستی فاخر	اتحادیه‌های صنفی ذریبط	۳	مقدمانی	-
	حسابرسان	جامعه حسابداران رسمی	۳	پایه	-
	دفترداران	سازمان ثبت اسناد و املاک کشور	۳	پایه	-
	وکلا	کانون و مرکز وکلا	۳	مقدمانی	-
سازمان غیرانتفاعی	بمن‌ها و موسسات خیریه	وزارت کشور	۳	پایه	-
دارایی مجازی	ارائه‌دهندگان خدمات دارایی مجازی	بانک مرکزی ج.ا.ا.	۲	مقدمانی	-
مراکز مبادله، تسویه و پردازش معاملات	شرکت بورس اوراق بهادار تهران	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی
	شرکت فرابورس ایران	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی
	شرکت بورس کالا	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی
	شرکت بورس انرژی	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی
	سپرده‌گذاری مرکزی اوراق بهادار و تسویه وجوه	سازمان بورس و اوراق بهادار	۱	مقدمانی	تخصصی
	شرکت شبکه الکترونیک پرداخت کارتی	بانک مرکزی ج.ا.ا.	۱	مقدمانی	تخصصی

- منظور از صندوق قرض‌الحسنه بزرگ، صندوق‌های دارای حداقل ۵۰۰۰۰۰۰ مشتری هستند. مرجع تشخیص تعداد مشتری، دستگاه متولی نظارت مربوطه است.
- به هر ترتیب در صورت تشکیل واحد مبارزه با پولشویی، کارکنان و مسئول این واحد می‌بایست سطح آموزش تخصصی مرتبط را بگذرانند.

عناوین سرفصل‌های آموزشی دوره تخصصی تحلیل و شناسایی موارد مشکوک به پولشویی

- فصل ۱: مبانی تحلیلی جرم پولشویی
- فصل ۲: شناسایی و احراز هویت مشتری (KYC)
- فصل ۳: گزارش‌دهی و نقش واحدهای سازمانی
- فصل ۴: شاخص‌ها و الگوهای شناسایی معاملات مشکوک
- فصل ۵: ردیابی و تحلیل اطلاعات مالی
- فصل ۶: رویکردهای تحلیلی در کشف تخلفات
- فصل ۷: فناوری‌های نوین در تحلیل و شناسایی موارد مشکوک
- فصل ۸: تحلیل صورت‌های مالی در کشف نشانه‌های پولشویی
- فصل ۹: مدیریت پرونده و محرمانگی اطلاعات

فصل ۱: مبانی تحلیلی جرم پولشویی

چه نیازی به تعریف جرم پولشویی به عنوان جرم مستقل وجود دارد؟

۱. ضرورت تعریف جرم پولشویی به عنوان جرم مستقل
۲. تمایز مفهومی میان جرم، تخلف و تخطی اداری در نظام‌های حقوقی
۳. بررسی جایگاه جرم منشأ در قوانین داخلی و بین‌المللی

پولشویی در ساده‌ترین شکل خود، فرآیندی است که طی آن منشأ و مالکیت سود حاصل از فعالیت‌های مجرمانه پنهان می‌شود.

در واقع، پول با روش‌های مشروع «پاکسازی» یا «شستشو» می‌شود و در نتیجه، درآمد حاصل، هویت مجرمانه خود را از دست می‌دهد و به نظر می‌رسد که از یک منبع مشروع آمده است.

واژه پولشویی فرآیندی را ترسیم می‌نماید که در خلال آن، **پول کثیف** و در واقع پول حاصل از **عمل یا اعمال مجرمانه** در چرخه‌ای از **فعالیت‌ها و معاملات مالی** **تطهیر شده** به گونه‌ای که به پول به ظاهر **قانونی و مشروع** و بدون هیچ اثری از جرم منشأ تبدیل می‌شود.

تعریف و جایگاه «جرم منشأ»

مستند قانونی:

بند (الف) ماده ۱ قانون مبارزه با پولشویی:

جرم منشأ، هر رفتاری است که مطابق ماده (۲) قانون مجازات اسلامی جرم محسوب شود

✳ پولشویی چگونه انجام می شود؟

✓ فرایند پولشویی در سه مرحله انجام می شود:

۱. **جای گذاری (Placement)** : در این مرحله، پول های غیرقانونی وارد سیستم مالی می شود. مثلاً با واریز پول نقد

به حساب بانکی یا خرید دارایی های گران قیمت مثل طلا یا خودرو.

۲. **لایه گذاری (Layering)** : در مرحله دوم، هدف پنهان کردن منبع اصلی پول است. پول از حسابی به حساب دیگر

منتقل می شود، گاهی بین چند کشور، یا از طریق خرید و فروش های پیچیده.

۳. **یکپارچه سازی (Integration)** : در نهایت، پول به شکل "قانونی" وارد اقتصاد می شود. مثلاً با سرمایه گذاری در

کسب و کارها، خرید ملک، یا انجام معاملات تجاری.

تحلیل:

- ✓ هر جرم اقتصادی، مالی یا سازمان یافته می تواند جرم منشأ پولشویی باشد.
- ✓ حتی جرایم واقع شده در خارج از کشور در صورت تطبیق با قوانین ایران، جرم منشأ محسوب می شوند (تبصره ۱ ماده ۳ قانون).
- ✓ جرایم قاچاق کالا و ارز نیز به طور خاص در زمره جرائم منشأ آمده اند.

مثال های کاربردی:

- ✓ قاچاق گسترده ارز و تبدیل وجوه حاصل به املاک و سهام.
- ✓ دریافت رشوه و انتقال وجوه به حساب اشخاص ثالث.
- ✓ درآمدهای ناشی از فرار مالیاتی که به حساب شرکت های صوری واریز می شود.

تفاوت میان «جرم» و «تخلف»

ویژگی	تخلف	جرم
مبنای حقوقی	مقررات اداری، صنفی یا انضباطی	قانون مجازات اسلامی و قوانین کیفری خاص (مثل قانون مبارزه با پولشویی)
مرجع رسیدگی	هیئت‌های رسیدگی به تخلفات یا مراجع اداری	دادگاه کیفری
نتیجه	تنبیه اداری (اخطار، تعلیق، انفصال از خدمت)	مجازات (حبس، جزای نقدی، مصادره)
مثال	قصور در ارسال گزارش STR توسط کارمند بانک	انجام عملیات مشکوک با علم به منبع غیرقانونی (ماده ۲)

همکار بر اساس تبصره ماده ۷ قانون مبارزه با پولشویی، مدیران یا کارکنانی که به قصد تسهیل جرایم از انجام تکالیف قانونی خودداری کنند، مرتکب جرم می‌شوند و در صورت تقصیر (نه عمد)، مشمول تخلف اداری هستند.

ساختار ملی مقابله با پولشویی

"شورای عالی مقابله و پیشگیری از جرائم پولشویی و تأمین مالی تروریسم" تشکیل می‌شود که ریاست آن با وزیر امور اقتصادی و دارایی است و وظایف زیر را بر عهده دارد:

۱. تعیین راهبردها و سیاست‌های ملی AML/CFT

۲. هماهنگی میان نهادهای ذی‌ربط (بانک مرکزی، وزارت اطلاعات، قوه قضاییه و...)

۳. تصویب آیین‌نامه‌های اجرایی و دستورالعمل‌های تخصصی.

دبیرخانه شورا در وزارت امور اقتصادی و دارایی مستقر است و

مرکز اطلاعات مالی (FIU) به عنوان بازوی اجرایی و تحلیلی شورا عمل می‌کند (ماده ۷ مکرر قانون).

نقش مرکز اطلاعات مالی (FIU) در تحلیل جرم پولشویی

بر اساس ماده ۷ مکرر قانون مبارزه با پولشویی:

✓ مرکز اطلاعات مالی مسئول دریافت، جمع‌آوری، تجزیه و تحلیل و ارزیابی اطلاعات مربوط به معاملات مشکوک است.

✓ این مرکز می‌تواند در صورت ظن قوی به وقوع جرم، توقیف موقت وجوه یا اموال مشکوک تا ۲۴ ساعت را دستور دهد (تبصره ۱ ماده ۷ مکرر).

✓ مرکز موظف است با دستگاه‌های امنیتی، قضایی، بانکی و مالیاتی تبادل اطلاعات داشته باشد.

فصل ۲: شناسایی و احراز هویت مشتری (KYC)

انواع مستندات و مدارک معتبر شناسایی مشتری کدامند؟

۱. انواع مستندات و مدارک معتبر برای شناسایی اشخاص حقیقی و حقوقی
۲. پایگاه‌های رسمی و مراجع اعتبارسنجی مرتبط با هر نوع مدرک (ثبت احوال، ثبت شرکت‌ها، سازمان امور مالیاتی و ...)
۳. نکات کلیدی در اصالت‌سنجی مدارک و پیشگیری از استفاده از اسناد جعلی

مستند قانونی

ماده ۷ قانون مبارزه با پولشویی (اصلاحی ۱۳۹۷) اشخاص مشمول را مکلف می‌کند به:

«احراز هویت و شناسایی مراجعان، مالکان واقعی و در صورت اقدام توسط نماینده یا وکیل، احراز سمت و هویت نماینده، وکیل و اصیل».

همچنین، طبق بند (ت) همین ماده، «اشخاص مشمول باید سوابق شناسایی ارباب رجوع، مالک و سوابق حساب‌ها و معاملات را حداقل پنج سال پس از پایان رابطه کاری نگهداری کنند».

تحلیل:

این ماده، KYC را به عنوان اولین خط دفاعی در برابر پولشویی و تأمین مالی تروریسم معرفی می‌کند. بدون اجرای دقیق این مرحله، تشخیص معاملات مشکوک در مراحل بعدی (مثل STR یا TTR) ممکن نیست.

H.M.AZIMI 0933870152

KYC PROCEDURES



تعریف و سطوح شناسایی (مطابق فصل پنجم آیین نامه اجرایی)

شناسایی فرایندی است شامل دریافت و بررسی اطلاعات ارباب رجوع.

برای احراز هویت و ارزیابی خطر (ریسک) AML/CFT سه سطح شناسایی وجود دارد:

نوع شناسایی	نمونه کاربرد	توضیح
ساده ●	سپرده گذاری خرد، خدمات معمول بانکی	برای مشتریان کم ریسک و معاملات با مبالغ محدود
معمول ●	افتتاح حساب های جاری، اعتباری یا ارزی	برای اکثر مشتریان با سطح ریسک متوسط
مضاعف ● (Enhanced Due Diligence)	شرکت های خارجی، مقامات سیاسی (PEPs)	برای مشتریان پرریسک (سیاسی، غیربومی، خارجی، پرمعامله)

در صورت وجود نشانه های خطر بالا مانند اقامت در مناطق پرخطر، حجم زیاد تراکنش ها یا ارتباط با اشخاص مظنون، باید شناسایی مضاعف انجام شود.

فصل پنجم - شناسایی ارباب رجوع (ماده ۵۰ - تبصره یک)

✓ ارائه خدمات به ارباب رجوع  به منزله تضمین انجام دادن رویه‌های شناسایی مقتضی ارباب رجوع توسط کارکنان اشخاص مشمول است؛

✓ مسئولیت وجود هر گونه تخطی در این زمینه بر عهده اشخاص مشمول و کارکنان ذی ربط است.

✓ اشخاص مشمول مکلفاند که از دادن خدمت به اشخاص بدون هویت قانونی یا اشخاصی که شناسه یکتای هویتی آنها به دلایلی (اعم از فوت و ...) توسط مراجع ذی ربط ابطال شده است، خودداری کنند.

🔍 فرآیند اجرایی KYC در اشخاص مشمول

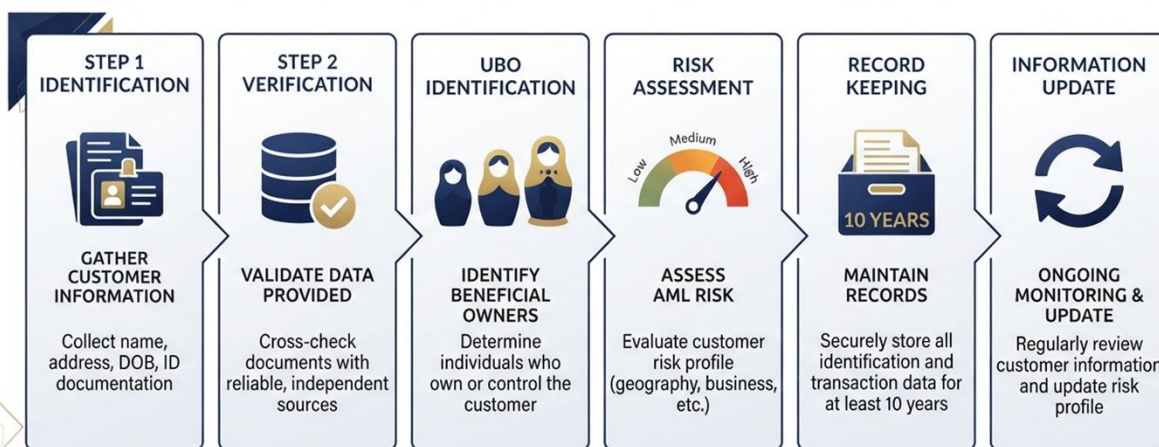
- گام ۱: شناسایی: دریافت اطلاعات شناسایی (نام، کد ملی، آدرس، شماره تماس، شغل، منبع درآمد و ...).
- گام ۲: احراز اصالت: تطبیق مدارک ارائه شده با پایگاه های رسمی ثبت احوال یا ثبت شرکت ها.
- گام ۳: شناسایی مالک واقعی: شناسایی شخصی که در نهایت مالک یا کنترل کننده واقعی دارایی است (UBO)
- گام ۴: ارزیابی خطر (Risk Assessment)

ارزیابی سطح ریسک مشتری بر اساس معیارهای ذیل:

- ✓ ماهیت فعالیت
- ✓ محل اقامت یا ثبت
- ✓ نوع خدمات درخواستی
- ✓ سابقه تعاملات مالی

- گام ۵: ثبت و نگهداری سوابق: نگهداری اطلاعات به صورت الکترونیکی یا فیزیکی حداقل ۱۰ سال پس از قطع رابطه
- گام ۶: به روزرسانی اطلاعات مشتری: در صورت تغییر آدرس، سمت، یا ساختار مالکیت، شناسایی باید به روزرسانی شود

KNOW YOUR CUSTOMER (KYC) PROCESS FLOW



H.M.AZIMI 0933870152

AML TRAINING MODULE

12

شناسایی ارباب رجوع

✓ ماده ۵۰ آیین نامه اجرایی: ارائه هرگونه خدمات و برقراری هرگونه تعامل کاری قبل از انجام شناسایی ممنوع است.

ماده ۵۲ آیین نامه اجرایی: حداقل اطلاعات مورد نیاز در شناسایی به شرح ذیل:

- ❖ نوع شخص (حقیقی یا حقوقی)،
- ❖ تابعیت،
- ❖ منطقه جغرافیایی محل سکونت و اقامت،
- ❖ مبدأ و مقصد مورد انتظار تراکنش ها و عملیات،
- ❖ شغل و نوع فعالیت،
- ❖ میزان درآمد و منابع اموال،
- ❖ خدمات مورد تقاضا یا رایحه شده،
- ❖ هدف افتتاح حساب یا ایجاد تعامل کاری،
- ❖ استفاده مستقیم یا با واسطه

اطلاعات مورد نیاز به منظور شناسایی مشتری و نگهداری در پروفایل مشتری

✓ هویتی

✓ اقتصادی

✓ مالک واقعی (ذینفع نهایی)

پایگاه‌های رسمی استعلام مدارک و اطلاعات

نوع اطلاعات	نهاد متولی	پایگاه رسمی مرتبط
اطلاعات هویتی اشخاص حقیقی	وزارت کشور	سازمان ثبت احوال کشور
اطلاعات اشخاص حقوقی	سازمان ثبت اسناد و املاک کشور	سامانه شناسه ملی اشخاص حقوقی
شماره اقتصادی و اظهارنامه مالیاتی	وزارت امور اقتصادی و دارایی	سازمان امور مالیاتی
مجوز فعالیت و صنفی	وزارت صمت	سامانه جامع اصناف ایران
وضعیت بیمه‌ای و اشتغال	وزارت کار	سامانه سازمان تأمین اجتماعی
استعلام سوابق مالی و بانکی	بانک مرکزی	بانک مرکزی جمهوری اسلامی ایران
اطلاعات افراد مظنون و تحریمی	وزارت امور اقتصادی و دارایی	سامانه مرکز اطلاعات مالی (FIU)

اصالت سنجی مدارک و جلوگیری از جعل

اشخاص مشمول باید:

۱. مدارک هویتی را از طریق سامانه‌های رسمی (برخط یا فیزیکی) راستی‌آزمایی کنند.
۲. از پذیرش تصویر یا کپی غیرمعتبر بدون تطبیق اصل خودداری نمایند.
۳. در صورت وجود مغایرت، مشتری را در فهرست مغایرت‌ها ثبت و موضوع را به FIU اعلام کنند.
۴. هنگام کشف جعل یا گزارش خلاف واقع، گزارش STR ارسال کنند.

ابلاغ مدارک شناسایی معتبر اشخاص حقیقی و حقوقی ایرانی برای احراز هویت

شماره: ۰۳/۴۵/۰۱/۶۸۰	 (جهت تولید با شرکت مردم)	معاون وزیر و رئیس مرکز اطلاعات مالی
تاریخ: ۱۴۰۳/۱۲/۱۹		دبیر شورای عالی مقابله و پیشگیری
پیوست: ندارد		از جراثیم پولشویی و تامین مالی تروریسم
باسمه تعالی		
انی - حائز اهمیت	از: مرکز اطلاعات مالی به: تمامی اشخاص مشمول موضوع مواد (۵) و (۶) قانون مبارزه با پولشویی موضوع: ابلاغ مدارک شناسایی معتبر اشخاص حقیقی و حقوقی ایرانی	

H.M.AZIMI 0933870152

30

ردیف	خوشه	گروه	مدارک شناسایی معتبر
۱	حقیقی	—	— کارت ملی هوشمند برای افراد بالای ۱۵ سال (در صورت نبود کارت ملی هوشمند، شناسنامه به همراه رسید درخواست کارت ملی مدرک معتبر شناخته می‌شود) — شناسنامه برای افراد تا ۱۵ سال
۲	شرکت‌های تجاری و مؤسسات غیرتجاری	—	— آخرین تغییرات روزنامه رسمی — اساسنامه یا شرکت‌نامه حسب مورد
۳	دستگاه‌های اجرایی	شرکت‌های دولتی	— آخرین تغییرات روزنامه رسمی — اساسنامه یا شرکت‌نامه حسب مورد
		وزارتخانه‌ها و مؤسسات دولتی	— دلیل سمت (احکام مبین سمت، تفویض و نمایندگی)
		مؤسسات و نهادهای عمومی غیردولتی (از جمله نظام‌های حرفه‌ای)	— مجوز تأسیس یا اساسنامه — حسب مورد آخرین تغییرات روزنامه رسمی — دلیل سمت (احکام مبین سمت، تفویض و نمایندگی)
۴	موقوفات و نهادهای مذهبی	موقوفات	— سند وقف یا وقف‌نامه — سند ثبتی ملک (عین موقوفه) — دلیل سمت (احکام متولی یا مبین سمت)
		اماکن و نهادهای مذهبی	— پروانه فعالیت یا مجوز تأسیس یا اساسنامه یا سند ثبتی ملک مورد بهره‌برداری — دلیل سمت (احکام مبین سمت، تفویض و نمایندگی)
۵	مدارس و هیئت‌های ورزشی	—	— مجوز تأسیس در صورت لزوم — دلیل سمت (احکام مبین سمت، تفویض و نمایندگی)

فصل ۳: گزارش‌دهی و نقش واحدهای سازمانی

۱. آشنایی با انواع گزارش‌های مورد نیاز مرکز اطلاعات مالی:

✓ گزارش معاملات مشکوک (STR)

✓ گزارش معاملات بیش از حد آستانه (TTR)

✓ گزارش فعالیت‌های مظنون (SAR)

۲. نقش و مسئولیت واحدهای مختلف سازمانی در فرایند گزارش‌دهی، به‌ویژه واحد مبارزه با پولشویی

❖ مبانی قانونی گزارش دهی

📄 مستندات قانونی:

✓ ماده ۷ بند «پ» قانون مبارزه با پولشویی :

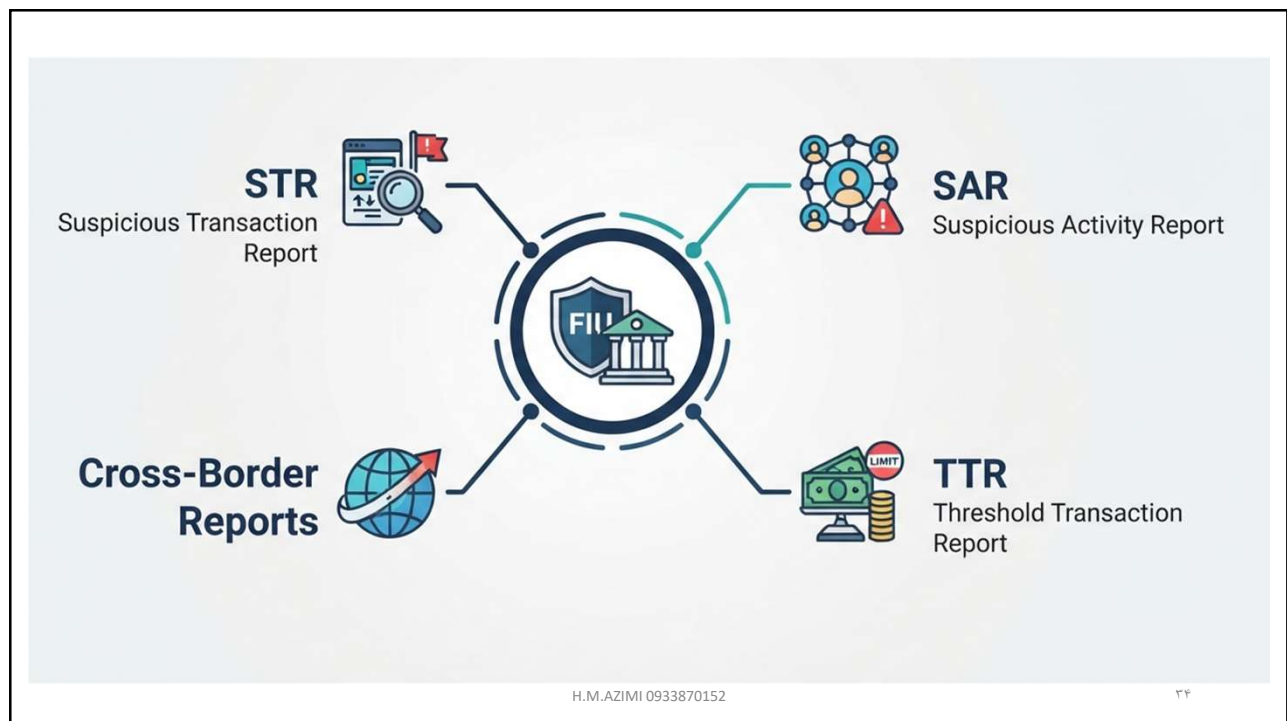
اشخاص مشمول موظفند گزارش معاملات یا عملیات بیش از میزان مصوب شورا یا معاملات و عملیات مشکوک بانکی، ثبتی، سرمایه گذاری، صرافی، کارگزاری و مانند آن را به مرکز اطلاعات مالی ارائه کنند.

✓ ماده ۷ مکرر قانون:

مرکز اطلاعات مالی موظف است اطلاعات و گزارش های دریافتی را تجزیه و تحلیل کرده و در صورت ظن قوی به وقوع جرم، پرونده را به مرجع قضایی ارسال نماید.

✓ فصل دهم آیین نامه اجرایی ماده (۱۴) الحاقی قانون مبارزه با پولشویی:

این فصل جزئیات مربوط به فرآیند گزارش دهی، مسئولیت ها و محرمانگی اطلاعات را تشریح می کند.



⚙️ انواع گزارش‌های مورد نیاز در نظام مبارزه با پولشویی

نوع گزارش	هدف	عنوان انگلیسی	مرجع دریافت‌کننده
گزارش معاملات مشکوک	شناسایی و گزارش فعالیت‌هایی که ظن وقوع جرم ایجاد می‌کنند	STR – Suspicious Transaction Report	مرکز اطلاعات مالی (FIU)
گزارش تراکنش بیش از حد آستانه	ثبت و پایش تراکنش‌های بالاتر از سقف مصوب	TTR – Threshold Transaction Report	FIU از طریق واحد مبارزه با پولشویی
گزارش فعالیت مظنون	گزارش رفتارها و الگوهای غیرعادی مشتری قبل از انجام معامله	SAR – Suspicious Activity Report	FIU
گزارش معاملات ارزی و نقدی سنگین	کنترل جریان نقدی و ارزی قابل ردیابی	CTR / LCTR	FIU و بانک مرکزی
گزارش تراکنش‌های بین‌المللی پرریسک	کنترل نقل و انتقال برون مرزی و جلوگیری از CFT	ITR – International Transaction Report	FIU و وزارت اطلاعات

نوع گزارش	عنوان انگلیسی
گزارش تراکنش‌های مشکوک؛ زمانی که یک تراکنش خاص با الگوی مالی مشتری همخوانی ندارد	STR (Suspicious Transaction Report)
گزارش فعالیت مشکوک؛ فراتر از یک تراکنش، به کل رفتار و تعاملات مشتری که ابهام‌برانگیز است اشاره دارد.	SAR (Suspicious Activity Report)
گزارش تراکنش‌های آستانه‌ای؛ گزارش خودکار مبالغ نقدی که از سقف قانونی (مثلاً ۱۵ میلیون تومان یا معادل آن) فراتر می‌روند.	TTR/CTR (Threshold Transaction Report)
به عنوان زیربنای تمام گزارش‌ها؛ تا مشتری را شناسید، نمی‌توانید رفتار او را "مشکوک" تشخیص دهید.	KYC/CDD (Know Your Customer)
شناسایی ذینفع نهایی؛ برای جلوگیری از پنهان شدن پشت شرکت‌های صوری.	UBO (Ultimate Beneficial Owner)
بررسی لیست تحریم‌ها و افراد سیاسی شناخته شده (PEP).	Sanction Screening

H.M.AZIMI 0933870152

۳۶

✓ **STR** متمرکز بر "پول" و جابه‌جایی آن است، اما **SAR** می‌تواند شامل رفتارهای غیرمالی هم باشد (مثلاً مشتری که از ارائه مدارک شناسایی خودداری می‌کند یا عصبی رفتار می‌کند).

✓ **اهمیت TTR** : این گزارش "عینی" است و نیاز به قضاوت کارمند ندارد؛ به محض عبور از رقم مشخص، سیستم باید گزارش کند. اما "STR/SAR ذهنی" هستند و به مهارت و هوشیاری کارمند بستگی دارند.

✓ **دینفع نهایی (UBO)** : تأکید کنید که در پولشویی‌های مدرن، لایه‌بندی (Layering) از طریق شرکت‌های پیچیده انجام می‌شود و گزارش باید شامل کسی باشد که در نهایت سود را دریافت می‌کند، نه فقط مدیر اسمی شرکت.

Cross-Border Reporting

✓ گزارش‌دهی فرامرزی یا (Cross-Border Reporting) که در ادبیات پولشویی گاهی به عنوان CBTR یا Cross-Border Transaction Report نیز شناخته می‌شود.

✓ به فرآیند پایش، ثبت و گزارش‌دهی هرگونه انتقال وجه، دارایی، یا ابزارهای مالی (مانند حواله‌ها، ارز فیزیکی، چک‌های مسافرتی و اوراق بهادار) از مرزهای جغرافیایی و قانونی یک کشور به کشور دیگر اشاره دارد.

✓ این مفهوم یکی از کلیدی‌ترین بخش‌ها در مرحله لایه‌بندی و ادغام چرخه پولشویی است.

شاخص های تشخیص معاملات و عملیات مشکوک در بخش اقتصادی مربوطه

STR



shutterstock.com • 351803450

شاخص‌های تشخیص معاملات و عملیات مشکوک

مطابق تبصره ماده ۷ قانون مبارزه با پولشویی و بند ۱۲ ماده ۱ آیین‌نامه اجرایی، معاملات مشکوک شامل هر نوع معامله یا انتقال وجهی است که بر اساس قرائن و اوضاع و احوال، ظن وقوع جرم را ایجاد کند.

شاخص‌های اصلی:

۱. مغایرت سطح تراکنش با وضعیت اقتصادی مشتری: مثال: حساب فرد بیکار که گردش چند میلیاردی در ماه دارد.
۲. کشف جعل، اظهار خلاف واقع یا ارائه اطلاعات نادرست: مثال: ارائه اسناد هویتی غیرواقعی یا گواهی‌های جعلی.
۳. معاملات صوری یا با مالک واقعی پنهان: مثال: انتقال دارایی از سوی شخصی به نماینده ظاهری.
۴. تراکنش با مناطق پرخطر یا اشخاص مظنون: مثال: انتقال وجوه به حساب شرکت‌های ثبت‌شده در کشورهایی که در فهرست پرخطر قرار دارند.
۵. فسخ ناگهانی معامله یا انصراف بدون دلیل منطقی: مثال: خرید ملک و سپس لغو قرارداد پیش از ثبت رسمی.

نقش و مسئولیت واحدهای سازمانی

۱. واحدهای عملیاتی (شعب، کارگزاری‌ها، صرافی‌ها و ...)

۲. واحد مبارزه با پولشویی (AML Unit)

۳. مدیر ارشد سازمان یا مقام پاسخگو

نقش و مسئولیت واحدهای سازمانی

۱. واحدهای عملیاتی (شعب، کارگزاری‌ها، صرافی‌ها و ...):

✓ نخستین نقطه تماس با مشتری هستند.

✓ موظف به ثبت دقیق اطلاعات و ارسال گزارش اولیه به «واحد مبارزه با پولشویی» هستند.

✓ در صورت مشاهده هرگونه مغایرت یا ظن، باید گزارش اولیه را حداکثر ظرف ۲۴ ساعت تنظیم کنند.

نقش و مسئولیت واحدهای سازمانی

۲. واحد مبارزه با پولشویی (AML Unit)

مطابق ماده ۳۷ آیین نامه اجرایی، این واحد در هر شخص مشمول ایجاد می شود و:

- ✓ مسئول جمع آوری، بررسی، تحلیل و طبقه بندی گزارش های دریافتی از واحدهای داخلی است.
- ✓ موظف است در صورت تأیید ظن به وقوع جرم، گزارش را در قالب STR یا TTR به FIU ارسال کند.
- ✓ باید محرمانگی هویت گزارش دهندگان داخلی را حفظ کند.
- ✓ گزارش های غیرمستند یا فاقد قرائن کافی را بایگانی ولی مستندسازی می کند.

۳. مدیر ارشد سازمان یا مقام پاسخگو:

- ✓ مسئول نهایی صحت گزارش های ارسالی به مرکز اطلاعات مالی است.
- ✓ در صورت اهمال یا قصور، مسئولیت کیفری یا اداری دارد.

🕒 فرآیند تهیه و ارسال گزارش‌ها

بر اساس فصل دهم آیین‌نامه اجرایی (مواد ۱۳۵ تا ۱۴۱):

گام ۱: شناسایی و ثبت اولیه

گام ۲: بررسی و تحلیل داخلی

گام ۳: تصمیم نهایی

گام ۴: ارسال به FIU

گام ۵: پیگیری و مکاتبات بعدی

🕒 فرآیند تهیه و ارسال گزارش‌ها

گام ۱: شناسایی و ثبت اولیه: کارشناس شعبه یا واحد اجرایی در صورت مشاهده مورد مشکوک، فرم گزارش اولیه را تکمیل می‌کند.

گام ۲: بررسی و تحلیل داخلی: واحد مبارزه با پولشویی گزارش را از نظر قرائن، مبلغ، الگو و منبع مالی بررسی می‌کند.

گام ۳: تصمیم نهایی: در صورت تأیید ظن معقول، گزارش نهایی STR یا TTR تهیه و با امضای مقام مسئول ارسال می‌شود.

گام ۴: ارسال به FIU: ارسال باید از طریق سامانه الکترونیکی یا محرمانه (در شرایط خاص) انجام شود. بر اساس ماده ۱۳۵ آیین‌نامه، تأخیر بیش از ۲۴ ساعت بدون عذر موجه تخلف محسوب می‌شود.

گام ۵: پیگیری و مکاتبات بعدی

FIU پس از تحلیل داده‌ها، ممکن است برای دریافت اطلاعات تکمیلی به واحد AML مراجعه کند. همکاری در ارائه داده‌های جدید الزامی است.

📁 نمونه‌های کاربردی از گزارش‌دهی

- مثال ۱:** کارشناس اعتبارات مشاهده می‌کند که مشتری اقدام به تسویه وام کلان نقدی از طریق چند حساب مختلف می‌کند. واحد *AML* باید گزارش (*STR* معامله مشکوک) تهیه و به *FIU* ارسال کند.
- مثال ۲:** صرافی معامله‌ای ۴۰۰ میلیون تومانی انجام می‌دهد که از سقف *TTR* (مثلاً ۲۵۰ میلیون) بالاتر است. طبق آیین‌نامه، گزارش (*TTR* تراکنش بالاتر از حد آستانه) باید ارسال شود.
- مثال ۳:** کارگزاری بورس متوجه رفتار غیرعادی مشتری در خرید سهام شرکت‌های کوچک می‌شود که هدف آن به‌نظر دست‌کاری قیمت است. گزارش (*رفتار مظنون*) باید به *FIU* ارسال شود.
- مثال ۴:** در یکی از شعب، کارمند متوجه مغایرت بین هویت واقعی مشتری و مدارک ارائه‌شده می‌شود. طبق آیین‌نامه، گزارش *STR* الزام‌است.

فصل ۴: شاخص‌ها و الگوهای شناسایی معاملات مشکوک

۱. شاخص‌ها و الگوهای رفتاری مشکوک در بخش‌های مختلف اقتصادی (بانکی، بیمه، کارگزاری، تولیدی و ...)
۲. تحلیل نمونه‌های واقعی از الگوهای کشف‌شده در حوزه‌های پرریسک

مبانی قانونی و مفهومی شاخص‌های معاملات مشکوک

مستند قانونی

۱. تبصره ماده ۷ قانون مبارزه با پولشویی: معاملات و عملیات مشکوک معاملاتی هستند که بر اساس قرائن و اوضاع و احوال، ظن وقوع جرم را ایجاد می‌کنند. معیارهای شناسایی این موارد به تصویب شورای عالی می‌رسد.

۲. بند (چ) ماده ۱ آیین‌نامه اجرایی: معامله یا عملیات مشکوک، هرگونه اقدام مالی یا غیرمالی است که با اوضاع و احوال اقتصادی، اجتماعی، شغلی یا درآمدی ارباب‌رجوع منطبق نبوده یا ظن تحصیل عواید نامشروع را ایجاد کند.

تحلیل:

✓ بنابراین، شاخص‌های معاملات مشکوک معیارهای رفتاری، مالی، یا اسنادی هستند که باعث ایجاد ظن معقول به وقوع جرم پولشویی می‌شوند.

✓ تشخیص این شاخص‌ها باید بر پایه تحلیل ریسک، شناخت مشتری، و الگوهای معمول رفتار مالی در بخش مربوطه انجام شود.

تقسیم‌بندی شاخص‌ها

شاخص‌ها به دو دسته کلی تقسیم می‌شوند:

نوع شاخص	توضیح	نمونه
شاخص‌های عمومی	در همه بخش‌ها و صنایع قابل استفاده‌اند	گردش غیرعادی حساب، استفاده از چند حساب، معاملات نقدی کلان
شاخص‌های اختصاصی	مختص هر بخش اقتصادی بر اساس ماهیت فعالیت آن	در بانک، بیمه، کارگزاری، تولید، صرافی و غیره

شاخص‌های عمومی معاملات مشکوک

۱. تغییر ناگهانی الگوی رفتاری مالی مشتری:
افزایش یا کاهش غیرمنطقی در گردش حساب، بدون تغییر در وضعیت اقتصادی یا شغلی.
۲. انجام مکرر معاملات نقدی یا خرد به منظور اجتناب از گزارش TTR :
تقسیم مبلغ کلان به تراکنش‌های خرد (Structuring) .
۳. استفاده از واسطه‌ها یا اشخاص ثالث برای انتقال وجوه:
انتقال مکرر وجوه بین اشخاص بدون توجیه اقتصادی روشن.
۴. عدم تناسب بین حجم تراکنش و وضعیت شغلی یا مالی مشتری:
مثال: گردش میلیاردی برای فردی با درآمد متوسط یا بدون شغل مشخص.

شاخص‌های عمومی معاملات مشکوک

۵. تغییر مکرر آدرس، شماره تماس یا حساب بانکی:
 نشانه تلاش برای پنهان‌سازی یا گمراه کردن سیستم نظارتی.

۶. ارسال یا دریافت وجوه از کشورها و مناطق پرخطر:
 کشورهایی که در فهرست سیاه FATF یا دارای نظارت ضعیف مالی هستند.

۷. خرید و فروش سریع دارایی‌های نقدشونده (طلا، ارز، سهام):
 انتقال سریع ارزش برای پنهان کردن منشأ پول.

۸. فسخ یا لغو غیرمنتظره معاملات بزرگ پس از انتقال وجه:
 سناریوی متداول برای پولشویی از طریق بازگشت وجوه.

شاخص‌های اختصاصی در بخش‌های اقتصادی

الف) بخش بانکی و مؤسسات اعتباری

- ✓ افتتاح چند حساب توسط یک شخص با نام‌های متفاوت یا شرکت‌های پوششی.
- ✓ استفاده از حساب‌های کوتاه‌مدت برای گردش مالی سنگین.
- ✓ سپرده‌گذاری‌های نقدی کلان توسط اشخاص بدون سابقه بانکی.
- ✓ انتقال وجوه بین حساب‌های مرتبط در بازه زمانی کوتاه (Layering)
- ✓ درخواست برداشت نقدی سنگین بلافاصله پس از واریز الکترونیکی.

شاخص‌های اختصاصی در بخش‌های اقتصادی

ب) بخش بیمه و کارگزاری بیمه‌ای

- ✓ خرید بیمه‌نامه‌های بلندمدت (عمر، پس‌انداز) با مبالغ غیرعادی.
- ✓ لغو بیمه‌نامه پیش از موعد و مطالبه بازپرداخت نقدی.
- ✓ انتقال منافع بیمه به اشخاص ثالث بدون رابطه مشخص.
- ✓ پرداخت حق بیمه از منابع ناشناخته یا حساب اشخاص دیگر.

شاخص‌های اختصاصی در بخش‌های اقتصادی

ج) بخش کارگزاری و بازار سرمایه

- ✓ خرید ناگهانی سهام شرکت‌های کم‌ارزش به مقادیر بالا.
- ✓ فروش سریع و متوالی اوراق بهادار بدون هدف سرمایه‌گذاری مشخص.
- ✓ ورود وجوه سنگین از اشخاص فاقد سابقه بورسی.
- ✓ استفاده از حساب‌های مشترک یا وکالتی در معاملات پرحجم.

شاخص‌های اختصاصی در بخش‌های اقتصادی

د) بخش صرافی و انتقال وجه ارزی

- ✓ خرید و فروش ارز به مبالغ سنگین با منشأ نامعلوم.
- ✓ تراکنش‌های ارزی از کشورهای با شفافیت مالی پایین.
- ✓ استفاده از صرافی‌های متعدد برای انجام نقل و انتقالات مشابه.
- ✓ عدم ارائه مستندات تجاری معتبر برای حواله‌های ارز

شاخص‌های اختصاصی در بخش‌های اقتصادی

هـ) بخش تولید و بازرگانی

- ✓ صدور یا دریافت فاکتورهای صوری برای صادرات یا واردات.
- ✓ تفاوت غیرعادی بین ارزش ثبت‌شده کالا و قیمت واقعی بازار.
- ✓ پرداخت‌های غیرمستقیم از طرف شرکت‌های نامرتبط.
- ✓ ثبت شرکت‌های زنجیره‌ای برای پنهان کردن منشأ درآمد.

رویکرد تحلیلی در استفاده از شاخص‌ها

✓ شاخص‌ها به تنهایی نشانه قطعی جرم نیستند؛ بلکه ابزاری برای ایجاد «ظن معقول» هستند.

✓ کارشناسان باید با تلفیق شاخص‌ها و تحلیل داده‌ها، به یک نتیجه مبتنی بر قرائن برسند.

روش‌های تحلیلی پیشنهادی:

۱. تحلیل رفتاری: (Behavioral Analysis)

بررسی تغییر در عادات‌های مالی مشتریان نسبت به سابقه خود.

۲. تحلیل مقایسه‌ای: (Peer Comparison)

مقایسه رفتار مالی مشتری با مشتریان مشابه در همان گروه شغلی یا درآمدی.

۳. تحلیل شبکه‌ای: (Network Analysis)

شناسایی ارتباط میان حساب‌ها، شرکت‌ها و اشخاص در یک شبکه مالی.

۴. تحلیل روندی: (Trend Analysis)

رصد الگوی زمانی تراکنش‌ها برای کشف فعالیت‌های غیرطبیعی.

نمونه‌های عملی از بخش‌های مختلف

مثال ۱ (بخش بانکی):

مشتری در عرض دو هفته، سه حساب جدید افتتاح کرده و هرکدام گردش بالایی دارد بدون سابقه فعالیت اقتصادی. ➔ شاخص‌های افتتاح چند حساب و گردش مالی نامتناسب فعال می‌شود. گزارش STR الزامی است.

مثال ۲ (بخش بیمه):

یک مشتری حق بیمه چند میلیاردی پرداخت می‌کند و دو ماه بعد تقاضای لغو بیمه‌نامه و دریافت وجه نقد دارد. ➔ شاخص فسخ زود هنگام بیمه‌نامه مشمول بررسی پولشویی است.

نمونه‌های عملی از بخش‌های مختلف

مثال ۳ (بازار سرمایه):

کارگزاری متوجه خرید و فروش سریع سهام بی‌ارزش توسط شخصی می‌شود که سود اقتصادی ندارد.
 ➔ شاخص معاملات فاقد منطق اقتصادی نشان‌دهنده الگوی لایه‌سازی (Layering) است.

مثال ۴ (صرافی):

فردی از چند صرافی مختلف در یک روز معادل بیش از سقف مجاز ارز خریداری کرده است.
 ➔ شاخص تجزیه تراکنش (Smurfing) فعال شده و باید گزارش TTR ارسال شود.

اهمیت ثبت و تحلیل شاخص‌ها در سامانه‌های نظارتی

اشخاص مشمول باید نظامی برای طبقه‌بندی، ردیابی و ثبت شاخص‌های مشکوک طراحی کنند. این نظام باید:

- ✓ بر پایه تحلیل ریسک مشتریان عمل کند،
- ✓ به‌طور خودکار الگوهای مشکوک را شناسایی کند،
- ✓ گزارش‌های STR را بر اساس داده‌های واقعی تولید نماید.

پیشنهاد اجرایی:

ترکیب سامانه‌های بانکی و مالی با سیستم‌های تحلیل داده (Data Mining) و یادگیری ماشین

(Machine Learning) برای کشف الگوهای پنهان و رفتارهای مشکوک.

فصل ۵: ردیابی و تحلیل اطلاعات مالی

۱. مراحل ردیابی جریانهای مالی مشکوک
۲. ابزارها و نرم افزارهای مورد استفاده در تحلیل تراکنشها
۳. اصول تجمیع و پاک سازی دادهها (Data Cleansing & Aggregation)

ردیابی و تحلیل اطلاعات مالی

(Financial Intelligence Analysis)

- ✓ **ردیابی مالی** به معنای شناسایی و بازسازی مسیر حرکت وجوه یا دارایی‌هایی است که مظنون به منشأ غیرقانونی‌اند، از لحظه تولید تا تبدیل نهایی یا ادغام در اقتصاد رسمی.
- ✓ **ردیابی وجوه مشکوک** شامل گردآوری، مستندسازی، تحلیل و بازسازی جریان مالی است تا منشأ، مسیر، و مقصد نهایی آن مشخص شود.

مبانی قانونی و نهادی ردیابی اطلاعات مالی

ماده (۷ مکرر) قانون مبارزه با پولشویی :

✓ مرکز اطلاعات مالی مسئول «دریافت، جمع‌آوری، تجزیه و تحلیل و ارزیابی اطلاعات مربوط به معاملات مشکوک» است و در صورت ظن قوی به وقوع جرم، پرونده را برای اقدام قضایی ارسال می‌کند.

✓ مراجع قضایی، انتظامی، اطلاعاتی، مالیاتی، گمرک و بانک مرکزی موظف‌اند به درخواست مرکز اطلاعات مالی، اطلاعات مورد نیاز را در چارچوب مقررات ارائه کنند.

اهداف اصلی ردیابی مالی:

۱. کشف منشأ و مقصد وجوه مشکوک.
۲. شناسایی ذی نفعان نهایی (Ultimate Beneficial Owners).
۳. شناسایی ساختارهای پوششی (شرکت‌ها، واسطه‌ها، حساب‌های موقت).
۴. مستندسازی قابل استناد برای مراجع قضایی و FIU.

مراحل ردیابی وجوه و اطلاعات مالی

مرحله	عنوان	شرح فعالیت
۱	جمع آوری داده‌ها (Data Collection)	دریافت اطلاعات از سیستم‌های داخلی، بانک‌ها، کارگزاری‌ها، صرافی‌ها و پایگاه‌های رسمی
۲	پاک‌سازی داده‌ها (Data Cleansing)	حذف داده‌های تکراری، اشتباه یا ناقص و استانداردسازی فرمت‌ها
۳	یکپارچه‌سازی داده‌ها (Data Integration)	ترکیب داده‌های بانکی، مالیاتی و تجاری در یک چارچوب تحلیلی
۴	تحلیل جریان وجوه (Flow Analysis)	شناسایی مسیر ورود و خروج وجوه، حساب‌های واسط، و الگوهای تکرارشونده
۵	تحلیل شبکه‌ای (Network Analysis)	کشف ارتباط میان اشخاص، شرکت‌ها، حساب‌ها و معاملات مرتبط
۶	مستندسازی و گزارش‌دهی (Reporting)	تهیه گزارش تحلیلی نهایی و ارسال به مرکز اطلاعات مالی

ابزارها و روش‌های تحلیل اطلاعات مالی

۱. تحلیل جریان نقدی (Cash Flow Analysis)

بررسی الگوهای ورود و خروج وجه نقد به منظور کشف جریان‌های نامتعارف، مانند گردش غیرمنطقی بین حساب‌های شخصی و شرکتی.

۲. تحلیل الگوهای زمانی (Temporal Analysis)

شناسایی تغییرات ناگهانی در زمان‌بندی تراکنش‌ها؛ مانند افزایش فعالیت در پایان سال مالی یا قبل از اعلام مقررات جدید.

۳. تحلیل شبکه‌ای (Network & Link Analysis)

شناسایی ارتباطات پنهان بین افراد، شرکت‌ها، حساب‌ها و تراکنش‌ها با استفاده از گراف‌ها و داده‌کاوی.

ابزارهای پیشنهادی: i2 Analyst's Notebook، Neo4j، GraphX.

۴. تحلیل رفتاری (Behavioral Analysis)

مقایسه رفتار فعلی مشتری با رفتار مالی گذشته با الگوی عمومی شغل و طبقه درآمدی او.

۵. تحلیل فرضیه‌محور (Hypothesis Testing)

فرضیه‌سازی بر اساس نشانه‌های اولیه (مثلاً «منبع درآمد غیرقانونی») و آزمون آن با داده‌های واقعی.

۶. تحلیل اکتشافی داده‌ها (Exploratory Data Analysis)

کشف الگوهای پنهان یا روابط غیرمنتظره در داده‌ها با استفاده از ابزارهای داده‌کاوی (Data Mining).

ابزارهای نرم‌افزاری و سامانه‌های کمکی در ردیابی مالی

نوع ابزار	کاربرد	نمونه‌های رایج
سامانه‌های داخلی FIU	دریافت و تجزیه و تحلیل گزارش‌های STR و TTR	سامانه جامع گزارش‌دهی معاملات مشکوک
سامانه‌های تحلیلی بانکی	تشخیص الگوهای مشکوک در تراکنش‌ها	AML Monitoring Tools (FICO, SAS, Actimize)
ابزارهای متن‌باز (Open Source)	تحلیل شبکه‌ای و داده‌کاوی اطلاعات مالی	Elastic Stack, Maltego CE, MISP
نرم‌افزارهای هوش مصنوعی	تحلیل الگوهای غیرعادی و پیش‌بینی تخلفات	Power BI, RapidMiner, Python ML

نحوه همکاری با مرکز اطلاعات مالی (FIU)

نقش واحد مبارزه با پولشویی (AML Unit) :

۱. جمع‌آوری و تجزیه و تحلیل داده‌های داخلی.
۲. شناسایی موارد مشکوک بر اساس شاخص‌های مصوب.
۳. تهیه گزارش تحلیلی در قالب STR با پیوست مستندات.
۴. ارسال محرمانه گزارش به FIU از طریق سامانه الکترونیکی.
۵. پاسخگویی به استعلام‌های تکمیلی مرکز.

نقش مرکز اطلاعات مالی (FIU):

۱. دریافت و ثبت گزارش‌ها از اشخاص مشمول.
۲. بررسی صحت داده‌ها و حذف موارد تکراری.
۳. تحلیل شبکه‌ای ارتباط میان اشخاص و حساب‌ها.
۴. تهیه پرونده اطلاعات مالی (Financial Dossier) برای هر مورد مشکوک.
۵. ارسال پرونده به مراجع قضایی یا امنیتی در صورت ظن قوی به وقوع جرم.

نکته مهم:

طبق تبصره ۱ ماده ۷ مکرر قانون،
 FIU می‌تواند دستور توقیف موقت
 وجوه یا اموال مشکوک به مدت ۲۴
 ساعت را صادر کند تا بررسی تکمیلی
 انجام شود.

فصل ۶: رویکردهای تحلیلی در کشف تخلفات

۱. رویکرد فرضیه‌محور (Hypothesis-driven Analysis) در شناسایی پولشویی
۲. رویکرد اکتشافی (Exploratory Analysis) و نقش داده‌کاوی در کشف الگوهای پنهان
۳. مقایسه نقاط قوت و ضعف هر رویکرد در تحلیل مالی

رویکرد فرضیه‌محور (Hypothesis-driven Analysis) در شناسایی پولشویی

در این روش، تحلیل‌گر با فرضیه یا سؤال مشخصی کار را آغاز می‌کند. مثلاً؛
“آیا حساب X برای لایه‌سازی وجوه استفاده می‌شود؟” و داده‌ها را برای تأیید یا رد آن فرضیه بررسی می‌کند.

مراحل اجرایی:

۱. تعریف فرضیه (براساس شاخص‌ها، رفتار مشتری، یا گزارش STR).
۲. جمع‌آوری داده‌های مرتبط از سیستم‌ها و پایگاه‌ها.
۳. آزمون فرضیه با داده‌های واقعی.
۴. نتیجه‌گیری و تهیه گزارش تحلیلی.

رویکرد فرضیه‌محور (Hypothesis-driven Analysis) در شناسایی پولشویی

کاربرد:

✓ بررسی پرونده‌های خاص و متمرکز.

✓ تحلیل تراکنش‌های مرتبط با افراد یا شرکت‌های مشخص.

✓ استفاده در گزارش‌های قضایی یا نظارتی.

محدودیت‌ها:

✓ نیاز به دانش قبلی از موضوع.

✓ احتمال از دست رفتن الگوهای جدید یا ناشناخته.

مزایا:

✓ کنترل دقیق بر مسیر تحلیل.

✓ مناسب برای پرونده‌های خاص و تحقیقات متمرکز.

تحلیل اکتشافی (Exploratory Data Analysis - EDA)

در این روش، هدف یافتن الگوها و روابط پنهان در داده‌ها بدون فرضیه اولیه است؛ سیستم به‌طور خودکار روابط غیرمعمول و رفتارهای ناهنجار را کشف می‌کند.

مراحل اجرایی:

۱. جمع‌آوری و آماده‌سازی داده‌های جامع.
۲. تحلیل الگوهای رفتاری، خوشه‌بندی (Clustering) و روابط شبکه‌ای.
۳. شناسایی موارد غیرعادی (Anomalies) یا رفتارهای غیرطبیعی.
۴. ارزیابی و برچسب‌گذاری نتایج برای آموزش مدل‌های بعدی.

تحلیل اکتشافی (Exploratory Data Analysis - EDA)

کاربرد:

- ✓ کشف الگوهای جدید از تخلفات و پولشویی.
- ✓ پایش مستمر سامانه‌های مالی.
- ✓ طراحی سیستم‌های هشداردهی هوشمند.

محدودیت‌ها:

- ✓ نیاز به حجم زیاد داده و ابزارهای تحلیلی پیشرفته.
- ✓ امکان بروز هشدارهای کاذب (False Positives)

مزایا:

- ✓ توان کشف الگوهای ناشناخته و پیچیده.
- ✓ امکان به‌روزرسانی خودکار مدل‌ها.

ترکیب دو رویکرد برای تحلیل هوشمند

در عمل، ترکیب هر دو رویکرد بهترین نتیجه را در کشف پولشویی دارد:

نوع رویکرد	هدف	مرحله
اکتشافی	کشف الگوهای جدید از داده‌های بزرگ	۱
فرضیه‌محور	بررسی و تأیید صحت الگوهای کشف‌شده	۲
یادگیری ماشینی	آموزش مدل‌های شناسایی خودکار بر اساس داده‌های واقعی	۳

نتیجه: سیستم‌های AML نوین از هر دو رویکرد به‌صورت هم‌زمان استفاده می‌کنند تا دقت و سرعت تحلیل افزایش یابد.

ابزارها و الگوریتم‌های داده‌محور در تحلیل تخلفات

۱. تحلیل شبکه‌ای (Network Analysis)

✓ برای شناسایی ارتباطات مالی بین افراد، شرکت‌ها، حساب‌ها و تراکنش‌ها.

✓ ابزارها: Maltego، Gephi، Neo4j، i2 Analyst's Notebook

۲. یادگیری ماشین (Machine Learning)

هوش مصنوعی با استفاده از مدل‌های یادگیری می‌تواند الگوهای پولشویی را به صورت خودکار شناسایی کند.

نوع یادگیری	کاربرد در AML	الگوریتم‌های رایج
یادگیری با ناظر (Supervised Learning)	آموزش مدل با داده‌های برچسب‌دار (مشکوک/عادی)	Random Forest, XGBoost, SVM
یادگیری بدون ناظر (Unsupervised Learning)	کشف الگوهای پنهان بدون برچسب‌گذاری	K-Means, DBSCAN, Isolation Forest
یادگیری نیمه‌ناظر (Semi-Supervised)	تلفیق داده‌های برچسب‌دار و بدون برچسب	Autoencoder, GANs
یادگیری تقویتی (Reinforcement Learning)	بهبود تدریجی مدل در مواجهه با داده‌های جدید	Q-Learning, Deep RL

ساختار داده‌محور واحد تحلیل در سازمان

گام ۱: جمع‌آوری و ذخیره‌سازی داده‌های مالی

از سامانه‌های داخلی، بانک‌ها، بیمه‌ها، بورس و پایگاه‌های رسمی.

گام ۲: پالایش داده (Data Cleaning)

حذف داده‌های ناقص، تکراری و مغایر با ساختار.

گام ۳: یکپارچه‌سازی (Data Integration)

تجمیع داده‌ها در یک پایگاه تحلیلی واحد.

گام ۴: تحلیل داده (Data Analysis)

اجرای الگوریتم‌های آماری، شبکه‌ای و هوش مصنوعی.

گام ۵: تولید هشدار (Alert Generation)

سیستم به‌صورت خودکار موارد مشکوک را شناسایی و به کارشناس گزارش می‌دهد.

گام ۶: ارزیابی و بازخورد (Feedback Loop)

کارشناس AML نتیجه بررسی را به مدل اعلام می‌کند تا دقت سیستم افزایش یابد.

شاخص‌های تحلیلی در رویکرد داده‌محور

نوع شاخص	تعریف	مثال
شاخص رفتاری	انحراف رفتار مشتری از الگوی عادی خود	افزایش ناگهانی حجم تراکنش‌ها
شاخص ارتباطی	ارتباط غیرمعمول بین حساب‌ها و اشخاص	چند شرکت با آدرس مشترک و حساب‌های متقاطع
شاخص زمانی	تمرکز تراکنش‌ها در بازه خاص	افزایش تراکنش‌ها در روزهای تعطیل یا پایان ماه
شاخص جغرافیایی	نقل و انتقال وجوه بین مناطق پرخطر	ارسال مکرر وجه به کشور تحریمی
شاخص ساختاری	استفاده از شرکت‌های واسطه برای پنهان‌سازی مالک واقعی	شرکت‌های پوششی (Shell Companies)

مثال‌های کاربردی از تحلیل داده‌محور

مثال ۱:

✓ الگوی شناسایی شده توسط مدل یادگیری ماشین نشان می‌دهد مشتریانی با گردش بالای نقدی و ارتباط با شرکت‌های تازه تأسیس، احتمال STR بالاتری دارند.
 ➔ تحلیل فرضیه‌محور: بررسی سوابق این مشتریان برای تأیید یا رد منشأ وجوه.

مثال ۲:

✓ تحلیل خوشه‌ای داده‌های بانکی نشان می‌دهد گروهی از حساب‌ها در چند بانک با مقادیر نزدیک و زمان‌های مشابه تراکنش می‌کنند.
 ➔ تحلیل اکتشافی: احتمال وجود شبکه‌ای هماهنگ از حساب‌های واسطه.

مثال ۳:

✓ مدل هوش مصنوعی با بررسی داده‌های تراکنش‌های بین‌المللی، کشف می‌کند که برخی مشتریان از کشورهای که در فهرست پرخطر هستند، وجوهی با منشأ غیرشفاف منتقل می‌کنند.
 ➔ سیستم هشداردهی خودکار فعال و STR ارسال می‌شود.

H.M.AZIMI 0933870152

۸۰

فصل ۷: فناوری‌های نوین در تحلیل و شناسایی موارد مشکوک

۱. کاربرد هوش مصنوعی در شناسایی الگوهای غیرعادی و پیشگیری از پولشویی

۲. آشنایی با انواع الگوریتم‌های یادگیری ماشین:

✓ یادگیری با ناظر (Supervised Learning)

✓ یادگیری بدون ناظر (Unsupervised Learning)

۳. معرفی مهم‌ترین و کارآمدترین الگوریتم‌های تحلیل تخلف در حوزه مالی

۴. نقش ربات‌ها (RPA) در خودکارسازی فرآیندهای AML و پایش معاملات

۵. مروری بر سامانه‌ها، پلتفرم‌ها و ابزارهای متن‌باز (Open-source) در حوزه AML

H.M.A21M09387622

۸۱

نقش هوش مصنوعی در سیستم‌های AML

هوش مصنوعی می‌تواند در چهار سطح اصلی از چرخه AML به کار گرفته شود:

مرحله	نقش هوش مصنوعی	نتیجه مورد انتظار
۱	احراز هویت و KYC هوشمند	شناسایی خودکار چهره و تطبیق مدارک هویتی با پایگاه‌های رسمی
۲	پایش تراکنش‌ها (Transaction Monitoring)	کشف الگوهای غیرعادی در حجم بالا و در لحظه (Real-time Detection)
۳	تحلیل رفتاری (Behavioral Analytics)	مدل‌سازی رفتار مالی مشتری و کشف انحرافات
۴	پیش‌بینی تخلف (Predictive Analytics)	پیش‌بینی احتمال وقوع پولشویی بر اساس داده‌های تاریخی

انواع یادگیری ماشین در مبارزه با پولشویی

۱. یادگیری با ناظر (Supervised Learning)
۲. یادگیری بدون ناظر (Unsupervised Learning)
۳. یادگیری نیمه ناظر (Semi-Supervised Learning)
۴. یادگیری تقویتی (Reinforcement Learning)

۱. یادگیری با ناظر (Supervised Learning)

- ✓ مدل بر اساس داده‌های برچسب‌دار (مثلاً تراکنش مشکوک / غیر مشکوک) آموزش می‌بیند.
- ✓ کاربرد: طبقه‌بندی تراکنش‌ها، تشخیص رفتارهای مشکوک، امتیازدهی ریسک مشتری.

الگوریتم	کاربرد اصلی	مزایا	کاربرد اصلی
Logistic Regression	پیش‌بینی احتمال تخلف	سادگی و تفسیرپذیری	پیش‌بینی احتمال تخلف
Random Forest	دسته‌بندی تراکنش‌ها	دقت بالا و کنترل خطا	دسته‌بندی تراکنش‌ها
Gradient Boosting (XGBoost)	تحلیل تراکنش‌های کلان	یادگیری قوی از داده‌های نامتوازن	تحلیل تراکنش‌های کلان
Support Vector Machine (SVM)	تشخیص الگوهای پیچیده	عملکرد بالا در داده‌های کوچک	تشخیص الگوهای پیچیده

۲. یادگیری بدون ناظر (Unsupervised Learning)

✓ در این روش، مدل بدون داده‌های برچسب‌دار، الگوها و خوشه‌های پنهان را کشف می‌کند.

✓ کاربرد: کشف رفتارهای ناشناخته و شناسایی گروه‌های جدید مشتریان پریسک.

ویژگی‌ها	کاربرد	الگوریتم
شناسایی خوشه‌های پریسک	خوشه‌بندی مشتریان با رفتار مشابه	K-Means Clustering
کشف تراکنش‌های ناهنجار بدون الگوی ثابت	کشف نقاط پرت و غیرعادی	DBSCAN
کاهش هشدارهای کاذب	تشخیص ناهنجاری در داده‌های بزرگ	Isolation Forest
مناسب برای داده‌های حجیم بانکی	بازسازی رفتارهای عادی و تشخیص انحراف	Autoencoder (شبکه عصبی خودرمزگذار)

۳. یادگیری نیمه‌ناظر (Semi-Supervised Learning)

- ✓ ترکیب داده‌های برچسب‌دار و بدون برچسب برای افزایش دقت مدل.
- ✓ کاربرد: در محیط‌هایی که داده‌های تأییدشده محدود است (مثل تراکنش‌های STR واقعی).

الگوریتم	توضیح	مزیت
Self-Training	مدل از داده‌های جدید برای یادگیری خودکار استفاده می‌کند	افزایش دقت مدل در طول زمان
GANs (Generative Adversarial Networks)	تولید داده‌های مصنوعی شبیه نمونه‌های واقعی	بهبود عملکرد در کمبود داده‌های واقعی

۴. یادگیری تقویتی (Reinforcement Learning)

- ✓ مدل از طریق تجربه و بازخورد کارشناس AML یاد می‌گیرد چه تصمیمی بهترین نتیجه را دارد.
- ✓ کاربرد: سیستم‌های هشداردهی خودتنظیم‌شونده (Adaptive AML Alerts).

معماری سامانه هوشمند AML مبتنی بر هوش مصنوعی

ساختار پیشنهادی:

۱. پایگاه داده جامع: (Data Lake)

شامل داده‌های تراکنش، مشتری، مالیاتی، بیمه‌ای و خارجی.



۲. لایه پیش پردازش: (Preprocessing Layer)

پاک‌سازی، استانداردسازی و نرمال‌سازی داده‌ها.

۳. لایه تحلیل هوشمند: (AI Engine)

اجرای مدل‌های ML برای تشخیص الگوهای مشکوک.

۴. سیستم هشداردهی: (Alerting System)

تولید هشدار با اولویت‌بندی بر اساس ریسک.

۵. بازخورد انسانی: (Human Feedback)

بررسی کارشناسان AML و تغذیه نتایج به مدل. (Learning Loop)

H.M.AZIMI 0933870152

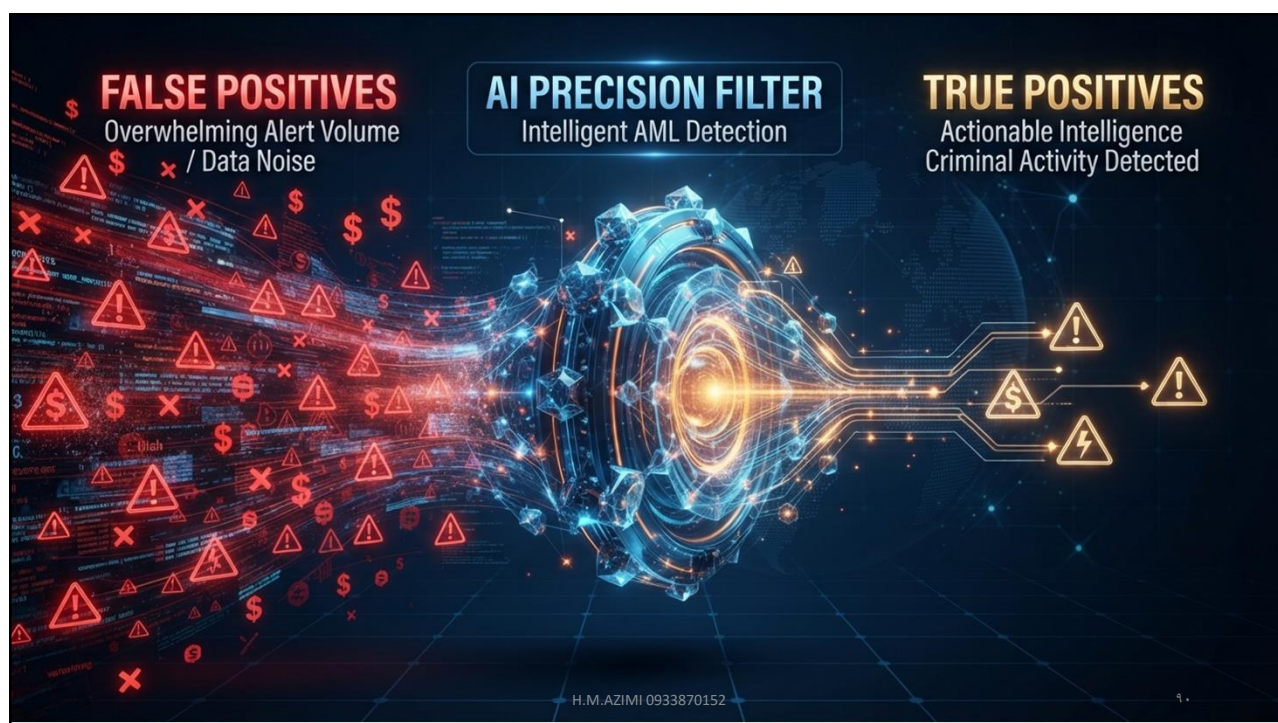
۸۸

کاهش هشدارهای کاذب (False Positive Reduction)

- ✓ یکی از چالش‌های بزرگ در AML، حجم بالای هشدارهای بی‌مورد است.
- ✓ هوش مصنوعی با تحلیل رفتاری دقیق و یادگیری مداوم، می‌تواند خطای انسانی را تا ۷۰٪ کاهش دهد.

راهکارهای کلیدی:

۱. تحلیل زمینه‌ای (Contextual Analysis) برای درک منطق تراکنش.
۲. مدل‌سازی فردی رفتار مشتری به‌جای الگوهای ثابت جمعی.
۳. بازخورد مستمر از کارشناسان انسانی برای اصلاح مدل‌ها.
۴. استفاده از الگوریتم‌های anomaly detection برای تمرکز بر داده‌های واقعاً غیرعادی.



مثال‌های کاربردی از هوش مصنوعی در AML

مثال ۱ - بخش بانکی:

یک بانک بزرگ ایرانی از مدل‌های **Random Forest** و **Autoencoder** برای پایش لحظه‌ای تراکنش‌ها استفاده می‌کند. نتیجه: کاهش ۶۵٪ در هشدارهای کاذب و افزایش دقت کشف **STR** از ۷٪ به ۱۸٪.

مثال ۲ - بخش بیمه:

الگوریتم **K-Means** خوشه‌هایی از مشتریان بیمه عمر را شناسایی می‌کند که لغو بیمه‌نامه‌های زود هنگام و بازخرید وجه دارند. نتیجه: کشف شبکه‌ای از تظہیر درآمد حاصل از جرائم اقتصادی.

مثال ۳ - بخش کارگزاری:

با استفاده از یادگیری بدون ناظر (**DBSCAN**)، مجموعه‌ای از حساب‌ها شناسایی شد که به صورت گروهی سهام شرکت‌های کم‌ارزش را خرید و فروش می‌کردند.

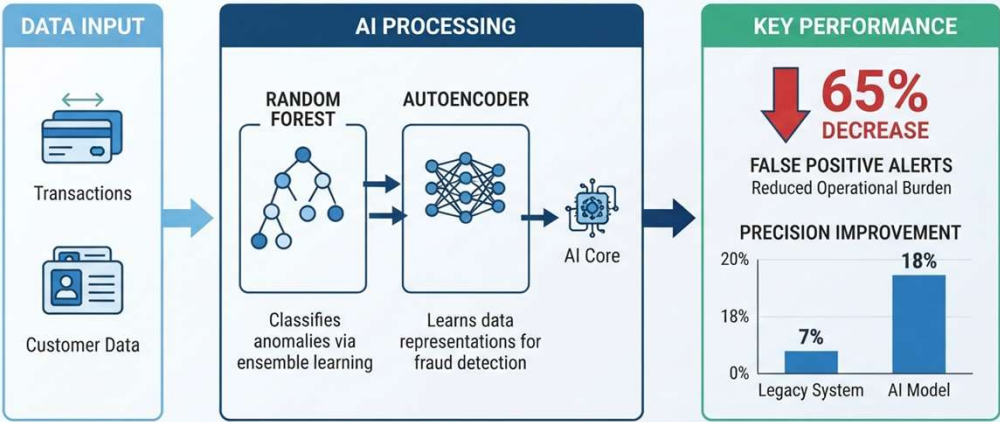
نتیجه: شناسایی شبکه سازمان‌یافته دست‌کاری بازار و پولشویی.

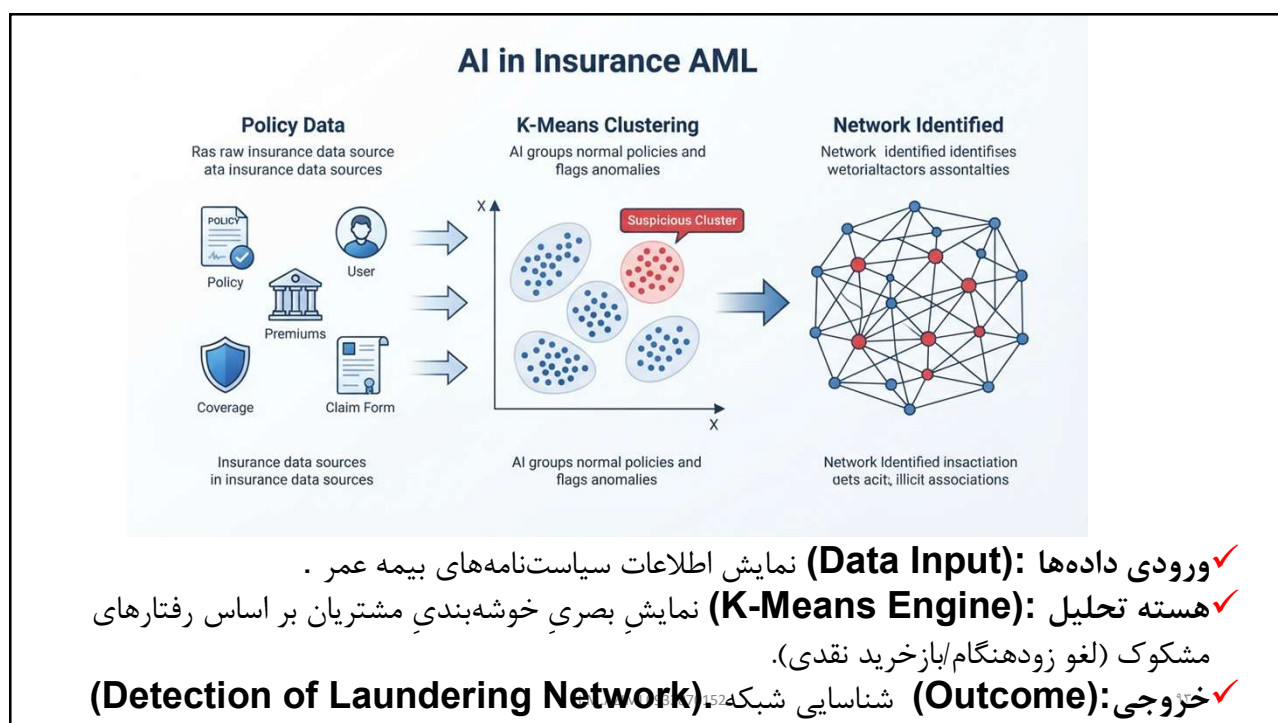
مثال ۴ - **FIU**:

مرکز اطلاعات مالی با ترکیب داده‌های بانکی، گمرکی و مالیاتی در یک مدل **XGBoost** توانست انتقال‌های مالی غیرعادی بین شرکت‌های وابسته را شناسایی کند که منجر به تشکیل پرونده قضایی شد.

H.M.AZIMI 0933870152

AI IN BANKING AML: APPLICATION FLOWCHART



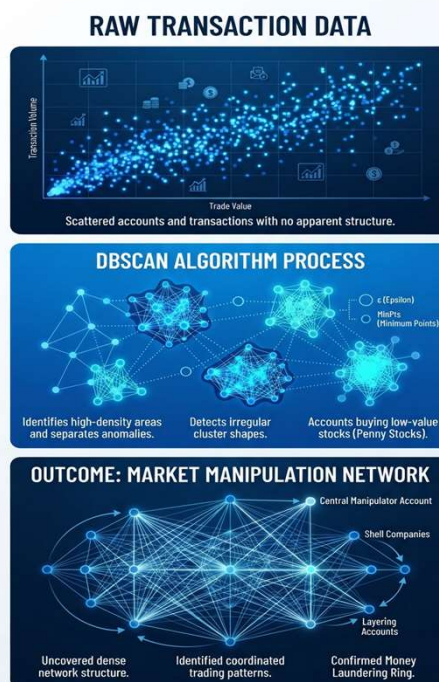


بخش اول: مجموعه‌ای از حساب‌های کاربری (Accounts) به صورت نقاط پراکنده (Scatter plot).

بخش دوم: تمرکز الگوریتم DBSCAN که این نقاط را به شکل خوشه‌های متراکم و غیرمنظم شناسایی می‌کند.

بخش سوم: نتیجه نهایی که نشان‌دهنده یک شبکه سازمان‌یافته (Network Graph) است.

H.M.AZIMI 0933870152



فصل ۸: تحلیل صورت‌های مالی در کشف نشانه‌های پولشویی

۱. نحوه استخراج و تفسیر اطلاعات از صورت‌های مالی و اظهارنامه‌های مالیاتی

۲. تحلیل تطبیقی بین اطلاعات مالی، حسابرسی و رفتار معاملاتی مشتری

تحلیل صورت‌های مالی و اظهارنامه مالیاتی در کشف نشانه‌های پولشویی

مبانی قانونی و الزامات افشای مالی

۱. ماده (۵) قانون مبارزه با پولشویی:

اشخاص مشمول موظفاند سوابق مالی، معاملاتی و اسناد مربوط به مشتریان را نگهداری و در صورت درخواست مراجع ذیصلاح ارائه نمایند.

۲. ماده (۷) همان قانون:

اشخاص مشمول باید گزارش‌های معاملات و عملیات مشکوک را به مرکز اطلاعات مالی ارسال نمایند.

۳. ماده (۶۲) آیین‌نامه اجرایی ماده ۱۴: اشخاص مشمول موظفاند در ارزیابی ریسک مشتریان حقوقی، از اطلاعات مالی، مالیاتی و حسابرسی‌شده بهره‌برداری نمایند.

اجزای اصلی صورت‌های مالی از منظر AML

کاربرد در AML	مفهوم کلیدی	جزء صورت مالی
بررسی افزایش ناگهانی دارایی‌ها یا بدهی‌های بدون منشأ شفاف	نمایش دارایی‌ها، بدهی‌ها و حقوق صاحبان سهام	ترازنامه (Balance Sheet)
کشف درآمدهای غیرمتناسب با فعالیت واقعی شرکت	نشان‌دهنده درآمد و هزینه در دوره مالی	صورت سود و زیان (Income Statement)
تشخیص انتقال وجه به اشخاص غیرمرتبط یا حوزه‌های پرریسک	جریان ورود و خروج نقدینگی	صورت جریان وجوه نقد (Cash Flow Statement)
کشف معاملات صوری یا انتقال بین‌شرکتی مشکوک	جزئیات دارایی‌ها، بدهی‌ها و معاملات با اشخاص وابسته	یادداشت‌های توضیحی (Notes)
شناسایی مغایرت بین سود ابرازی و سود واقعی شرکت	اطلاعات رسمی ارسالی به سازمان مالیاتی	اظهارنامه مالیاتی

Main Components of Financial Statements from an AML Perspective				
Financial Statement Component		Key Concept	AML Use	
	Balance Sheet	Shows assets, liabilities, and equity	Detects sudden increases in assets or liabilities without a clear source	
	Income Statement	Shows revenues and expenses during a financial period	Detects revenue inconsistent with the company's real business activity	
	Cash Flow Statement	Shows cash inflows and outflows	Identifies transfers to unrelated parties or high-risk jurisdictions	
	Notes to Financial Statements	Provides details on assets, liabilities, and related-party transactions	Detects fictitious transactions or suspicious intercompany transfers	
	Tax Return	Official financial information submitted to tax authorities	Identifies discrepancies between declared profit and actual company performance	

شاخص‌های مالی و مالیاتی مشکوک به پولشویی

شاخص‌های ترازنامه‌ای

نشانه	توضیح	احتمال
افزایش غیرمنطقی دارایی‌های جاری یا نقدی	بدون رشد فروش یا درآمد	لایه‌سازی وجوه نقد
افزایش سریع سرمایه ثبت‌شده شرکت	بدون تغییر در عملکرد واقعی	تزریق وجوه غیرشفاف
بدهی‌های بلندمدت بدون منبع مشخص	وام از اشخاص حقیقی غیرمرتبط	پوشش برای انتقال پول

Balance Sheet Red Flags for AML

Suspicious Financial & Tax Indicators

Red Flag	Explanation	Possible AML Meaning
Unusual rise in current assets or cash 	No matching growth in sales or revenue	 Cash layering 
Rapid increase in registered capital 	No real change in operations or performance	 Injection of opaque funds 
Long-term liabilities with unclear source 	Loans from unrelated individuals	 Cover for money transfer 
AML Review Focus  balance sheet review  source-of-funds check  related-party screening		

شاخص‌های جریان نقدی

شاخص‌های ترازنامه‌ای

نشانه	توضیح	احتمال
ورود نقدینگی بالا از اشخاص ناشناس	فاقد توجیه اقتصادی	مرحله «Placement» پولشویی
خروج وجه به حساب‌های وابسته خارجی	از طریق حواله یا شرکت‌های واسطه	«Integration» درآمد مجرمانه
گردش نقدی نامتناسب با عملکرد فروش	تفاوت بین درآمد حسابداری و جریان نقدی	احتمال حساب‌سازی مالی

شاخص‌های مالیاتی

شاخص‌های ترازنامه‌ای

نشانه	توضیح	احتمال
مغایرت شدید بین اظهارنامه مالیاتی و صورت‌های مالی حسابرسی شده	نشان‌دهنده گزارش‌دهی ناقص یا صوری	پنهان‌سازی درآمد مجرمانه
معافیت‌های مالیاتی غیرقابل توجیه	استفاده از پوشش خیریه یا صادراتی	تطهیر از طریق شرکت‌های معاف
تأخیر یا امتناع از ارائه اظهارنامه	قصد مخفی‌سازی جریان درآمدی	پولشویی یا فرار مالیاتی هم‌زمان

شاخص‌های مالی و مالیاتی مشکوک به پولشویی

شاخص‌های سود و زیان

نشانه	توضیح	احتمال
حاشیه سود غیرعادی بالا یا پایین	مغایر با میانگین صنعت	پنهان‌سازی یا تزریق سود ساختگی
هزینه‌های اداری و متفرقه غیرمعمول	هزینه‌های مشاوره یا بازاریابی صوری	پوشش برای پولشویی
کاهش ناگهانی سود خالص در سال خاص	پس از رشد سریع درآمدها	تطهیر از طریق بازخرید یا انتقال وجه

فصل ۹: مدیریت پرونده و محرمانگی اطلاعات

۱. گردش کار پرونده‌های مشکوک از مرحله شناسایی تا ارسال به FIU
۲. اصول حفاظت گفتار و رعایت محرمانگی هویت گزارش‌دهندگان
۳. الزامات امنیت اطلاعات و نگهداری سوابق در واحد مبارزه با پولشویی

حفاظت از اطلاعات و محرمانگی

✓ مطابق ماده ۸ قانون مبارزه با پولشویی:

افشای اطلاعات و اسناد یا استفاده از آنها به نفع خود یا دیگری به طور مستقیم یا غیرمستقیم ممنوع است و مرتکب به مجازات حبس تعزیری درجه پنج محکوم می شود.

✓ اطلاعات گزارش دهندگان باید محرمانه بماند و هویت آنان نباید برای ارباب رجوع یا اشخاص ثالث افشا شود.

✓ نکته اجرایی: در سازمان ها، معمولاً تنها مدیر واحد AML یا نماینده رسمی مجاز به ارسال مستقیم گزارش ها به FIU است تا زنجیره محرمانگی حفظ شود.

اصول محرمانگی و نگهداری سوابق

۱. ماده (۸) قانون:

افشای اطلاعات مربوط به گزارش‌ها یا داده‌های دریافتی جرم است و مرتکب به حبس تعزیری درجه پنج محکوم می‌شود.

۲. ماده (۱۴۲) آیین‌نامه:

اطلاعات، سوابق و اسناد باید حداقل به مدت ۱۰ سال در محل امن نگهداری شوند.

۳. بند (ت) ماده ۷ قانون:

نگهداری سوابق شناسایی ارباب‌رجوع و معاملات برای تحلیل‌های آتی الزامی است.

۴. اصول محرمانگی در ردیابی:

- ✓ تفکیک سطح دسترسی کارکنان به داده‌ها.
- ✓ رمزنگاری سوابق و ارتباطات الکترونیکی.
- ✓ حذف یا ناشناس‌سازی اطلاعات غیرضروری در مستندسازی.

اصول محرمانگی و نگهداری سوابق

حفاظت گفتار یعنی جلوگیری از انتقال یا افشای هرگونه اطلاعات مرتبط با پرونده‌های مشکوک، چه در قالب گفتار، پیام، ایمیل، یا مکاتبه اداری..

۱. ماده (۱۴۲) آیین‌نامه:

اطلاعات، سوابق و اسناد باید حداقل به مدت ۱۰ سال در محل امن نگهداری شوند.

۲. بند (ت) ماده ۷ قانون:

نگهداری سوابق شناسایی ارباب‌رجوع و معاملات برای تحلیل‌های آتی الزامی است.

۳. اصول محرمانگی در ردیابی:

- ✓ تفکیک سطح دسترسی کارکنان به داده‌ها.
- ✓ رمزنگاری سوابق و ارتباطات الکترونیکی.
- ✓ حذف یا ناشناس‌سازی اطلاعات غیرضروری در مستندسازی.



نهادهای متولی مبارزه با پولشویی

- ♦ شورای عالی مقابله و پیشگیری از جرایم پولشویی و تأمین مالی تروریسم
- ♦ مرکز اطلاعات مالی (F.I.U)
- ♦ دستگاه‌های متولی نظارت
- ♦ بانک مرکزی ♦ بیمه مرکزی ♦ سازمان بورس و اوراق بهادار ♦ وزارت صنعت، معدن و تجارت
- ♦ سازمان ثبت اسناد و املاک کشور ♦ و غیره
- ♦ اشخاص مشمول
- ♦ بانک‌ها ♦ بیمه‌ها ♦ مؤسسات مالی و اعتباری ♦ کارگزاری‌های بورس اوراق بهادار ♦ و غیره
- ♦ قوه قضاییه
- ♦ ضابطان دادگستری
- ♦ ضابطان عام ♦ ضابطان خاص ♦ وزارت اطلاعات ♦ سازمان اطلاعات سپاه

H.M.AZIMI 0933870152



قانون و آیین نامه مبارزه با پولشویی



آئین نامہ
اجرائی

قانون اصلاح قانون مبارزہ با پولشویی

H.M.AZIMI 0933870152

۱۱۱

شاخص‌ترین تغییرات و اصلاحات قانون جدید مبارزه با پولشویی:

- الف) اتخاذ تدابیر و سیاست‌های جنایی و کیفری سخت‌گیرانه تر از طریق افزایش درجه مجازات‌ها و جرم‌انگاری جدید،
- ب) قراردادن بار اثبات جرم بر عهده مظنون در موارد معاملات مشکوک در حوزه تحصیل دلایل و انتساب ادله به متهمین،
- ج) ارتقاء جایگاه و تکالیف واحد اطلاعات مالی به مرکز اطلاعات مالی،

دلایل جرم‌انگاری مستقل:

- تمایز با جرم منشأ:
جرم منشأ ممکن است قاچاق، اختلاس، رشوه، فرار مالیاتی، یا جرائم سازمان‌یافته باشد؛ اما پولشویی عملی ثانویه است که در پی آن انجام می‌شود و هدف آن پنهان کردن منبع غیرقانونی درآمد است.
- ضرورت مقابله با اثرات اقتصادی:
پولشویی سبب اختلال در شبکه اقتصادی، افزایش فعالیت‌های زیرزمینی، و تضعیف بخش تولید و اشتغال می‌شود.
- پاسخ به الزامات بین‌المللی (FATF):
استقلال جرم پولشویی برای انطباق با استانداردهای بین‌المللی در حوزه AML/CFT ضروری است.
- افزایش قدرت پیگرد قانونی:
با جرم‌انگاری مستقل، دستگاه‌های قضایی می‌توانند صرف‌نظر از اثبات جرم منشأ، مرتکب را تحت تعقیب قرار دهند (ماده ۹ قانون).

جرم منشأ

- هر رفتاری است که مطابق ماده (۲) قانون مجازات اسلامی مصوب ۱۳۹۲/۰۲/۰۱ جرم محسوب شود. از منظر این قانون تخلفات مذکور در قانون مبارزه با قاچاق کالا و ارز با اصلاحات بعدی جرم محسوب می شود.

مال

- هر نوع دارایی اعم از مادی یا غیر مادی، منقول یا غیرمنقول، مشروع یا غیرمشروع و هر نوع منفعت یا امتیاز مالی و همچنین کلیه اسناد مبین حق اعم از کاغذی یا الکترونیکی نظیر اسناد تجاری، سهام یا اوراق بهادار.

مال حاصل از جرم:

- هر مالی که به طور مستقیم یا غیرمستقیم از جرم منشأ به دست آید از قبیل مالی که از جرائم اقتصادی و جرم تأمین مالی تروریسم حاصل می شود، همچنین، مال موضوع جرم یا مالی که برای ارتکاب جرم اختصاص داده شده است در حکم مال به دست آمده از جرم است.

منابع

- ❑ قانون اصلاح قانون مبارزه با پولشویی (مصوب ۱۳۹۷)
- ❑ آیین نامه اجرایی مقابله و پیشگیری از جرایم پولشویی و تأمین مالی تروریسم (مصوب ۱۴ آبان ۱۴۰۴)
- ❑ FATF
- ❑ UNODC
- ❑ ACAMS
- ❑ و منابع در دسترس



مركز مالی ایران
MAZINI FINANCIAL CENTER

به پایان آمد این دفتر، حکایت همچنان باقی

باسپاس از توجه شما عزیزان

حمید محمد عظیمی

0933 870 1752

hamid.mazimi@gmail.com

118