الأمن المالي

№ 41
آذار / مارس 2024

رئيس الأكاديمية الروسية للعلوم

غينادي كراسنيكوف:

"نشهد اليوم ثورة علمية وتكنولوجية تُحدث تغييرات جذرية في العالم من حولنا. وتزداد أهمية التوعية بقضايا تطبيق التقنيات الحديثة والاستفادة من خبرات المطورين والباحثين في هذا المجال"

كلمة افتتاحية

يوري شيخانتشين -
مدير هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)
رئيس هيئة التحرير

القراء الأعزاء!

لا يمكننا تخيل وجود العالم اليوم من دون التكنولوجيا المتطورة، فقد أصبحت تلعب دورًا محوريًا في تشكيل حاضرنا ومستقبلنا. واتّسعت دائرة تأثيرها لتشمل جميع مجالات الحياة تقريبًا، وأصبحت جزءًا لا يمكن الاستغناء عنه في ممارساتنا اليومية. إذ تُقدم لنا التكنولوجيا المالية حلولاً ذكية لإجراء عمليات الشراء بسهولة بنقرة واحدة فقط، دون الحاجة إلى زيارة المتجر، كما توفر لنا إمكانية تحويل الأموال ودفع الفواتير والحصول على القروض بشكل سريع وآمن. وهذا يُوفر علينا الكثير من الوقت والجهد.

كما أدى الاتجاه نحو التحول الرقمي إلى تغيير جذري في طريقة عمل الهيئات الحكومية. حيث تُدرج هيئة الرقابة المالية الروسية، أسوةً بمعظم الوكالات الأخرى، استخدام إمكانيات أدوات تكنولوجيا المعلومات ضمن نهجها العملي بشكلٍ فاعل.

وعلى سبيل المثال، تتمثل إحدى طرق تفاعل خدمتنا مع الجهات المشاركة في نظام مكافحة غسل الأموال من خلال استخدام حساب شخصي في الموقع الالكتروني لهيئة الرقابة المالية الروسية. إذ تُرسل إلينا ما يُقرب من مليون رسالة يوميًا ونُرسل ردودنا في غضون ساعات قليلة من استلامها. ولا شك أن معالجة هذا الكم الهائل من المعلومات يدويًا أمر غير ممكن.

ومن هنا لا يمكننا أن نغفل دور الأشخاص الذين ساهموا في تطوير هذه التقنيات. إن الذكاء الاصطناعي، بقدر ما يزخر به من إمكانيات هائلة، لا يعدو كونه سوى مساعد للإنسان في حل المشكلات المعقدة. ولا يمكن لأي نظام أو آلة أن تحل محل الإنسان في اتخاذ القرار.

ومع التطور المُتسارع للتكنولوجيا المتقدمة، نشهد ارتفاعًا ملحوظًا في المخاطر المُتعلقة بإساءة استخدامها لأغراض غير قانونية. فقد بدأ المجرمون باستغلال تقنيات الذكاء الاصطناعي وابتكارات تكنولوجيا المعلومات الأخرى في ارتكاب جرائم مثل: الاختلاس وغسل الأموال وتمويل الإرهاب والاتجار بالمخدرات والأسلحة في ارتكاب أعمال أخرى. وفي الوقت ذاته، اتسع نطاق الجرائم الإلكترونية لتتخذ طابعًا عابرًا للحدود الوطنية.

ومن هذا المنطلق، تبرز في وقتنا الحالي أهمية التعاون بين مختلف الأطراف، بدءًا من المجتمع الدولي، مرورًا بأجهزة الدولة، ووصولًا إلى القطاع الخاص والمجتمع المدني، وذلك لمواجهة التحديات والتهديدات الجديدة.

تستعرض صفحات هذه المجلة دراسات حالة حول تطبيق الأدوات الرقمية والذكاء الاصطناعي في عمل الهيئات الحكومية والبنوك في روسيا والعالم، مع تسليط الضوء على جوانب تنظيم سوق الخدمات المالية، وتبادل الخبرات في مجال مكافحة الجرائم الإلكترونية، واستخدام التكنولوجيا المتقدمة، ومناقشة التحديات الحالية في مجال الأمن السيبراني واستخدام العملات الرقمية.

ندعو قراءنا إلى خوض غمار عالم التكنولوجيا المُتطوّرة والتأمل من جديد في تأثيرها على مختلف جوانب حياتنا.

المحتويات

6 **غ. يا. كراسنيكوف**
تحية طيبة لقراء مجلة "الأمن المالي"

التكنولوجيا المتقدمة في خدمة الأمان المالي

8 **أنطون ليسيتسين**
مكافحة غسل الأموال وتمويل الإرهاب في عصر التكنولوجيا الرقمية: تحدي العصر

11 **السيد كيشاف أناند**
السيدة م. شانموغا بريا،
التطورات في مجال التكنولوجيا المالية بالهند: التركيز على الابتكار والأمان المالي ومكافحة الجرائم الإلكترونية

15 **السيد يوري كوروتكي**
"المراقبة المالية هي بمثابة تصوير مقطعي مالي"

19 **أوتابيك أوليموفيتش رحمانوف**
آليات تنظيم مكافحة غسل الأموال وتمويل الإرهاب في سوق التكنولوجيا المالية: دراسة حالة أوزبكستان

24 **فيكتوريا كابارتشوك**
يانا بايراشنايا،
ألكسندر كوريانوف
استخدام التكنولوجيا الرقمية في الأنشطة الرقابية وتعزيز كفاءة الجهات الخاضعة للمساءلة

31 **دينارا موسينا**
سجلّ المُستفيدين الفعليين. تجربة كازاخستان

الذكاء الاصطناعي في التقنيات المالية: نظرة على الحاضر والمستقبل

35 **سفيتلانا أورلوفا**
"المنتجات والحلول الرقمية هي ركيزة أساسية لتطوير المراجعة المالية الحكومية"

39 **ف. ل. دوستوف**
تقنيات الذكاء الاصطناعي في القطاع المالي وتأثيرها على بعض جوانب مكافحة غسل الأموال وتمويل الإرهاب

11
السيد كيشاف أناند
السيدة م. شانموغا بريا،
التطورات في مجال التكنولوجيا المالية بالهند: التركيز على الابتكار والأمان المالي ومكافحة الجرائم الإلكترونية

15
السيد يوري كوروتكي
"المراقبة المالية هي بمثابة تصوير مقطعي مالي"

35
سفيتلانا أورلوفا
"المنتجات والحلول الرقمية هي ركيزة أساسية لتطوير المراجعة المالية الحكومية"

43 **ميخائيل سيرغيفيتش برونين**
توظيف الذكاء الاصطناعي في أعمال هيئة الرصد المالي

46 **أليكسي غيليتا**
"سوق التكنولوجيا المالية في روسيا هو أحد أكثر الأسواق ابتكارًا وتقدمًا في العالم من الناحية التقنية "

كشف الجرائم الإلكترونية وقمعها

50 **بوغدان ألكساندروفيتش شابليا**
مكافحة "المُتواطئين في الاحتيال" والعمليات عالية المخاطر بين الأفراد (P2P) تمثل أولوية قصوى في مجال الرقابة المالية

53 **فاديم ألكسندروفيتش أوفاروف،**
الأمن المعلوماتي في السوق المالية: مكافحة الاحتيال الإلكتروني في عمليات تحويل الأموال

57 **نيكولايفيتش راستاشينوف**
تقييد الوصول إلى المعلومات الممنوع نشرها في روسيا الاتحادية قبل الحصول على أمر قضائي

60 **رومان فياتشيسلافوفيتش موخلينوف**
"الاتجاهات الحالية في سوق مقدمي الخدمات المالية غير الشرعيين"

63 **أوليغ فياتشيسلافوفيتش كيبكايف**
توظيف التكنولوجيا الرقمية في عملية جمع المعلومات والبيانات التحليلية وغيرها، ومعالجتها وتحليلها، وغيرها من البيانات المستخدمة في أنشطة الادعاء: دراسة حالة لنظام المعلومات والتحليل "المكتب الإلكتروني للمدعي العام"

العملات الرقمية: رحلة البحث عن حلول

68 **أولغا تيسن**
التنظيم القانوني لتداول الأصول الافتراضية ومكافحة استخدامها لأغراض غسل الأموال وتمويل الإرهاب في بلدان محددة من مجموعة العمل الأوراسية

73 **ديمتري سيرغيفيتش ماتشيخين**
تحقيقات AML في قطاع Web-3

77 **شون منير**
إدارة الأصول الرقمية: العملات المشفرة، والرموز غير القابلة للاستبدال (NFT)، وتعزيز الأمن المالي

منبر الشباب

80 **صوفيا رودكوفيتش -**
الحتمية القانونية لتنظيم عمل مقدمي خدمات الأصول الافتراضية في مجال مكافحة غسل الأموال وتمويل الإرهاب على الصعيد الدولي

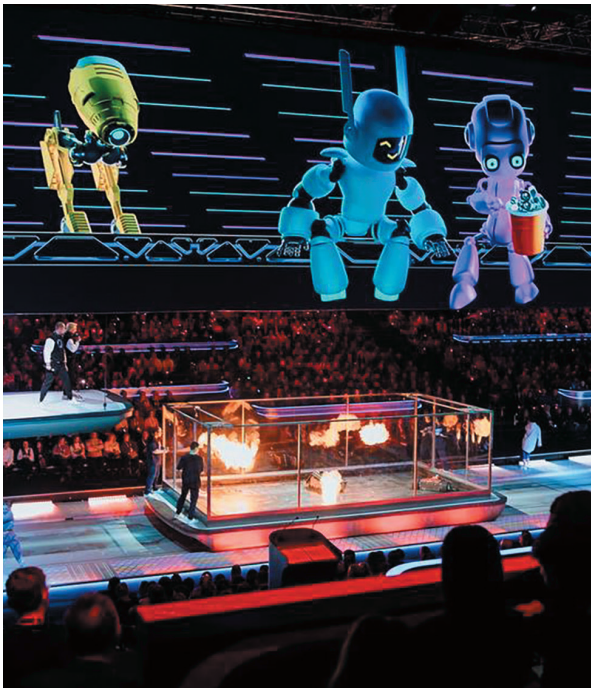
أخبار نظام مكافحة غسل الأموال

84 "ألعاب المستقبل". الفائزون في بطولة "كأس القارات الأربع" يتوافدون على قازان

85 الاجتماع الأول لمجلس بريكس لمكافحة غسل الأموال وتمويل الإرهاب ينعقد بمشاركة واسعة

85 قضايا الأمن المالي أصبحت محورًا للنقاش في مهرجان الشباب العالمي

68 **أولغا تيسن**
التنظيم القانوني لتداول الأصول الافتراضية ومكافحة استخدامها لأغراض غسل الأموال وتمويل الإرهاب في بلدان محددة من مجموعة العمل الأوراسية



84 "ألعاب المستقبل". الفائزون في بطولة "كأس القارات الأربع" يتوافدون على قازان

تحية طيبة لقراء مجلة "الأمن المالي"

غ. يا. كراسنيكوف
رئيس الأكاديمية الروسية للعلوم
أستاذ بأكاديمية العلوم الروسية

القراء الأعزاء!

تحتفل الأكاديمية الروسية للعلوم هذا العام بمرور 300 عام على تأسيسها. وبمناسبة هذه الذكرى السنوية الهامة، لا نستذكر فقط صفحات المجد في تاريخ العلم الوطني، بل نتطلع أيضًا بثقة إلى ما يخبئه المستقبل. يبذل علماؤنا قصارى جهودهم في سبيل معالجة المسائل المرتبطة بتوطيد السيادة العلمية والتكنولوجية لروسيا، ويحرزون تقدمًا ملحوظًا في أرقى مجالات المعرفة العلمية.

من المهم أن نُشير إلى أننا اليوم أمام مشهد مُذهل للتقدم العلمي والتكنولوجي الذي يُلقي بظلاله على عالمنا المألوف ويُغيّر ملامحه. ويتبوّأ التثقيف مكانة محورية في سياق تبنّي التكنولوجيا الحديثة، مع الاستفادة من خبرات فريقنا من المطورين والباحثين.

ويُعدّ تركيز مجلة "الأمن المالي" على جمهورٍ عريض يتجاوز المختصين في المجال ميزةً هامّةً في هذا الصدد. ويُتيح هذا العمل أيضًا لجمهور واسع من القراء استكشاف الموضوعات الأكثر تعقيدًا ذات الصلة بالأمن السيبراني، والتعرف على إمكانيات استخدام الذكاء الاصطناعي في القطاع المالي، فضلاً عن المخاطر التي ينطوي عليها تطبيقه على نطاق واسع.

أؤمن إيمانًا راسخًا بأنّ قراء هذه المجلة سيجدون على صفحاتها مقالات لكبار الباحثين والخبراء، من داخل البلاد وخارجها، بالإضافة إلى ممثلي السلطات الحكومية، كما ستُتيح لهم المجلة فرصة فهم مسار تطوّر عمليات التحول الرقمي للاقتصاد والمالية في المستقبل بشكل أوضح.

أتمنى لكم دوام الصحة والتوفيق في تحقيق المزيد من الإنجازات الرائعة، وكل التمنيات الطيبة.

التكنولوجيا المتقدمة في خدمة الأمان المالي

8 **أنطون ليسيتسين**
مكافحة غسل الأموال وتمويل الإرهاب في عصر التكنولوجيا الرقمية: تحدي العصر

11 **السيد كيشاف أناند**
السيدة م. شانموغا بريا،
التطورات في مجال التكنولوجيا المالية بالهند: التركيز على الابتكار والأمان المالي ومكافحة الجرائم الإلكترونية

15 **السيد يوري كوروتكي**
"المراقبة المالية هي بمثابة تصوير مقطعي مالي"

19 **أوتابيك أوليموفيتش رحمانوف**
آليات تنظيم مكافحة غسل الأموال وتمويل الإرهاب في سوق التكنولوجيا المالية: دراسة حالة أوزبكستان

24 **فيكتوريا كابارتشوك**
يانا بايراشنايا،
ألكسندر كوريانوف
استخدام التكنولوجيا الرقمية في الأنشطة الرقابية وتعزيز كفاءة الجهات الخاضعة للمساءلة

31 **دينارا موسينا**
سجلّ المُستفيدين الفعليين. تجربة كازاخستان

مكافحة غسل الأموال وتمويل الإرهاب في عصر التكنولوجيا الرقمية: تحدي العصر

يبرز دور رقمنة كافة العمليات في المجتمع كعنصرٍ هامٍ في عالمنا المعاصر، حيث تُتيح فرصًا وتُطرح تحدياتٍ جديدةً لمختلف الصناعات وقطاعات الاقتصاد. إذ يشهد العالم ثورة رقمية تقودها تقنيات مثل الإنترنت والتطبيقات المحمولة والحوسبة السحابية والبيانات الضخمة والذكاء الاصطناعي، تفضي إلى إحداث نقلة نوعية في حياة الأفراد، ونماذج عمل الشركات، وتفاعلاتها الداخلية، ووظائف القطاع العام.

أنطون ليسيتسين،
نائب مدير الهيئة الاتحادية للرقابة المالية

كما يشهد القطاع المالي أيضًا تحولات جوهرية مدفوعة بالتطورات الرقمية. وتُتيح الخدمات المصرفية عبر الإنترنت والمدفوعات عبر الهاتف المحمول والمحافظ الرقمية إنجاز المعاملات والمدفوعات المصرفية بشكل أسرع وأسهل، بينما تُقدم تقنية سلاسل الكتل (البلوكشين) والعملات المشفرة فرصًا جديدة لم تكن متاحة من قبل.

وأصبحت الابتكارات والتحول الرقمي تلعب دورًا محوريًا في نهضة الدول في ظل الاقتصاد الرقمي، إذ تُساهم في تكوين قطاعات ووظائف حديثة، ورفع كفاءة الإنتاج، وتحسين مستوى المعيشة. ويُتيح استخدام التقنيات الرقمية في الإدارة الحكومية تبسيط العمليات وأتمتتها، ورفع مستوى إمكانية حصول المواطنين على الخدمات الحكومية، وتعزيز كفاءة وشفافية عمل المؤسسات الحكومية، بالإضافة إلى تمكينها من مواكبة التطورات والتغيرات.

كما يُقدم توظيف تقنيات الذكاء الاصطناعي والأتمتة إمكانيات هائلة لتحسين كفاءة العمليات التجارية ورفع مستوى الأداء في عالم الاقتصاد الرقمي. ويُقدم الذكاء الاصطناعي حلولًا فعّالة لأتمتة المهام المتكررة، وتحليل كميات هائلة من البيانات، واتخاذ القرارات المُستندة إلى الخوارزميات، وتحسين الإنتاجية، ممّا يُتيح آفاقًا جديدة في مجال

تحليل البيانات وتطوير الأنظمة الذكية.

عند الحديث عن رقمنة آليات عمل هيئة الرقابة المالية الفيدرالية، لا يسعنا إلا أن نشير إلى أن مفهوم تطوير نظام المعلومات الموحد لهيئة الرقابة المالية الروسية (روسفينمونيتورينغ) ينص على تنفيذ عدد من المجالات التي يبرر فيها استخدام آليات الذكاء الاصطناعي، ومن المتوقع أن تؤدي هذه الآليات إلى زيادة إنتاجية موظفي الهيئة.

تُمثل البيانات المتراكمة في النظام المعلوماتي للهيئة على مدار سنوات عملها حجمًا كبيرًا من المعلومات الضرورية للقيام بالأنشطة التحليلية.

وفي كثير من الأحيان، تكون البيانات المستمدة من مصادر خارجية متعددة متنوعة غير مُنظمة وغير مُصنفة، مما يستلزم معالجة أو إثراء إضافيًا.

وتُصبح عملية تصنيف البيانات المشار إليها ذات أهمية بالغة عند معالجتها، حيث تُمكن من تحديد هوية الجهات الفاعلة الاقتصادية بهدف الكشف لاحقًا عن مؤشرات الأنشطة غير القانونية، بالإضافة إلى تشكيل مساحة من السمات لتصنيف المخاطر حسب فئاتها.

ومعالجة هذا الكم الهائل من المعلومات أمرٌ لا يمكن تحقيقه دون الاستعانة بتقنيات معالجة البيانات الآلية. وقد طورت هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) ونفذت بنجاح العديد من تقنيات الذكاء الاصطناعي على أرض الواقع، بما في ذلك مكون يسمح بتصميم وتدريب وتطبيق نماذج رياضية لتحليل سلوك المؤسسات الاقتصادية.

ويتضمن هذا المكون نموذجًا للتصنيف قابلًا للتدريب، مما يُمكن من تحديد المؤسسات ذات المؤسسين والمديرين الاسمين أو الأفراد الطبيعيين الاسمين الذين يمارسون غسل الأموال، بالإضافة إلى مؤشرات أخرى على النشاط المشبوه أو غير القانوني من بين ملايين المؤسسات الاقتصادية.

وفي سياق معالجة اللغة الطبيعية، تُستخدم وظيفة التعرف على بيانات الدفع المستخرجة من معالجة الرسائل المنشورة على مواقع التواصل الاجتماعي والتي تُظهر مؤشرات على جمع الأموال لأغراض غير مشروعة.

وعلى نحو مماثل، تجري عملية تحليل المحتوى الروسي على شبكة الإنترنت العالمية. إذ يعمل المكوّن على استخراج الكيانات ذات الصلة لخدمة الرقابة المالية الفيدرالية وتحليلها وتحديد علاقاتها.

تُستخدم البيانات المُستلمة لتوسيع نطاق المعلومات الخاص بهيئة الرقابة المالية الروسية (روسفينمونيتورينغ) من خلال إضافة معلومات جديدة حول المؤسسات.

وفي ظل هيمنة الاقتصاد الرقمي، تُفتح الأبواب على مصراعيها أمام استخراج معلومات ذات قيمة من خلال تحليل الكميات الهائلة من البيانات المُجمّعة والمُخزّنة، ممّا يُعزّز دورها المحوري في عمليّات اتّخاذ القرار، وبناء نماذج جديدة تُبنى على أنماط واتجاهات خفيّة، فضلًا عن تحسين كفاءة سير العمل.

ومن خلال الاستفادة من قدرات تحليل البيانات الضخمة، تُقدم هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) خدمة مبتكرة تتمثل في إنشاء منصة دولية لوحدات الاستخبارات المالية في سبع دول هي: جمهورية أرمينيا، وجمهورية بيلاروسيا، وجمهورية كازاخستان، وجمهورية قيرغيزستان، وروسيا الاتحادية، وجمهورية طاجيكستان، وجمهورية أوزبكستان.

وتتيح المنصة التقنية "المركز الدولي لتقييم المخاطر"، التي أنشأت هيئة الرقابة المالية الروسية داخل رابطة الدول المستقلة، لشركائها توظيف أساليب مبتكرة لتنسيق وتعزيز التعاون الدولي في مجال رصد وتخفيف حدة التهديدات العابرة للحدود، وهو الأمر الذي بات عنصرًا حاسمًا في العمل في ظل التقلبات العالمية.

ويُعدّ إنشاء المركز الدولي لتقييم المخاطر خطوةً حتميةً لمواجهة المخاطر المشتركة التي تواجهها جميع الدول في مجال مكافحة غسل الأموال وتمويل الإرهاب، والحاجة إلى اتباع نهج تعاوني لتقليل هذه المخاطر بشكل فعّال. وتشمل هذه المخاطر، على سبيل المثال لا الحصر، التدفقات المالية المشبوهة العابرة للحدود الوطنية، واستخدام الشركات الوهمية أو أصحاب المشاريع الفردية، وعمليات السحب النقدي، وتجارة المخدرات العابرة للحدود الوطنية، ونقل رأس المال إلى منصات أجنبية عامة لغسل الأموال.

وتتيح عملية دمج المعلومات المتعلقة بالتدفقات المالية لجميع الدول الأعضاء في إطار فضاء معلوماتي موحد إجراء تحليل شامل للعمليات المالية على أراضي رابطة الدول المستقلة، فضلاً عن تهيئة الظروف لتنبؤ فعال بالمخاطر المحتملة بهدف تطبيق تدابير وقائية وإجراءات حمائية مشتركة.

وتتيح المنصة التقنية "المركز الدولي لتقييم المخاطر"، التي أنشأت هيئة الرقابة المالية الروسية داخل رابطة الدول المستقلة، لشركائها توظيف أساليب مبتكرة لتنسيق وتعزيز التعاون الدولي في مجال رصد وتخفيف حدة التهديدات العابرة للحدود، وهو الأمر الذي بات عنصرًا حاسمًا في العمل في ظل التقلبات العالمية.

ومن شأن وجود تصور موحد للمخاطر وتبادل البيانات السريع والمتطور تقنيًا للدول الأعضاء في مجلس رؤساء وحدات الاستخبارات المالية للدول بتطبيق أدوات الاستجابة بفعالية للحد من مستوى التهديدات المشتركة، مع التركيز بشكل مباشر على مكافحة الجريمة وتعزيز التعاون في سياق مكافحة الأنشطة غير القانونية.

وتُشكل عملية تعزيز كفاءة العمل التحليلي لوحدات الاستخبارات المالية من خلال الاستفادة من البيانات التي تتيحها الدول الشريكة عنصرًا جوهريًا في تفاعل الدول على مستوى المركز الدولي لتقييم المخاطر. ومن شأن الحصول على معلومات محدثة حول حالة وتطور المعاملات المالية العابرة للحدود والمخاطر المرتبطة بها في مجال مكافحة غسل الأموال وتمويل الإرهاب سيسمح بإجراء عمليات دولية مستهدفة للوقاية والمكافحة بمشاركة وحدات الاستخبارات المالية وغيرها من الهيئات الوطنية للدول الأعضاء في مجلس رؤساء وحدات الاستخبارات المالية للدول.

ومن العناصر الإضافية التي تُساهم في ضمان الرقابة المالية لحماية المصالح الوطنية للدولة هو "الحزام الوطني للأمن المالي". في هذا السياق، تلعب تقنيات البيانات الضخمة "Big Data" دورًا هامًا في دعم عملية اتخاذ القرار وتوفير الأدوات المنهجية والبرامجية والأجهزة اللازمة لتحسين أنظمة التحكم بشكل نوعي. نظام "الحزام الوطني للأمن المالي" هو نظام يجمع بين مجموعة من الأساليب المنهجية لتنظيم وتحليل المعلومات، وطرق معالجة البيانات، وحلول البرمجيات والأجهزة لتخزين المعلومات والبحث عنها وتصورها.

يؤدي نظام "الحزام الوطني للأمن المالي" الوظائف الرئيسية التالية:

- تحليل البيانات في مجالات مختلفة.
- استكشاف الروابط واكتساب المعارف الجديدة من خلال ربط مجالات الرصد المختلفة.
- الاستفادة من المعلومات المُجمّعة لاتخاذ إجراءات استباقية أو احترازية أو وقائية في الوقت المناسب.

وبشكل أساسي، يُمثل هذا تحليلًا متعدد التخصصات لدراسة الأحداث في نطاقات الرصد المتنوعة. ويوفر هذا التحليل القدرة على تحديد نقاط تركيز المخاطر وعوامل الخطر الجديدة. إنّ دمج مثل هذا النظام في خطوات التخطيط الاستراتيجي يُشكّل قاعدة لاتخاذ إجراءات تهدف إلى خفض المخاطر.

لا بد من التأكيد أيضًا على دور تقنيات سلسلة الكتل (البلوكشين) في إحداث تحول جذري في الطريقة التي تمارس بها الشركات أعمالها وتعزيز الثقة في ظل بيئة الاقتصاد الرقمي. وتُكفل تقنية سلسلة الكتل (البلوكشين) أمان وشفافية المعاملات الرقمية في عالمنا المعاصر. وعلى الرغم من إمكانية الوصول إلى البيانات الأولية (عناوين إرسال واستقبال العملات المشفرة، وقيمة ووقت المعاملة)، إلا أن هذه البيانات تفتقر بشكل عام إلى المعلومات التي تسمح بتحديد هويات الأفراد المشاركين.

وبهدف التصدي لهذه التحديات، تستخدم الخدمة في أنشطتها حاليًا نظام "البلوكشين الشفاف" لتحليل معاملات العملات المشفرة، ويشتمل هذا النظام على آلية لتصنيف مُستخدمي سوق العملات المشفرة، مما يسمح بمتابعة نشاطهم وتتبعه.

ورغم كون "البلوكشين الشفاف" منتجًا حديثًا نسبيًا، إلا أن أكثر من 7 آلاف مستخدم من بين موظفي وكالات إنفاذ القانون الروسية ووحدات الاستخبارات المالية الأجنبية لديهم بالفعل إمكانية الوصول إلى الخدمة. وتملك الخدمة سجلًا حافلًا من الإنجازات في مجال التحقيقات المالية بالتعاون مع وكالات إنفاذ القانون، وقد نفذت الوحدات الهيكلية التابعة للوكالة تحقيقات ناجحة في مجال مكافحة استخدام العملات المشفرة في الأنشطة غير القانونية، وقد أثمرت هذه الجهود عن فتح قضايا جنائية. وتُبذل حاليًا جهود مكثفة لضمان الأداء السلس للخدمة وتطورها الديناميكي، ومن المؤكد أنها ستلعب دورًا محوريًا في النظام البيئي الرقمي لهيئة الرقابة المالية الروسية (روسفينمونيتورينغ).

ومع ازدياد الاعتماد على التقنيات الرقمية وتطورها، تظهر احتياجات جديدة للتعليم والمهارات الضرورية للاندماج بفعالية والتطور المهني في هذا العالم سريع التغير. وبات اكتساب المهارات الرقمية إلى عنصر لا غنى عنه في العملية التعليمية. ويقتضي هذا الأمر مهارة الاستخدام الفعال للتقنيات الرقمية، ومعالجة المعلومات، والتعامل مع البيانات، وتوظيف الأدوات الرقمية لحل المشكلات. كما ينبغي تعزيز مرونة البرامج التعليمية وقدرتها على التكيف لضمان تزويد الطلاب بالمهارات والمعارف المُتطلبة التي تُلبي متطلبات العصر. وتتطلب ضرورة مواكبة التطورات والتغيرات المتسارعة في الاقتصاد الرقمي تحديث المناهج الدراسية وطرق التدريس لضمان تلبية احتياجاته.

وفي ظل هذه الظروف، تُظهر الهيئة اهتمامًا متزايدًا، أكثر من أي وقت مضى، بضمّ موظفين يتمتعون بمستويات عالية من الكفاءة في مجالات تعلم الآلة، وعلم البيانات (Data Science)، وبرمجة بايثون (Python)، وغيرها من المجالات التي تُتيح ضمان التطور المُستدام في العصر الرقمي.

التطورات في مجال التكنولوجيا المالية بالهند: التركيز على الابتكار والأمان المالي ومكافحة الجرائم الإلكترونية

شهد قطاع الخدمات المصرفية الرقمية والجوالة في الهند نموًا هائلًا خلال السنوات الأخيرة. ويعزى هذا النمو إلى مبادرات الحكومة الرامية إلى توسيع نطاق الوصول إلى الخدمات المالية، بالإضافة إلى تطوير البنية التحتية للإنترنت وانتشار الهواتف الذكية بأسعار معقولة على نطاق واسع.

السيد كيشاف أناند
نائب مدير
وحدة الاستخبارات المالية في الهند

السيدة م. شانموغا بريا،
المدير المساعد
وحدة الاستخبارات المالية في الهند

يُعزى النمو السريع لشركات التكنولوجيا المالية الناشئة في الهند إلى تدفق سنوي من المتخصصين التقنيين والخبراء الماليين من خريجي الجامعات والكليات المرموقة، إلى جانب سياسة الحكومة الداعمة للشركات الناشئة والنمو المستدام للناتج المحلي الإجمالي للبلاد. كل ذلك يُشكل نظامًا بيئيًا ديناميكيًا يُرسي القواعد للتطور السريع لشركات التكنولوجيا المالية الناشئة.

لعب اعتماد واجهة الدفع الموحدة (Unified Payments Interface — UPI) دورًا محوريًا في الارتقاء بقطاع التكنولوجيا المالية، إذ تُقدم هذه الخدمة حلولًا مبتكرة للدفع الفوري عبر الهاتف المحمول. شهدت الفترة من يناير 2019 إلى يناير 2024 زيادة هائلة في عدد المعاملات المالية، حيث ارتفع عددها من 672 مليون إلى 12,203 مليون معاملة، بينما ارتفعت قيمة المعاملات من 109,932 كرور روبية هندية (حوالي 15.5 مليار دولار أمريكي) إلى 1,841,084 كرور روبية هندية (حوالي 221.5 مليار دولار أمريكي)[1].

على الرغم من التقدم المحرز في توسيع نطاق الخدمات المالية ليشمل شرائح

[1] https://www.npci.org.in/what-we-do/upi/product-statistics

أوسع من المجتمع، إلا أن تطوير التكنولوجيا المالية قد أدى أيضًا إلى ظهور مخاطر جديدة على الاستقرار المالي. وتُعد الجرائم الإلكترونية المالية مصدر قلق متزايد في ظل تنامي قطاع التكنولوجيا المالية. وتُدرك جميع الأطراف المعنية، بما في ذلك الهيئات التنظيمية وجهات إنفاذ القانون وأجهزة الاستخبارات وممثلي قطاع التكنولوجيا المالية، خطورة هذه المخاطر. واليوم يجري العمل المشترك على التصدي لهذه الجرائم من خلال اتخاذ خطوات للقضاء عليها ورفع مستوى الوعي العام بها.

السرية وإمكانية الوصول عبر الإنترنت وارتفاع معدلات الجرائم الإلكترونية

تُعد السرية التي توفرها التكنولوجيا والإنترنت من أهم العوامل التي تُعزز ازدياد جرائم الإنترنت المالية. وبات بإمكان أي شخص، حتى ذاك الذي لا يملك سوى مهارات تقنية بسيطة، جني الأموال بطرق غير مشروعة دون الحاجة للخروج من منزله. وعلى الرغم من اتخاذ تدابير قوية للأمن السيبراني، إلا أن بعض الثغرات الأمنية لا تزال موجودة في الأنظمة، مما قد يُعطي المجرمين فرصة لاستغلالها. وتستغل الهجمات الإلكترونية هذه الثغرات، بينما تُتيح المراقبة الخفية اكتشاف مثل هذه الأساليب المُستخدمة في الاختراق. وبفضل سهولة الوصول عبر الشبكة، يُصبح الفضاء الإلكتروني أداةً للعمل على المستوى العالمي دون أي عوائق تذكر.

المخاطر التي تهدد الاستقرار المالي

وكشف تقييم وطني للمخاطر في الهند، تم إجراؤه في شهر نوفمبر من عام 2022، أن الاحتيال الإلكتروني والثغرات الأمنية في أنظمة الأمن السيبراني تشكل تهديدات جوهرية على الاستقرار المالي. وتُعد هذه المسألة ذات أهمية جوهرية فيما يتعلق بالمعاملات المصرفية، والإقراض، وعمليات الدفع، والأوراق المالية، وأسواق النقد. ولا يقتصر تأثير الاحتيال الإلكتروني على الإضرار بسمعة البنوك فحسب، بل يخلق أيضًا مجموعة من المخاطر، تشمل: اضطرابات في العمليات التشغيلية والحد من الموارد والخسائر المالية ومشاكل في السيولة. وأصبح التصاعد المُقلق لعمليات الاحتيال الإلكتروني في الآونة الأخيرة يُشكل خطرًا جسيمًا على القطاع المالي من ناحية الثغرات في منظومة مكافحة غسل الأموال.

تزايد حالات الاحتيال المالي: أبرز اتجاهات الجرائم الإلكترونية

أظهر تقرير I4C للربع الثاني[2] من عام 2022، الذي نشرته مجلة Cyber Pravaha، ارتفاعًا ملحوظًا في عدد جرائم الإنترنت المُسجلة على البوابة الوطنية لتسجيل جرائم الإنترنت في الهند (NCRP)، فقد ارتفع عدد الجرائم إلى 237,658 جريمة، مقارنة بـ 97,179 جريمة تم تسجيلها خلال نفس الفترة من العام السابق. وتتصدر جرائم الاحتيال المالي عبر الإنترنت قائمة جرائم الإنترنت، حيث تشكل 67,9% من جميع جرائم الإنترنت المسجلة. وسجلت منصة UPI أكبر قفزة في حالات الاحتيال مقارنة بغيرها من منصات الدفع، حيث ارتفعت من 18,864 إلى 84,145 في الربع الثاني مقارنة بالعام السابق. بالإضافة إلى ذلك، شهدت نفس الفترة زيادة كبيرة في حالات الاحتيال التي استهدفت بطاقات الخصم والائتمان، من 8,628 إلى 26,793 حالة، كما ازدادت الشكاوى المتعلقة بالاحتيال في مجال الخدمات المصرفية عبر الإنترنت، من 5,104 إلى 19,267 شكوى.

التحليل الاستراتيجي للمعلومات الاستخبارية

قام فريق التحليل الاستراتيجي التابع لوحدة الاستخبارات المالية في الهند بإجراء مراجعة شاملة للبلاغات المتعلقة بالمعاملات المشبوهة المرتبطة بالجرائم الإلكترونية التي تم تلقيها خلال الفترة من أبريل 2018 إلى ديسمبر 2022. وشهدت هذه الرسائل زيادة ملحوظة في عددها، حيث ارتفع بمعدل 12 مرة. الأنواع الرئيسية للجرائم الإلكترونية هي عمليات الاحتيال التي تستهدف بطاقات الائتمان، والتصيد الاحتيالي، وعمليات احتيال التوظيف، وسرقة البيانات الشخصية، والتطبيقات المزيفة لبطاقات الائتمان/الألعاب/المقامرة.

ولغرض الكشف عن الأفراد والشركات المتورطين في الجرائم الإلكترونية مع إخضاعهم لعملية فحص مُفصلة، تم وضع منهجية جديدة تستند إلى تقييم المخاطر. يُراعي هذا الأسلوب تنوع الجهات المشاركة في الإبلاغ عن العمليات المشبوهة، وتواتر هذه البلاغات، وأنواع الجرائم الأولية التي تُركز عليها.

بالإضافة إلى ذلك، تم اتخاذ إجراءات وقائية وتشغيلية بناءً على التحليل المكاني لتحديد بؤر الجرائم الإلكترونية والقضاء عليها.

وقد وضعت خطط عمل مُفصلة للتصدي لخطر مجموعات الجريمة الإلكترونية ذات المخاطر العالية، وذلك اعتمادًا على نتائج التحليل الاستراتيجي وتقييم المخاطر. تشمل هذه الأنشطة تحليل سلوكيات مجموعات الجريمة الإلكترونية، وتدريب مختلف الجهات على كيفية التعامل مع هذه الجرائم، والتواصل مع المبلغين لجمع المعلومات وتحسين الاستراتيجيات، وتطوير خطط مكافحة غسل الأموال عبر الإنترنت في ظل ازدياد حالات الجرائم الإلكترونية.

[2] المركز الهندي لتنسيق مكافحة الجرائم الإلكترونية (I4C)، وهو مركز متخصص أنشأته وزارة الداخلية الهندية لتنسيق جهود مكافحة الجرائم الإلكترونية.

التدابير الرامية إلى الحد من المخاطر

تلعب عملية مراقبة الممارسات الاحتيالية التي تقوم بها وحدة الاستخبارات المالية الهندية بالتعاون مع جهات إنفاذ القانون والمؤسسات المالية دورًا هامًا في مكافحة الجرائم الإلكترونية وغسل الأموال. وقد قامت مجموعة عمل متخصصة بتطوير وتطبيق ما يُعرف باسم - "الأعلام الحمراء" وهي مؤشرات نموذجية لعمليات الاحتيال الإلكتروني. مع التركيز بشكل رئيسي على إبراز خطورة العمليات الاحتيالية والأنظمة المُستخدمة في التطبيقات الاحتيالية المختلفة، بما في ذلك تلك المتعلقة بالقروض، والمراهنات، وألعاب القمار، والاستثمارات، والتوظيف، والمواعدات. وتمّ تعزيز الإجراءات الوقائية لتشمل مراقبة مخاطر التطبيقات، وتعديل إجراءات التحقق الأمني، والتحقق من عناوين IP والبيانات الجغرافية لضمان مكافحة هذه الجرائم بفعالية أكبر.

تُجري وحدة الاستخبارات المالية في الهند، بالتعاون مع الجهات المبلغة، مراقبة مستمرة ودقيقة للتطبيقات والمواقع ومنصات التواصل الاجتماعي التي تُعرف بتهديدها للسلامة العامة، وذلك من خلال استخدام أساليب متنوعة للجرائم الإلكترونية. وتنشر المعلومات التي تم جمعها بفضل هذه التدابير بين المؤسسات المشاركة، ووكالات الاستخبارات الأخرى، وأجهزة إنفاذ القانون، بهدف تحليلها واستخدامها لاتخاذ خطوات لاحقة. علاوة على ذلك، يُساهم تحليل الاستراتيجيات الحديثة للجرائم الإلكترونية في تعزيز الوعي لدى عامة الناس، ومساعدة المؤسسات المُبلغة على رصد مثل هذه الممارسات غير القانونية والتعامل معها من خلال أنظمة مكافحة غسل الأموال المُطبقة لديها.

وسعيًا منه لخفض المخاطر، اتخذ بنك الاحتياطي الهندي (RBI) سلسلة من الإجراءات للحد من المخاطر وأصدر توصيات للبنوك لمكافحة الاحتيال والجرائم الإلكترونية. وتُحدّد التوصيات الخاصة أيضًا بشكل دقيق الأساليب التي يستخدمها المحتالون، بما في ذلك الهجمات على الحسابات المصرفية ومحافظ الأدوات المدفوعة مسبقًا (Prepaid Instrument - PPI). وتُلزم البنوك باتخاذ إجراءات فورية لحل هذه المشكلات من خلال تقييم أساليب الاحتيال ووضع استراتيجيات لإصلاح الثغرات الأمنية المُكتشفة.

كما أصدر بنك الاحتياطي الهندي (RBI) مبادئ توجيهية للبنوك لمكافحة الاحتيال والجرائم الإلكترونية في مجالات عمليات الاحتيال الاستثمارية وعروض العمل بدوام جزئي والخطط المالية الاحتيالية (المعروفة باسم - "المخططات الهرمية"). ويشدد بنك الاحتياطي الهندي (RBI) على الحاجة إلى ما يلي: (أ) إنشاء نظام موثوق به

أنشأت وحدة الاستخبارات المالية الهندية، بالتعاون مع بنك الاحتياطي الهندي (Reserve Bank of India — RBI) وعدد من البنوك الأخرى، فريق عمل لمكافحة حسابات المُتواطئين في الاحتيال التي يستخدمها مجرمو الإنترنت في أنشطتهم غير المشروعة. وتمت صياغة مجموعة من التوصيات أهمها:

1. توحيد عملية الكشف عن حسابات المُتواطئين في الاحتيال وحضرها من خلال تقييم المخاطر وإجراءات التحقق من المصداقية والتدابير التكنولوجية.
2. تعزيز التواصل بين المؤسسات المالية لقطع الطريق على تحويلات الأموال التي تم الاستيلاء عليها بطريق الاحتيال.
3. توظيف تقنيات التعرف على السلوكيات المشبوهة من خلال القياسات البيومترية لتعزيز كفاءة الكشف عن الجرائم.
4. تصنيف الحسابات حسب مستوى المخاطر.
5. إنشاء نظام لمتابعة الأنشطة المشبوهة على الشبكات التي يستخدمها مجرمو الإنترنت.

للكشف عن الحسابات المُتواطئين في الاحتيال ومراقبتها. (ب) تحسين إجراءات التحقق من هوية العملاء، وإجراءات مكافحة غسل الأموال، بما في ذلك التقييم القانوني الشامل، والتحقق من الهوية، وتحديد المخاطر، والمراقبة في الوقت الفعلي، والتعامل مع الحسابات التي يُشتبه في استخدامها لأغراض غير قانونية. (ج) ضمان المراقبة والرصد الفعالين للمعاملات الرقمية، بما في ذلك المعاملات التي تتم عبر منصة مدفوعات UPI، والإبلاغ عن الأنشطة المشبوهة في وحدة الاستخبارات المالية الهندية، حتى لو كانت هذه العمليات تدار من قبل طرف ثالث من مقدمي الخدمات.

المبادرات المؤسسية لمكافحة الجرائم الإلكترونية

في عام 2019، أنشأت وزارة الشؤون الداخلية الهندية مركز التنسيق الهندي لمكافحة الجرائم الإلكترونية (I4C) ليكون بمثابة مركز لمكافحة الجرائم الإلكترونية. وتوفر البوابة الوطنية للإبلاغ عن الجرائم الإلكترونية إمكانية الإبلاغ عن هذه الجرائم على مدار الساعة، مع التركيز على الجرائم التي تستهدف النساء والأطفال. ويُسهل نظام الإبلاغ عن الجرائم الإلكترونية من قبل المواطنين (Citizen Financial Cyber Fraud Reporting and Management System) اتخاذ إجراءات سريعة ضد المحتالين الإلكترونيين من خلال توفير خط ساخن برقم 1930 لتقديم الشكاوى عبر الإنترنت.

يُمكن للوكالات المختصة بإنفاذ القانون من خلال بوابة CyTrain، الاستفادة من برامج تدريبية متقدمة تُقدم عبر الإنترنت، لتنمية قدراتهم في مجال التحقيقات وملاحقة مرتكبي الجرائم الإلكترونية، تُعزز بوابة CyTrain التعاون بين مختلف الجهات المعنية بمكافحة الجرائم الإلكترونية من خلال مجموعات التنسيق المشتركة، لتوفير جبهة موحدة لمواجهة التهديدات الإلكترونية. ويُقدم المختبر الوطني للتحاليل الجنائية للجرائم الإلكترونية أدوات وخدمات متقدمة في مجال الطب الشرعي الإلكتروني لدعم التحقيقات في جرائم الإنترنت.

ويختص فريق الاستجابة لحوادث الحاسب الآلي (CERT-In) بمعالجة حوادث أمن تكنولوجيا المعلومات وتعزيز تطبيق أفضل الممارسات في هذا المجال. وتُعنى المبادرة الهندية للأمن السيبراني (Cyber Surakshit Bharat) بتعزيز الأمن السيبراني في الهند من خلال توفير برامج تدريبية لموظفي تكنولوجيا المعلومات في القطاع الحكومي على مواجهة التهديدات الإلكترونية ونشر الوعي حول أفضل الممارسات للأمن السيبراني بين أفراد المجتمع من خلال برنامج Cy-berDost.

وعلى هذا النحو تواصل وحدة الاستخبارات المالية الهندية، بالشراكة مع الهيئة التنظيمية المالية والجهات الحكومية الهندية الأخرى المشاركة في مكافحة الجرائم الإلكترونية، جهودها الدؤوبة لمنع الاحتيال الإلكتروني والحد من الخسائر المالية التي يتسبب بها المحتالون الإلكترونيون. وبفضل التعاون الوثيق بين وحدة الاستخبارات المالية الهندية ونظيراتها من وحدات الاستخبارات المالية في الدول الأخرى والهيئات المُختصة، تمّ إحباط عمليات تحويل الأموال غير القانونية عبر الحسابات المصرفية للمجرمين الإلكترونيين، مما حال دون وقوع خسائر مالية للعديد من المواطنين وحافظ على استقرار النظام المالي للبلاد. وبفضل المبادرات الحكومية الهندية لمكافحة الجرائم الإلكترونية، تسير الهند بخطى ثابتة نحو القضاء على هذا الخطر في المستقبل القريب.

وبفضل التعاون الوثيق بين وحدة الاستخبارات المالية الهندية ونظيراتها من وحدات الاستخبارات المالية في الدول الأخرى والهيئات المُختصة، تمّ إحباط عمليات تحويل الأموال غير القانونية عبر الحسابات المصرفية للمجرمين الإلكترونيين، مما حال دون وقوع خسائر مالية للعديد من المواطنين وحافظ على استقرار النظام المالي للبلاد.

السيد يوري كوروتكي:

"المراقبة المالية هي بمثابة تصوير مقطعي مالي"

يستعرض يوري كوروتكي التطورات في أنظمة المعلومات في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)، ونظام تكنولوجيا المعلومات المثالي للمستقبل، والتحديات المتعلقة بالامتثال للعملات الرقمية.

السيد يوري كوروتكي: شخصية بارزة في المجال القانوني، حاصل على شهادة الدكتوراه في القانون، حائز على لقب "أستاذ مُكرم" من روسيا الاتحادية، وله خبرة واسعة ومهارات استثنائية في مكافحة غسل الأموال وتمويل الإرهاب.

التحق يوري كوروتكي بلجنة الرقابة المالية بعد عام واحد من تأسيسها، وعمل في مجال الاستخبارات المالية لمدة 22 عامًا. وتحت إشرافه، تم تحسين مجموعة كبيرة من أدوات التحليل، وتم تصميم وتنفيذ أدوات تحليل جديدة، ووضع منهجية إنشاء عملية إدارة مخاطر مكافحة غسل الأموال وتمويل الإرهاب.

في مقابلة حصرية مع مجلة "الأمن المالي"، كشف يوري كوروتكي النقاب عن كواليس تطوّر نظام تكنولوجيا المعلومات في الاستخبارات المالية الروسية، وناقش فعالية الأساليب المُستخدمة لتحليل المخاطر العالية، وأكد على أهمية تنظيم تداول العملات المشفرة.

السيد يوري كوروتكي، إنّ تفانيكم لأكثر من 20 عامًا لخدمة هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) جعلكم رائدًا بارزًا لأنظمة المعلومات الخاصة بالهيئة. فما هي نقطة انطلاق هذه المسيرة؟

إن أي نظام معلوماتي هو مزيج من ثلاث مكونات: "المعلومات" + "الأجهزة" + "العقول". وباستخدام لغة تقنية المعلومات يُعد هذا موردًا معلوماتيًا ونظامًا برمجيًا معقدًا وأداة تحليلية. عندما بدأت العمل في الهيئة في نوفمبر 2001 (التي كانت تُعرف آنذاك باسم لجنة الرقابة المالية وليس "الهيئة")، كان قد تم تأسيس البنية التحتية الأساسية لنظام جمع المعلومات وتخزينها ومعالجتها، والذي كان يُشار إليه آنذاك باسم "المعلومات" و "الأجهزة". ومن باب الإنصاف،

وستُحاكي أنظمة تكنولوجيا المعلومات في المستقبل تقنية المسح التلقائي متعدد الممرات للبيئة التشغيلية، مستخدمةً كمية هائلة من البيانات وآلاف المؤشرات.

لا بدّ من الإشارة إلى أنّني لست صاحب الفضل في كل هذا الأمر. ولا يسعني هنا إلا أن أشيد بمساهمات رواد نظامنا المعلوماتي المتميزين، مثل ألكسندر إيغوركين، ويوري غريبنشيكوف، وفاليري ماكشين، وغيرهم الكثير.

أما فيما يتعلق بالمكون التحليلي الثالث، فقد كان لي شرف المساهمة فيه بشكل فعلي. وقد بدأ كل شيء بنظام المحاسبة المتخصصة. وفي ذلك الوقت، كانت تُعرف باسم - "نظام إدارة السجلات المُخصص" ونظمت بشكل دقيق الأسباب والمبررات وإجراءات فتح القضايا المتعلقة بالتحقيقات المالية وإنجازها. وهذا يعني أنه جرى وضع خوارزميات محددة لكل خطوة من خطوات العملية التحليلية. وما زال هذا العنصر يحافظ على أهميته حتى الآن، ولم يتعرض لتعديلات جوهرية تُذكر على مدار أكثر من عقدين من الزمن. وقد تغير اسمه بالفعل إلى "عنصر دعم التحقيق المالي".

نُدرك بأنك صاحب منهجية لبناء عملية إدارة مخاطر مكافحة شرعنة الأموال الناتجة عن الأنشطة الإجرامية وتمويل الإرهاب. إذ تُعد عملية تقييم المخاطر في سياقات محددة أحد الأفكار الرئيسية لهذه المنهجية. فما هي مزايا اتباع هذا النهج تحديدًا؟

أودّ أن أضيف أنّه، في رأيي، ليس هذا مجرد ميزة بل هو النهج الوحيد السليم، وذلك لأنّ ما يثير الشكوك ليس العملية بحدّ ذاتها بل الظروف المحيطة بتنفيذها. وبالتالي، لا يمكن تقييم مدى احتمال كون العملية مشبوهة إلا من خلال الظروف المحيطة بها. من وجهة نظري، يُعدّ هذا الاستنتاج بديهيًا. فعلى سبيل المثال، تقييم مدى احتمال كون العملية مشبوهة في مجال الموازنة يتطلب تحليلًا دقيقًا لجوانب العقود الحكومية، وآلية تحديد الأسعار، وخصائص الإجراءات التنافسية، ومبررات اختيار المُورد، وإمكانية وجود ارتباطات مصلحية بين المتعاقد والعميل، إلى جانب العديد من العوامل الأخرى التي تشكل سياق العمليات المتعلقة بإنفاق الموارد المالية.

الاستخبارات المالية هي وكالة تقتضي طبيعة عملها استخدام تقنيات المعلومات المالية الحديثة لمراجعة وتحليل كم هائل من البيانات بشكلٍ متكرر. ما هي الخصائص التي يجب أن يمتلكها النظام حتى يتكيف بسرعة مع التحديات والتهديدات؟ هل تسمح بنية النظام بتحقيق التكيف السريع؟

لا شكّ أنّ قدرة النظام على التأقلم السريع مع الظروف المتبدّلة والاستجابة الفورية للتحديات والتهديدات المتغيرة باستمرار، تُعدّ من أهمّ المتطلبات الأساسية التي يجب أن يتمتع بها النظام. ولكن هذا الشرط وحده لا يكفي. فالنظام الذي يقتصر على هذه القدرات سيبقى عالقًا في حلقة مفرغة من الانخراط في "مطاردة" مستمرة للتحديات والردّ عليها "بعد وقوعها". يجب أن يتنبأ النظام بالأحداث ويتخذ الخطوات اللازمة تجاهها. كيف؟ أعيدك إلى السؤال السابق - حيث يكمن الجواب في السياق. فنحن لا نزال نجهل نوايا المجرم المستقبلية وحتى هويته. وإذ نعي ذلك، فإننا على دراية بالمكان والطريقة التي من المرجح أن يظهر بها. وهنا سأمتنع عن الكشف عن جميع التفاصيل الخاصة بأسرارنا ومؤشرات المخاطر التي نعتمد عليها في تحديد نطاقات المراقبة المُكثّفة، حيث يتم برمجة النظام مسبقًا للتنبؤ بالعلامات والأحداث المحتملة قبل حدوثها، وبالتالي يكون جاهزًا للتعامل معها. إن مباغتة العدوّ من خلال نصب كمين له تُعدّ إجراءً استباقيًا. وهذا لا يمكن تحقيقه إلا من خلال تحليلات استباقية.

ما هي خصائص نظام تكنولوجيا المعلومات المثالي للمستقبل لتعزيز نظام مكافحة غسل الأموال؟

هل تقترح أن نفكر ونحلم؟ لقد لاحظت منذ زمن طويل تشابهًا كبيرًا بين دور نظام الرصد المالي ودور التصوير المقطعي المحوسب في الطب. فمهامهم متطابقة: تشخيص المرض في الوقت المناسب أو التعرف على أعراضه. والمراقبة المالية أشبه بالتصوير المقطعي للوضع المالي. وستُحاكي أنظمة تكنولوجيا المعلومات في المستقبل تقنية المسح التلقائي متعدد الممرات للبيئة التشغيلية، مستخدمةً كمية هائلة من البيانات وآلاف المؤشرات. وستُنتج هذه التقنية نتائج مشابهة لتلك المُستخدمة في المجال الطبي، حيث يتم تقييم الحالة الصحية وتشخيص الأمراض ووضع خطة العلاج. وسيجري كل ذلك بفضل تقنيات الذكاء الاصطناعي. ما رأيك بهذا السيناريو المستقبلي؟

يبدو هذا مثيرًا للاهتمام ومبشرًا. ولكن ما هي الأدوات، في رأيك، الأكثر فائدة لتقييم التهديدات الخارجية والنقاط الضعيفة الداخلية للبلاد؟

باختصار، لا تملك أي أداة بمفردها القدرة على تحقيق ذلك. بل يتطلب الأمر مجموعة من الأدوات ونظامًا تلقائيًا لاختيار الأدوات المُهيأة خصيصًا للتعامل مع أ) نوع التهديد/الثغرة المُكتشفة وب) خصائص مجال الموضوع الذي توجد فيه التهديد/الثغرة.

ما هي الاتجاهات السائدة في مجال تطوير أنظمة تكنولوجيا المعلومات لأغراض المراقبة التي يمكنك تسليط الضوء عليها؟

في ظل النقاشات الدائرة حول التحول الرقمي، برزت مقولة أحد محاضري دورة "قيادة التحول الرقمي" حول إمكانية رقمنة أي شيء، حتى القمامة. لكن مساعينا لتحقيق الرقمنة قد لا تؤدي إلى ما نأمله، بل قد تُفضي إلى فوضى عارمة في المجال الرقمي. وهذا صحيح بلا شك. يجب أن يسبق التحول الرقمي تحول فكري لدى أولئك الذين سيتم رقمنة عملهم. وهنالك مفهومٌ يُطلق عليه اسم - "النضج الرقمي" يُشترط تحقيقه من قبل النظام وعناصره. وتشكل هذه العملية جزءًا لا يتجزأ من الإجراءات المتبعة، ولا يمكن إكمال المهمة دون المرور بها. ولكن من الممكن، بل من الواجب، تسريعها. وفي هذا الوقت بالتحديد، أرى أننا نعيش مرحلة "النضج الرقمي". ولكن ما هي سمات هذه المرحلة؟ وهي تتمثل بثلاث اتجاهات جوهرية تمّ تثبيتها في مفهومنا، وهنا لا أقدم أي أفكار جديدة:

- فهم وتشكيل بنية مجال تطبيقات مكافحة شرعنة الأموال الناتجة عن الأنشطة الإجرامية وتمويل الإرهاب (علم المفاهيم).
- المنهج العملي وهو وصف تفصيلي خطوة بخطوة لعملية تحقيق النتائج النهائية والمؤشرات المستهدفة للكفاءة.
- الانتقال من تكنولوجيا إدارة البيانات إلى تكنولوجيا استخلاص المعرفة وإدارتها.

التحول من طريقة "توسيع حدقة العين" إلى الأتمتة: في رأيك، ما هي الطرق الحديثة لتحليل العمليات عالية المخاطر التي أثبتت فعاليتها؟

نتذكر بابتسامة ساخرة أسلوب "توسيع حدقة العين" الذي استخدمناه في بداية تحليل سيل الرسائل الواردة. وبالتالي، فإن المبدأ الأساسي ظل على حاله دون تغيير. إذ تُشكل مؤشرات المخاطر العمود الفقري لعملنا، سواءً في الماضي قبل 20 عامًا أو الحاضر. في السابق، كانت الاستجابة لهذه المخاطر تعتمد على ملاحظة المحللين، بينما توفر التقنيات الحاسوبية الآن أدوات أكثر دقة، حيث لا تكتفي بتلقي إشارات التحذير من المخاطر فحسب، بل تسمح بقياس النقاط وتحديد مناطق ذات مستويات مختلفة من المخاطر (ما يُعرف باسم - "إشارات المرور")، وإنشاء خرائط حرارية توضح الوضع التشغيلي بشكل دقيق مع إبراز العوامل التي تشكل "المناطق الحمراء". وعلى الرغم من أن "مصفوفة المخاطر" التي صممناها لم تُطبق بشكل كامل بعد في ممارسات التحليل الظرفي والتقييم الوطني للمخاطر، ولكنني على يقين من أنها تمثل مستقبل هذا المجال، وأنها تُتيح مجالًا واسعًا لتطبيق الذكاء الاصطناعي.

تواصل هيئة الرقابة المالية الروسية (روسفينمونتورينغ) مساعيها في تعزيز التعاون مع الدول الصديقة وتوسيع آفاقه على الصعيد الدولي. مع اختلاف أنظمة تكنولوجيا المعلومات في أجهزة الاستخبارات المالية، ما هي الآليات الأساسية لبناء التعاون، بما في ذلك مع المنتجات التقنية الجديدة، في ظل الخصوصيات الوطنية؟ وهل يمكن الاستفادة من تكنولوجيا المعلومات كأداة لتعزيز التعاون وتبادل المعلومات؟

وعلى الرغم من أن "مصفوفة المخاطر" التي صممناها لم تُطبق بشكل كامل بعد في ممارسات التحليل الظرفي والتقييم الوطني للمخاطر، ولكنني على يقين من أنها تمثل مستقبل هذا المجال، وأنها تُتيح مجالًا واسعًا لتطبيق الذكاء الاصطناعي.

نتبع هنا تسلسلًا محددًا، حيث يتم أولاً تطوير خوارزميات العمل المشترك، وبالتزامن مع ذلك يتم وضع الأساس التنظيمي لها، وأخيرًا يتم ربط مشاريع

تكنولوجيا المعلومات المشتركة. لذلك، في هذه الحالة، يكون وجود الإرادة والعمل الجماعي أمرًا بالغ الأهمية. وبمجرد وضع هذا الأساس، سيستمر مهندسو تكنولوجيا المعلومات في "تحقيق الإنجازات". وتُشكل مسائل تكييف ودمج الأنظمة المختلفة تحديات تقنية معقدة، إلا أنها قابلة للحل بشكل كامل. ويُعدّ تشكيل مساحة تشغيلية موحدة واعتماد نهج مشترك لإدارتها أمرًا بالغ الأهمية.

ما هي رؤيتكم لتطور ممارسات الامتثال في ظل الحاجة إلى تنظيم الأصول الرقمية؟

يُترجم مصطلح "Compliance" بجملة - "الالتزام بالقواعد". وعليه، فإن تطوير نظام الامتثال في مجال تداول الأصول الرقمية يعتمد بشكل مباشر على سرعة إرساء نظام تنظيمي شامل لسوق العملات المشفرة. في المرحلة الحالية، حيث يقتصر عمل الامتثال على نطاق تداول العملات الورقية فقط، يجب علينا استكمال نظام الرقابة الداخلية الحالي بأساليب وأدوات لكشف "الروابط" بين العمليات المصرفية للعملاء ومعاملاتهم بالعملات المشفرة. ولكي نفهم بشكل كامل طبيعة نقاط الالتقاء بين نظامين تشغيليين مختلفين: النظام المالي التقليدي ونظام العملات المشفرة، من الضروري إتقان مهارات التعرف على "المُتواطئين في الاحتيال" ومدفوعات P2P وغيرها من نقاط الالتقاء بين هذين النظامين. وتقع هذه المشكلة بالتحديد ضمن اهتماماتنا الآن، ونعمل على معالجتها بتكليف من رئيس روسيا الاتحادية، في إطار مشروع "البلوكشين الشفاف".

أما فيما يتعلق بآفاق تنظيم سوق العملات المشفرة المحلية، فأنا على قناعة تامة بأنّه يجب تجنب نهج "إقصاء" المعاملات الرقمية ودفعها إلى السوق السوداء، بل على العكس من ذلك يجب اتباع نهج يهدف إلى تعزيز شفافيتها. ويمثل مجال الوساطة في العملات المشفرة الاتجاه الثاني المهم. ويتطلب هذا الأمر استبدال مزودي خدمات الأصول الافتراضية الأجانب ببدائل وطنية، وإنشاء سوق محلي لخدمات العملات المشفرة مع نظام امتثال خاص به للعملات الرقمية. بالإضافة إلى ذلك، يتمتع فريقنا بخبرة واسعة في "دمج" شركات تكنولوجيا المعلومات الأجنبية الكبرى في السوق الروسية، مع ضمان امتثالها التام للقوانين واللوائح المحلية، بما في ذلك القوانين الضريبية ومكافحة غسل الأموال. ومن الضروري تعميم هذه التجربة على مزودي خدمات الأصول الافتراضية غير المقيمين. إن عدم خضوع شركات تبادل العملات المشفرة الأجنبية العاملة في روسيا للرقابة، وبالتالي بقائها خارج نطاق الولاية القضائية الروسية، ووجودها عمليًا في منطقة "ثغرات تنظيمية" - يطرح مخاطر أكبر بكثير من تلك المرتبطة بالعملات المشفرة نفسها. وتُواجه عملية سدّ هذه "الثغرات" تباطؤًا مقلقًا.

أما فيما يتعلق بآفاق تنظيم سوق العملات المشفرة المحلية، فأنا على قناعة تامة بأنّه يجب تجنب نهج "إقصاء" المعاملات الرقمية ودفعها إلى السوق السوداء، بل على العكس من ذلك يجب اتباع نهج يهدف إلى تعزيز شفافيتها.

آليات تنظيم مكافحة غسل الأموال وتمويل الإرهاب في سوق التكنولوجيا المالية: دراسة حالة أوزبكستان

أوتابيك أوليموفيتش رحمانوف -
نائب رئيس إدارة البنك المركزي
لجمهورية أوزبكستان

يبلغ عدد سكان أوزبكستان 36.5 مليون نسمة، ويتميز بوجود شريحة شبابية واسعة تتراوح أعمارها بين 15 عامًا وما فوق، حيث يصل عددهم إلى 25 مليون نسمة. ويُؤسس ذلك قاعدةً محتملةً لتوسيع نطاق استخدام التكنولوجيا المالية، نظرًا لميول الشباب إلى تبني الحلول الرقمية الجديدة.

نظرة عامة على سوق التكنولوجيا المالية - الجهات الفاعلة

يوجد في السوق 35 بنكًا موزعة على 2510 فرعًا ومكتبًا لتقديم الخدمات المصرفية. ويضمن ذلك انتشارًا واسعًا للخدمات المالية في جميع أنحاء البلاد، مما يجعلها متاحة بسهولة لجميع السكان.

كما يوجد في أوزبكستان 49 مؤسسة دفع مرخصة، مما يدل على تنوع الخيارات المتاحة للمستهلكين فيما يتعلق بالخدمات المالية. فضلاً عن ذلك، يوجد 12 نظامًا للمال الإلكتروني و6 أنظمة دفع، ممّا يُساهم في تنوع السوق وازدياد التنافسية فيه.

ويعمل في السوق ثلاثة مشغلين لأنظمة الدفع، يوفرون البنية التحتية لإجراء التحويلات المالية وتنفيذ المعاملات بفعالية.

وتُظهر هذه البيانات دورًا هامًا للقطاع المالي في أوزبكستان، حيث تُبيّن امتلاك البلاد لبنية تحتية متطورة تُمكّن من تنفيذ مختلف المعاملات المالية، الأمر الذي يُشكل بدوره أرضية خصبة لازدهار التكنولوجيا المالية.

نظرة عامة على سوق التكنولوجيا المالية - مجالات التطبيق

تُشير الإحصائيات إلى وجود أكثر من 427 ألف نقطة بيع (POS) في البلاد، وهو رقم هائل يُظهر انتشارًا واسعًا لأنظمة الدفع غير النقدي في المتاجر ولدى مقدمي الخدمات.

وتُفوق أعداد أجهزة الصراف الآلي وأكشاك المعلومات 24 ألف جهاز. ويُظهر ذلك مستوى عالٍ من سهولة

الوصول إلى الخدمات المالية للسكان، نظرًا لتواجد هذه الأجهزة بكثافة في كل من الفروع المصرفية والمواقع العامة.

ويبلغ عدد بطاقات الدفع المتداولة 42.4 مليون بطاقة، مما يُشير إلى شيوع استخدام وسائل الدفع الإلكترونية في جميع أنحاء البلاد. ويُسهل هذا الأمر على المستهلكين استخدام الخدمات ويُشجع على استخدام المدفوعات الإلكترونية.

وتُشكل البطاقات الصادرة عن أنظمة الدفع الدولية، مثل Visa وUnionPay و Mastercard، ما مجموعه 6.7 مليون بطاقة من إجمالي عدد البطاقات المصرفية. ويعكس هذا التطور اندماج المنظومة المالية الأوزبكية في النسيج الاقتصادي العالمي، ويفتح آفاقًا جديدة لإجراء المعاملات الدولية على مستوى الأفراد والشركات.

وعليه، فإنّ أدوات التكنولوجيا المالية في أوزبكستان تتمتع بمجموعة واسعة من الإمكانيات وتُتيح تقديم خدمات متنوعة على الصعيدين المحلي والدولي.

سوق التكنولوجيا المالية - الضوابط التنظيمية

تعتمد أوزبكستان على إطار تشريعي وقواعدي شامل لتنظيم سوق التكنولوجيا المالية، تركز على تعزيز الأمن المالي ومكافحة الأنشطة غير المشروعة. ويُعتبر قانون جمهورية أوزبكستان رقم II-660 "مكافحة عملية شرعنة الأموال المتحصل عليها من الأنشطة الإجرامية وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل" الصادر في 26 أغسطس 2004، أحد أهمّ النصوص القانونية في هذا المجال. يُنظم هذا القانون الإجراءات الأساسية لمكافحة الجرائم المالية ويحدد المسؤولية عن ارتكابها.

وقد أقرّ مجلس الوزراء خطوات إضافية لتنفيذ القانون المذكور بقراره رقم 402 بتاريخ 29 يونيو 2021، ممّا يُؤكّد على حرص الحكومة على تعزيز منظومة التشريعات في هذا المجال. وتشمل هذه التدابير أحكامًا وتعليمات محددة لمكافحة فعالة لعمليات غسل الأموال وتمويل الإرهاب وانتشار أسلحة الدمار الشامل.

وتلعب قواعد الرقابة الداخلية، التي يضعها البنك المركزي ووحدة الاستخبارات المالية، دورًا هامًا في تنظيم القطاع المالي. وهذه القواعد مخصصة لتنظيم عمل المؤسسات المالية، بما في ذلك المصارف، وشركات تشغيل أنظمة الدفع، وشركات أنظمة النقود الإلكترونية، ومؤسسات الدفع، وتهدف إلى تعزيز تدابير مكافحة الجرائم المالية.

وحرصًا على تعزيز أمان المعاملات وتعزيز التعرّف على هوية العملاء، تمّ إصدار "تعليمات تنظيمية حول إجراءات التعرف الرقمي على هوية العملاء" بموجب قرار البنك المركزي رقم 3322 الصادر في 30 سبتمبر 2021. ويُمكن من خلال ذلك التحقق من هوية العملاء بشكل فعّال في بيئة الإنترنت وبالتالي الحد من مخاطر الاحتيال المالي.

التقنيات المالية المبتكرة - خطوات دمجها في الممارسات التجارية.

يُمثل دمج التقنيات المالية الجديدة في الممارسات التجارية عملية متعددة الخطوات تستلزم تقييمًا دقيقًا وتدابير وقائية لضمان سلامة وكفاءة المعاملات.

المرحلة الأولى: تُعرف بمرحلة استكشاف المنتج، وتشمل دراسة متعمقة لمكوناته الوظيفية، وإمكانياته، وفوائده المحتملة للشركة والعملاء. يلي ذلك تحديد المخاطر والتهديدات والثغرات المرتبطة بالمنتج الجديد للحصول على رؤية واضحة للعواقب السلبية المحتملة لاستخدامه.

تُجرى بعد ذلك عملية تحليل المخاطر، والتي تتضمن تقييم احتمالية ظهور مخاطر مختلفة وتأثيرها السلبي المحتمل على الأعمال التجارية والعملاء. ووفقًا لنتائج التحليل، يتم صياغة استراتيجيات لتقليل المخاطر، والتي قد تتضمن تحسينات في المنتج أو في آليات استخدامه أو في قواعد الأمان الخاصة بالشركة.

ويُعدّ إخطار البنك المركزي خطوة أساسية قبل طرح أي منتج جديد. وهذا الأمر ضروري لضمان الامتثال للقوانين والأنظمة المنظمة للسوق المالي. وعقب إبلاغه، يجوز للبنك المركزي إجراء تقييم مستقل للمنتج وتقديم مقترحات لتعزيزه أو فرض إجراءات وقائية إضافية.

وبمجرد استكمال إجراءات الحصول على التوصيات والموافقة من جانب البنك المركزي، يتم البدء في طرح المنتج الجديد في السوق. ومع ذلك، لا تنتهي العملية عند هذا الحد. بل يتم إجراء تقييم دوري للمخاطر المرتبطة بالمنتجات السابقة والحالية على الأقل مرة واحدة في السنة، وذلك في إطار مكافحة غسل الأموال وتمويل الإرهاب. يُتيح هذا النهج الاستجابة السريعة للتغيرات في البيئة من خلال إجراء التعديلات اللازمة على استراتيجيات الأمن وإدارة المخاطر.

التقنيات المالية - حلول التحقق الرقمي من الهوية

تضطلع التقنيات المالية بدور محوري في تأمين سلامة وفاعلية العمليات المالية، ويُعدّ التحقق الرقمي من الهوية أحد المكونات الجوهرية لهذه العملية. وقد طورت أوزبكستان حلولًا وطنية للتحقق الرقمي من الهوية، تتيح إمكانية إجراء عمليات التعرف على الهوية فقط للأفراد المقيمين في أراضيها.

ويعتبر كشف الحيوية (Liveness Detection) من بين أهم الآليات

المستخدمة في التحقق الرقمي من الهوية. إذ توفر هذه الآلية الحماية ضد انتحال الشخصية من خلال استخدام شبكات عصبونية عميقة ومدربة لتحديد ما إذا كان الشخص المحدد في الصورة مستخدمًا "حقيقيًا".

ومن الجوانب الهامة الأخرى هناك تقنية التعرف على الوجه (Face Recognition)، والتي تُمكّن من مقارنة صورة وجه واحد مع جميع صور الوجوه الموجودة في قاعدة البيانات. وتُتيح هذه الطريقة تحديد هوية شخص واحد من بين مجموعة كبيرة، مما يُحسّن من دقة عملية التعرّف على الهوية.

مُقارنة الوجوه (Face Comparison) وهي أداة هامة أخرى تُستخدم للتحقق من احتمالية أن تنتمي صورتان لشخص واحد. وتُظهر هذه الطريقة فائدتها بشكل خاص عند الحاجة إلى التحقق من هوية شخص ما، وذلك في حال استخدام صور أو رسومات متعددة تمثله.

ويمكن استخدام طرق متنوعة في عملية التحقق الرقمي للهوية، بما في ذلك العمليات الآلية بدون تدخل بشري، والطرق التي تتطلب تدخلًا بشريًا. ويتوجبّ في كلا الحالتين ضمان تحقيق دقة وأمان فائقتين لعملية تحديد الهوية، وذلك بغية حماية مصالح العملاء بشكل فعّال وضمان الامتثال الكامل للمتطلبات التنظيمية المعمول بها.

تقنيات الرقابة المالية - حدود المعاملات المشبوهة.

تضع قواعد الرقابة الداخلية لمكافحة غسل الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل في جمهورية أوزبكستان مجموعة من الشروط والضوابط المُحددة لتصنيف العمليات المالية على أنها مشبوهة. وتهدف هذه القواعد إلى ضمان سلامة المعاملات المالية ومنع استخدامها لأغراض غير قانونية.

ومن بين أهم المؤشرات التي تدل على العمليات المشبوهة في قواعد الرقابة الداخلية لمكافحة غسل الأموال وتمويل الإرهاب في أوزبكستان ما يلي:

- قيام العميل بتحويل الأموال من بطاقة مصرفية إلى بطاقة أو أكثر من بطاقات الائتمان أو المحافظ الإلكترونية باستخدام تطبيق الهاتف المحمول، دفعة واحدة أو بشكل متكرر خلال 30 يومًا كحد أقصى، بشرط أن يبلغ المبلغ الإجمالي 500 ضعف الحد الأدنى لوحدة الحساب الأساسية أو أكثر.
- سحب العميل للأموال من بطاقة بنكية واحدة أو أكثر أو من محافظ إلكترونية على بطاقة بنكية واحدة أو أكثر، بقيمة إجمالية تساوي أو تزيد عن 500 ضعف الحد الأدنى لوحدة الحساب الأساسية، دفعة واحدة أو على فترات متعددة خلال فترة لا تتجاوز 30 يومًا.
- إجراء تحويلات مالية عبر تطبيق الهاتف المحمول من خمس بطاقات مصرفية (أو أكثر) أو محافظ إلكترونية إلى محفظة إلكترونية أجنبية واحدة دفعة واحدة أو على فترات متعددة خلال مدة لا تزيد عن 30 يومًا.
- تلقي تحويلات مالية على 5 أو أكثر من بطاقات مصرفية (محافظ إلكترونية) من محفظة إلكترونية أجنبية واحدة دفعة واحدة أو بشكل متكرر خلال فترة زمنية لا تتجاوز 30 يومًا.
- إجراء تحويلات الأموال من خلال تطبيق الهاتف المحمول من بطاقة مصرفية واحدة (أو محفظة إلكترونية) إلى 5 أو أكثر من البطاقات المصرفية الأجنبية أو المحافظ الإلكترونية دفعة واحدة أو على فترات متعددة خلال مدة لا تزيد عن 30 يومًا.
- تلقي تحويلات مالية من 5 أو أكثر من البطاقات المصرفية أو المحافظ الإلكترونية الأجنبية على بطاقة مصرفية واحدة (محفظة إلكترونية) دفعة واحدة أو بشكل متكرر خلال فترة لا تزيد عن 30 يومًا.

سوق مؤسسات الدفع.

يتسم سوق مؤسسات الدفع في أوزبكستان بمجموعة واسعة من إجراءات وأدوات يتم تبنيها واستخدامها للتقليل من مخاطر المعاملات ذات الصلة بغسل الأموال وتمويل الإرهاب. ومن منطلق الحرص على ضمان أمن واستقرار النظام المالي للبلاد، تعمل مؤسسات الدفع على تبنّي مجموعة واسعة من الأساليب والإجراءات المُتنوّعة بهدف حماية العمليات المالية من المخاطر والتحديات المختلفة.

أنظمة التحقق من هوية العملاء CDD ((Customer Due Diligence واعرف عميلك KYC (Know Your Customer): تُستخدم هذه الأنظمة للتحقق من هوية العملاء والتأكد من امتثالهم للقوانين واللوائح التنظيمية المعمول بها. وتشمل هذه المجموعة نظام e-KYC (نظام إلكتروني للتحقق من هوية العملاء) الذي يسمح بإجراءات تحديد هوية أكثر كفاءة وسرعة.

الأنظمة والإجراءات التشغيلية الداخلية: تضع مؤسسات الدفع أنظمة وإجراءات تشغيلية داخلية لتنظيم تفاعل موظفيها ووكلائها ووكلائها الفرعيين مع العملاء. ويتضمن ذلك تحديد الإجراءات

المتبعة في التعامل مع العملاء ذوي المخاطر العالية، خاصةً أولئك الذين يشغلون مناصب عامة.

أنظمة مراقبة عمليات العملاء: تستخدم مؤسسات الدفع أنظمة مراقبة متخصصة تُعنى بالرصد والتحليل التلقائي لعمليات العملاء بهدف الكشف عن المعاملات المشبوهة.

أنظمة الكشف عن العمليات المشبوهة والإبلاغ عنها: تُوظف مؤسسات الدفع آليات للتعرّف على المعاملات المشبوهة وإبلاغها إلى الجهات الإشرافية والرقابية المعنية.

أنظمة تحليل المخاطر ومراقبتها: تُطبق مؤسسات الدفع بشكل منتظم عمليات تحليل وتقييم ومراقبة شاملة للمخاطر التي تكتنف المعاملات التي تُنفذها. فهي تُطور وتطبق استراتيجيات للتخفيف من مخاطرها بما يتماشى مع التهديدات المُحددة.

صياغة القواعد الداخلية وتحديثها: تقوم مؤسسات الدفع بشكل دوري بمراجعة قواعدها وإجراءاتها الداخلية وتحديثها، وذلك بهدف معالجة المخاطر المُكتشفة والتعامل مع التغييرات الطارئة على الأنظمة والقوانين. ويُمكنّها ذلك من التعامل بفعالية مع التحديات الجديدة ومتطلبات الجهات التنظيمية.

وتُعزّز جميع هذه التدابير والأدوات فعالية عملية مكافحة غسل الأموال وتمويل الإرهاب في القطاع المالي لأوزبكستان، مما يُساهم في ضمان استقرار النظام المالي للبلاد وأمانه.

أنظمة النقود الإلكترونية.

تلعب أنظمة الدفع الإلكتروني دورًا هامًا في البنية التحتية المالية الحديثة لأوزبكستان. ووفقًا لتشريعات البلاد، فإن البنوك هي الجهات الوحيدة المخولة بإصدار النقود الإلكترونية، مما يضمن مستوى إضافيًا من الموثوقية والتحكم في معاملات الدفع الإلكتروني.

ومع ذلك، تجدر الإشارة إلى أنه في بعض الحالات، لا يتم إجراء التحقق المناسب من هوية العملاء. على سبيل المثال، في حال لم تتجاوز قيمة أي معاملة باستخدام النقود الإلكترونية حدًا معينًا (مثل وحدة حسابية أساسية واحدة)، أو إذا ظلت قيمة النقود الإلكترونية في محفظة العميل منخفضة نسبيًا (مثل أقل من 5 وحدات حسابية أساسية). تُفرض هذه القيود بغية تبسيط وتسريع إتمام المعاملات الصغيرة والمتكررة، مع السعي إلى تقليص الأعباء البيروقراطية على العملاء.

وحرصًا على تقليل المخاطر المصاحبة المرتبطة بالمعاملات النقدية الإلكترونية، تم وضع قيود على كل من المعاملات الفردية والحجم الإجمالي للمعاملات خلال فترة زمنية محددة. على سبيل المثال، يُسمح بتحديد الحد الأقصى لمبلغ المعاملة الواحدة باستخدام النقود الإلكترونية، والحد الأقصى لمبلغ النقود الإلكترونية في محفظة العميل، والحد الأقصى لمبلغ معاملات النقود الإلكترونية خلال الشهر، بالإضافة إلى الحد الأقصى لمبلغ المعاملات التي تتم عبر البطاقة المصرفية خلال الشهر. توفر هذه الحدود للبنوك والجهات التنظيمية القدرة على التحكم في المخاطر المحتملة التي ينطوي عليها استخدام النقود الإلكترونية، ممّا يُساهم في ضمان سلامة النظام المالي واستقراره.

الابتكارات في المدفوعات المالية: تقنية الاتصال قريب المدى (NFC)، رموز الاستجابة السريعة (QR)، الدفع عبر الهاتف (Tap-to-phone).

شهدت السنوات الأخيرة ازديادًا ملحوظًا في اعتماد التقنيات المالية الحديثة، مثل تقنية الاتصال قريب المدى (NFC) ورموز الاستجابة السريعة (QR) والدفع عبر الهاتف (Tap-to-phone)، لتُصبح ركائز أساسية في منظومة الدفع العصرية. وبفضل ما توفره من سرعة ومرونة في إتمام المعاملات، أصبحت هذه الطرق هي الوسيلة المُفضلة للدفع لدى العديد من المستخدمين.

وتُعَدّ المدفوعات باستخدام تقنية الاتصال قريب المدى (NFC) من بين أكثر الأساليب انتشارًا للدفع اللاتلامسي. وسجلت العمليات التي تعتمد على هذه التكنولوجيا قفزة نوعية في السنوات الأخيرة، مما يؤكد على انتشارها وتبنيها على نطاق واسع. على سبيل المثال، بلغ حجم العمليات في عام 2021 ما يعادل 12.2 تريليون سوم، بينما ارتفع في عام 2023 ليصل إلى 31.6 تريليون سوم. ومع ذلك، تقع على عاتق المؤسسات المالية مسؤولية الامتثال لمعايير التحقق المناسب من هوية العملاء، خصوصًا في حالات الشك في وجود عمليات مشبوهة. وفي حال تعذر إجراء عملية تدقيق كهذه، تقع على عاتق المؤسسات المالية مسؤولية إبلاغ الجهات الحكومية المختصة بذلك وفسخ تعاملاتها مع العميل.

كما شهدت المدفوعات عبر رموز الاستجابة السريعة (QR) زيادة كبيرة في شعبيتها كوسيلة للدفع الإلكتروني. وشهد حجم المعاملات عبر رموز الاستجابة السريعة (QR) وعددها نموًا ملحوظًا خلال السنوات الماضية.

على سبيل المثال، سجل حجم العمليات في عام 2023 مبلغًا يساوي 315 مليار سوم، بينما وصل عدد المعاملات إلى 93.8 ألف. يُلقي هذا النمو بظلاله على ضرورة تعزيز تدابير الأمن ومكافحة الاحتيال، خاصة فيما يتعلق بغير المقيمين، والشخصيات التي تشغل مناصب عامة، وكذلك العملاء الذين يُمارسون أنشطة مشبوهة.

تتيح تقنية الدفع عبر الهاتف (Tap-to-phone) للمستخدمين تحويل أجهزتهم المحمولة إلى نقاط بيع (POS)، ممّا يُقلّل من التكاليف ويُتيح تجربة دفع أكثر سلاسة. وتبعًا لذلك، بات من الضروري اتخاذ خطوات حازمة للتحقق الدقيق من هوية العملاء. وتشمل هذه العملية الحصول على معلومات حول مصادر الأموال، بالإضافة إلى دراسة الأهداف المخطط لها أو التي قام بها العميل.

وبشكل عام، يُتيح ظهور تقنيات مالية مبتكرة فرصًا جديدة للمستخدمين، لكنه يفرض على المؤسسات المالية مسؤولية دائمة لضمان الأمن والامتثال للقوانين.

تقنيات الدفع الحديثة: الدفع بالوجه (Face pay)، نظام الدفع باستخدام بصمة الإصبع (ATTO)، تقنية الدفع عن طريق مسح راحة اليد (Palm pay).

وفي شهر سبتمبر 2023، تمّ الكشف عن تقنية دفع مبتكرة بدون تلامس، تُمثل نقلة نوعية في مجال التكنولوجيا المالية. تُقدم تقنية الدفع بالوجه (Face pay) طريقة مبتكرة وآمنة لإجراء المدفوعات من خلال الاستفادة من بيانات الوجه البيومترية للشخص. وتعتمد هذه التقنية على كاميرا ذكية تتعرف على السمات المميزة لوجه المستخدم وتقوم تلقائيًا بربطها بالبطاقة المصرفية المرتبطة بالحساب، لضمان أقصى درجات أمان البيانات وحمايتها.

فضلًا عن ذلك، تمّ إدخال حلّ في مجال النقل يحمل اسم ATTO (نظام الدفع باستخدام بصمة الإصبع)، وهو عبارة عن بطاقة بلاستيكية لا تتطلب التلامس تعمل بتقنية الاتصال قريب المدى (NFC). يمكن شراء بطاقات نظام الدفع باستخدام بصمة الإصبع (ATTO) من خلال آلات البيع المخصصة أو نقاط بيع تذاكر النقل، مما يجعلها متاحة لمجموعة واسعة من المستخدمين. وتوفر هذه التقنية إمكانية دفع أجرة النقل من خلال تطبيق الهاتف المحمول، مستخدمةً كلًا من تقنية الاتصال قريب المدى (NFC) ورموز الاستجابة السريعة (QR)، لتقديم تجربة سهلة ومريحة للركاب.

أدخلت المصارف المُبتكرة أنظمة دفع حديثة تعتمد على القياسات الحيوية للوجه وبصمات اليد لتقديم خدماتها للعملاء. على سبيل المثال، تتيح تقنيات الدفع بالوجه (FacePay) والدفع براحة اليد (PalmPay) للعملاء الاستمتاع بتجربة دفع سلسة وآمنة في المؤسسات المصرفية من خلال مسح وجوههم أو راحة أيديهم، مما يُعزز مستوى الأمان ويُقلل من الحاجة إلى استخدام الطرق التقليدية للتحقق من هوية المستخدم. وتتميز طرق الدفع هذه بأهميتها البالغة للعملاء الذين يُفضّلون السهولة والراحة عند إجراء المعاملات المالية.

وبشكل عام، يُتيح ظهور تقنيات مالية مبتكرة فرصًا جديدة للمستخدمين، لكنه يفرض على المؤسسات المالية مسؤولية دائمة لضمان الأمن والامتثال للقوانين.

استخدام التكنولوجيا الرقمية في الأنشطة الرقابية وتعزيز كفاءة الجهات الخاضعة للمساءلة

أصبحت التقنيات الرقمية والحلول الآلية لمعالجة مجموعات البيانات الضخمة جزءًا لا يتجزأ من أنشطة الرقابة في مجال مكافحة شرعنة الأموال الناتجة عن الأنشطة الإجرامية وتمويل الإرهاب، وتنفيذ منهجية قائمة على المخاطر، وتقييم الفعالية، وتعزيز التواصل مع الجهات الخاضعة للمساءلة، وأتمتة بعض العمليات التجارية. وتتمثل أهداف التحول الرقمي في تعزيز سرعة وفعالية التفاعل مع الجهات الخاضعة للمساءلة، وتخفيف العبء الإداري على الشركات، وتحرير موارد أجهزة الرقابة.

فيكتوريا كابارتشوك،
مستشار بإدارة تنظيم الأنشطة الرقابية في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)

يانا بايراشنايا،
خبير أول في إدارة تنظيم الأنشطة الرقابية في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)

ألكسندر كوريانوف،
رئيس إدارة تنظيم الأنشطة الرقابية في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)، دكتوراه في الاقتصاد

وتشير بعض تقديرات الخبراء إلى أن كثافة إدخال تعديلات على القوانين المنظمة للقطاع المالي على مستوى العالم قد ازدادت بأكثر من خمسة أضعاف خلال العقد الماضي. وعلى صعيد آخر، شهدت الفترة الأخيرة ازديادًا ملحوظًا في عدد حالات مساءلة المشاركين في السوق، وباتت الغرامات المفروضة على عدم الامتثال للمتطلبات الإلزامية أكثر شيوعًا وأشد صرامة. تُقدم التكنولوجيا التنظيمية RegTech (Regulatory Technology) أدوات فعالة لتحسين عملية الامتثال للمتطلبات الإلزامية، وذلك في ظل التحديات المتزايدة التي تواجهها الشركات بسبب كثرة القوانين واللوائح والتغييرات التي تطرأ عليها. وتميزت الفترة ما بين عامي 2017 و2019 بموجة من التطورات المتسارعة في مجال التكنولوجيا التنظيمية (RegTech)، مدفوعةً بارتفاع مستوى التدابير التنظيمية وتطور تقنيات الذكاء الاصطناعي بشكل متزامن.

تساهم حلول SupTech (التكنولوجيا الإشرافية) أيضًا في تحسين الامتثال للمتطلبات الإلزامية.

ويسلط الخبراء الضوء على مجموعة من المزايا التي توفرها التكنولوجيا التنظيمية "RegTech" ومنها:

رفع مستوى الأداء

تقنيات تمكن من معالجة كميات هائلة من البيانات بسرعة فائقة، بما في ذلك تحليل النصوص القانونية الخام بسرعة واستخلاص المعلومات الضرورية لأغراض الرقابة.

زيادة الدقة والاكتمال.

تُخلّف العمليات اليدوية غير المُنسّقة عادةً ثغرات في ضمان الامتثال، مما ينتج عنه أخطاء بشرية وارتفاع مخاطر التعرض للمساءلة التنظيمية. إنّ تطبيق التكنولوجيا التنظيمية (RegTech) ودمجها بذكاء يُتيح سدّ تلك الثغرات وتسهيل عملية الامتثال للمتطلبات الإلزامية.

الاتساق والتنسيق الداخلي

توفر الأدوات التكنولوجية قدرًا أكبر من الشفافية لجميع جوانب العمل، من خلال دمج العمليات والأفراد الذين كانوا يعملون بشكل منفصل في الماضي. ونتيجة لذلك، يتم إنشاء بيئة معلوماتية شاملة تربط بين جميع أقسام الشركة. ويُساعد هذا على تبادل البيانات بشكل أسرع، مما يؤدي إلى الارتقاء بمستوى الامتثال للمعايير المطلوبة بشكل كبير.

الإدارة النوعية للمخاطر.

تلعب أدوات التكنولوجيا التنظيمية (RegTech) دورًا هامًا في خفض أنواع مختلفة من المخاطر، مثل إساءة الاستخدام في السوق والهجمات الإلكترونية والاحتيال، وذلك من خلال مراقبة الأنظمة وإبلاغ الموظفين بالأنشطة المشبوهة.

وتلعب حلول التكنولوجيا الإشرافية SupTech (Supervisory Technology) دورًا هامًا في تعزيز الامتثال للمتطلبات الإلزامية.

ويُشير مصطلح التكنولوجيا الإشرافية (SupTech) إلى استخدام الهيئات التنظيمية والرقابية للأدوات الرقمية، بما في ذلك الأجهزة والبرامج، لتحقيق مهامها[1].

وأصبح استخدام تقنيات من هذا النوع ضرورة ملحة، نظرًا للنمو الهائل في حجم البيانات المنظمة وغير المنظمة التي يتم إنشاؤها، مع إمكانية جمعها وتخزينها وتحليلها وتصورها بفعالية. على سبيل المثال، بالإضافة إلى التقارير الرسمية المقدمة من الجهات الخاضعة للمساءلة، تستفيد الوكالات المختصة بشكل كبير من المعلومات المتاحة للجميع (مثل المنشورات على مواقع التواصل الاجتماعي) لتعزيز فهمها للقضايا المطروحة.

وبما أن الجهات التنظيمية والرقابية وجهات إنفاذ القانون تعتمد على البيانات والإجراءات الداخلية وأدوات العمل، فضلاً عن الموارد البشرية والموارد الأخرى، فإنها تواجه جميعًا تحديات مشتركة - وإن كانت بدرجات متفاوتة - تتعلق بجودة البيانات الرديئة والإجراءات اليدوية التي تتطلب جهدًا مكثفًا ووقتًا طويلًا. وتُقدم حلول التكنولوجيا الإشرافية (SupTech) إمكانيات هائلة للجهات المختصة لمعالجة هذه المشكلات بفعالية أكبر، وذلك من خلال تعزيز قدراتها وكفاءتها وفعاليتها في مجالات جمع البيانات وتحليلها، وتشمل هذه الحلول أتمتة المهام المتكررة، وتطوير أساليب تحليلية مبتكرة، وإنشاء معلومات مُعالجة جاهزة للاستخدام.

مع وجود تنوع في الآراء حول نطاق مفهوم التكنولوجيا الإشرافية (SupTech)، إلا أن هذا المصطلح يُستخدم بشكل أساسي للإشارة إلى ممارسات الرقابة التي تُشارك فيها المؤسسات المالية والمتعاملين بسوق الأوراق المالية. وهكذا، تؤكّد منظمة التعاون الاقتصادي والتنمية على دور حلول التكنولوجيا الإشرافية (SupTech) في تعزيز كفاءة الكشف عن جرائم الاتجار الداخلي والتلاعب في السوق، وغيرها من المخالفات.[2]

ويشهد مفهوم التكنولوجيا الإشرافية (SupTech) حاليًا توسعًا في نطاق تطبيقه ليشمل مختلف الجهات الرقابية، بما في ذلك تلك التي تُعنى بمراقبة قواعد المنافسة العادلة وضمان الالتزام بمتطلبات مكافحة الفساد وغيرها. ويُؤكد الخبراء على أن التكنولوجيا الإشرافية (SupTech) تعزز قدرات الجهات المختصة في مجالات الرقابة والتحليل وإنفاذ القانون، ممّا يُساهم بدوره في تحقيق نتائج إيجابية على صعيد الاستقرار المالي ونزاهة السوق ورفاهية المستهلكين.[3]

تُساهم أدوات التكنولوجيا الإشرافية (SupTech) في تمكين الجهات الرقابية من تعزيز قدراتها في جمع البيانات وإدارتها، ممّا يُتيح بدوره تحسين جودة تلك البيانات، ويُشكّل شرطًا أساسيًا لإجراء تحليل مُعمّق للبيانات.

[1] Going Digital: Shaping Policies, Improving Lives / OECD Publishing. URL: Mode of access: https://doi.org/10.1787/9789264312012-en.

[2] Using digital technologies to improve the design and enforcement of public policies // OECD. URL: https://dx.doi.org/10.1787/99b9ba70-en.

[3] The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: https://www.fsb.org/wp-content/uploads/P091020.pdf.

تتيح لنا ممارسة استخدام SupTech تسليط الضوء على المزايا الرئيسية التالية لتنفيذها من قبل السلطات الإشرافية:

تعزيز قدرات كشف المخالفات

تشير البيانات المتاحة إلى أن الجهات الرقابية، بما في ذلك تلك التي تنظم أسواق الأوراق المالية وتضمن الامتثال لقواعد مكافحة الاحتكار، بالإضافة إلى وكالات إنفاذ القانون المشاركة في مكافحة الفساد، تلجأ بشكل متزايد إلى أدوات التكنولوجيا الإشرافية (SupTech) لتحسين قدرتها على اكتشاف الجرائم التالية:

- ممارسات غسل الأموال وتمويل الإرهاب والتداولات غير العادلة وغيرها من الأنشطة غير المشروعة (مثل المبيعات غير القانونية والاحتيال).
- السلوكيات المناهضة للمنافسة.
- أفعال الرشوة والفساد التي تتم في بلدان أخرى.

تلعب تطبيقات التكنولوجيا الإشرافية (SupTech)، وعلى رأسها أدوات الذكاء الاصطناعي، دورًا هامًا في تحقيق هذه الأهداف، وذلك لأنّ الرقابة تستند إلى تحليل كميات هائلة من البيانات المُفصّلة والعاجلة وغير المُنَظّمة المُستقاة من مصادر مُتفرّقة. بالإضافة إلى ذلك، ونظرًا لأنّ التكنولوجيا الرقمية تُتيح المجال لظهور أشكال جديدة من الغسل وتوظيف الأموال، والممارسات غير النزيهة في السوق المالية، والاحتيال، والسلوكيات المناهضة للمنافسة، فإنّه من الضروريّ ابتكار أدوات جديدة للكشف عن هذه الجرائم ومكافحتها.

وتلعب أدوات الذكاء الاصطناعي دورًا هامًا في عمل وحدات الاستخبارات المالية من خلال تحليل البيانات الواردة: فرز المعلومات المدرجة في تقارير العمليات المشبوهة، ودمجها، وتحديد أولويتها.

وتلجأ جهات الرقابة إلى توظيف أدوات الذكاء الاصطناعي بهدف رصد التجاوزات في عمليات الشراء الحكومي والتدقيق على الشكاوى المتعلقة بالفساد. على سبيل المثال، في البرازيل، تُوظف تقنيات الذكاء الاصطناعي لتنفيذ عملية فرز شاملة للبلاغات المرتبطة بالفساد، وتحديد الحالات التي تستدعي إجراء تحقيقات معمقة، وفحص المؤشرات التي تدل على عمليات شراء حكومية غير قانونية قبل إبرام العقود.

تحسين فعالية إجراءات إنفاذ القانون

يُمكن لأدوات الذكاء الاصطناعي أن تُساهم في رفع كفاءة إنفاذ القانون بشكلٍ كبير، نظرًا لارتباط التحقيقات والملاحقات القضائية عادةً بتكاليف باهظة من حيث الوقت والموارد. في ضوء ما سبق، فإن أدوات الذكاء الاصطناعي تُقدم فائدة كبيرة في تحليل كميات هائلة من البيانات، وذلك من خلال التأكد من ملائمة المواد المقدمة للمتطلبات المحددة من حيث الشكل والبنية، إلى جانب تحليل الأدلة باستخدام تقنيات التعلم الآلي مثل معالجة اللغة الطبيعية (Natural Language Processing). وبشكل عام، تُبرز أدوات الذكاء الاصطناعي كفاءتها العالية في توحيد الإجراءات والمهام المتكررة التي تتعامل مع مجموعات بيانات ضخمة.

تحسين جمع البيانات

بسبب تزايد تعقيد متطلبات الإبلاغ الإلزامي، تُواجه أجهزة الرقابة تحديات تتمثل في تلقي بيانات مُبلغ عنها مُتأخرة ونقص في جودة هذه البيانات، مما قد يُؤثر سلبًا على قدرتها على أداء دورها الرقابي. وبالتزامن مع ذلك، تقع على عاتق المؤسسات الخاضعة للمساءلة نفقات باهظة لإعداد التقارير المطلوبة من قبل الجهات الرقابية.

وسعيًا منها لتطوير عمليات جمع البيانات، عمدت أجهزة الرقابة خلال السنوات الأخيرة إلى تبني تقنيات "الاستخلاص" التي تُمكّن الجهات الرسمية من الحصول على المعلومات من الكيانات الخاضعة لمساءلتها بشكل فوري عند الحاجة. كما تُطور الجهات الرقابية واجهات برمجة تطبيقات (API) تسمح للمنظمات الخاضعة لمساءلتها بتقديم البيانات، مما يُقلل من تكاليف إعداد التقارير ويُحسّن التواصل بين كلا الطرفين.[4]

وشرعت الجهات الرقابية في دراسة آليات تحويل إرشادات إعداد التقارير إلى صيغة قابلة للقراءة آليًا، وذلك لغرض أتمتة عملية الامتثال التنظيمي وتيسير الالتزام بالمتطلبات بشكل أكبر.

تحسين كفاءة إدارة البيانات

تتضمن إدارة البيانات مهام أساسية ثلاث هي التحقق من صحة البيانات ودمجها وتجسيدها، ولكل منها أهداف محددة ضمن دورة إدارة البيانات. ويشير التحقق من الصحة إلى التحقق من اكتمال البيانات وصحتها واتساقها وفقًا لقواعد إعداد التقارير، بينما يشير الدمج إلى تجميع البيانات من مصادر متعددة وبصيغ مختلفة، بينما يتضمن التصوّر تقديم المعلومات بطريقة مرئية.[5]

[4] The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions // Financial Stability Board. URL: https://www.fsb.org/wp-content/uploads/P091020.pdf.

[5] The Suptech Generations // di Castri, S. et al. URL: https://www.bis.org/fsi/publ/insights19.htm.

وبشكل عام، يمكن تحديد مجالات استخدام الحلول الرقمية في مجال الرقابة على مكافحة غسل الأموال وتمويل الإرهاب على النحو التالي:

- الرصد عن بعد لأنشطة الأشخاص الخاضعين للرقابة من أجل الاستخدام اللاحق للمعلومات التي تم الحصول عليها في نماذج تقييم المخاطر.
- المساعدة في اتخاذ قرارات مستنيرة بشأن العملاء بناءً على تقييم دقيق لمخاطرهم.
- مراجعة وتقييم المخاطر بشكل تلقائي وإبلاغ الأشخاص الخاضعين للرقابة بنتائج التقييم، بالإضافة إلى معلومات حول أي سلوكيات قد تشير إلى مخالفة المتطلبات الإلزامية.
- اتخاذ تدابير وقائية (تشمل توزيع مواد توعوية، مثل مقاطع فيديو تفاعلية، وإجراء استقصاءات، وتخصيص مساحات للرد على الأسئلة الشائعة faq) وما شابه ذلك.

وتُظهر تجارب الدول الأجنبية، وتحديدًا دول الاتحاد الاقتصادي الأوراسي، في تطبيق التكنولوجيا الإشرافية (SupTech) والتكنولوجيا التنظيمية (RegTech) في عمل الهيئات الرقابية، فوائد جمة تستحقّ الاهتمام.

وهكذا، تقوم وكالة جمهورية كازاخستان للمراقبة المالية، من خلال إتاحة خدمة "الحساب الشخصي" الإلكترونية على موقعها الإلكتروني، بإجراء عمليات تدقيق دورية على عمل الكيانات الخاضعة للمساءلة المالية الأولية على أساس يومي، مما يمكّنها من الاستجابة الفورية لأي مؤشرات تدل على وقوع مخالفات لقواعد مكافحة غسل الأموال وتمويل الإرهاب. يستخدم الحساب الشخصي لإرسال رسائل إلى وحدة الاستخبارات المالية، بالإضافة إلى تقديم قوائم لتطبيق العقوبات المالية المستهدفة بموجب قانون مكافحة الإرهاب.إعداد برامج تدريبية للجهات الخاضعة لمتطلبات الرقابة المالية الأولية (تشريعات مكافحة غسل الأموال، الإرشادات، المواد التوعوية، التحليلات الإحصائية، وصف الأنماط وما إلى ذلك)، ونشر بيانات تقريرية متنوعة حول مكافحة غسل الأموال وتمويل الإرهاب، وتقديم التعليقات والملاحظات. وساعد اعتماد نظام الحساب الشخصي على تحسين التفاعل مع القطاع الخاص، وبشكل خاص خفض حجم الأعمال الورقية.

تقوم CNBV المكسيكية (Comision Nacio-nal Bancaria y de Valores)، التي تقوم بالرقابة (الإشراف) في مجال مكافحة غسل الأموال وتمويل الإرهاب، بتنفيذ مشروع يتضمن الحوسبة السحابية لمعالجة كميات كبيرة من البيانات المتعلقة بالامتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب الإلزامية، مما يسمح بزيادة حجم ومرونة التخزين والتنقل وقوة الحوسبة. تتيح المنصة أيضًا تطوير التحليلات التطلعية الأساسية والمتقدمة لتحسين كفاءة المراقبة وتحديد أنماط السلوك غير النمطية بشكل أفضل.

اعتمدت سنغافورة حلول تكنولوجيا المعلومات لوضع قائمة بترتيب المنظمات حسب مستوى المخاطر. إذ يتبنى تقييم المخاطر المتأصلة في البنوك عادةً نهجًا يعتمد على جمع بيانات مجمعة بشكل دوري من كل بنك لتقييم مستوى المخاطر المناسب لمكافحة غسل الأموال وتمويل الإرهاب. غالبًا ما يكون هذا عملية شاقة تتطلب غالبًا جهدًا ووقتًا كبيرين، وتتضمن مقارنةً شاملة للبيانات بين البنوك المُقارنة، وقد تتطلب عددًا كبيرًا من التقييمات النوعية الدقيقة.

ومع إدراك قدرات تحليل البيانات في تعزيز إمكانيات جمع كميات كبيرة من المعلومات ومعالجتها، قامت الجهة الرقابية في سنغافورة بالتعاون مع خبراء تحليل البيانات بإعداد قائمة شاملة بمؤشرات مخاطر غسل الأموال وتمويل الإرهاب ذات الصلة، ووضع نموذج لجمع البيانات المطلوبة في صيغة قابلة للقراءة آليًا، ووضع منهجية لتقييم المخاطر لضمان التطبيق المتسق.

واليوم، بات من الممكن إنشاء تقييم شامل لمخاطر غسل الأموال وتمويل الإرهاب لكل بنك، مصحوبًا تقرير يوضح العوامل الأساسية التي أدت إلى تكوينه، وذلك فور استلام البيانات. أدى ذلك إلى تمكين الجهات الرقابية من تحسين عملية تحديد المؤسسات المالية ذات المخاطر العالية وتركيز عمليات الرقابة عليها بشكل أكثر صرامةً. علاوة على ذلك، في حال رصد تغييرات جوهرية غير متوقعة وعلى نحو مستمر في ملفات المخاطر الخاصة ببنوك معينة، فقد يتم اتخاذ إجراءات رقابية عاجلة تجاه هذه البنوك.

وتلعب تقنيات تحليل الروابط الشبكية دورًا هامًا في ممارسات الرقابة لمكافحة غسل الأموال وتمويل الإرهاب في سنغافورة. وتشمل مصادر البيانات البلاغات عن أنشطة مشبوهة. ومن خلال توظيف أساليب التحليل الشبكي، طورّت الجهات الرقابية أداة تحليلية للكشف عن شبكات الكيانات القانونية والأفراد المترابطين عبر مجموعات من الإبلاغات عن أنشطة مشبوهة متنوعة تم تقديمها في فترات زمنية مختلفة من قبل كيانات تخضع للمساءلة. وتُقارن البيانات المذكورة ببيانات ملف تعريف الشركة مما يسمى بسجل الشركات (مثل: معلومات حول الأنشطة التجارية، وأسماء المديرين، وهوية المالكين الحقيقيين).

وباستخدام التحليل الشبكي لمعالجة هذه البيانات متعددة الأبعاد، يمكن للجهات التنظيمية تحديد المجالات ذات المخاطر

العالية والمؤسسات المالية التي تتطلب تدابير رقابية محددة.

ومن شأن التكنولوجيا أيضًا أن تُحدث ثورة في كيفية تنفيذ عمليات التفتيش الميدانية. تستعين الأجهزة الرقابية في سنغافورة، على سبيل المثال، بأدوات تحليلية خلال عمليات التفتيش بغية الكشف عن الحسابات والمعاملات غير المعتادة بغرض التحقق منها، وذلك حتى في حال عدم تقديم المؤسسة المعنية بلاغات عن معاملات مشبوهة. تقوم هذه الأداة التحليلية الآلية بتدقيق جميع المعاملات المالية للجهة المُراد تقييمها خلال الفترة الزمنية التي تسبق عملية التقييم بمدة تتراوح بين عامين إلى ثلاثة أعوام. وتُوفر التكنولوجيا للمفتشين إمكانية التخلي عن التحقق اليدوي لبيانات المعاملات للكشف عن الأنشطة غير المعتادة.

نتيجة لذلك، يُتيح هذا النهج للهيئة الرقابية التركيز بشكل أكبر خلال عمليات التدقيق على المناطق عالية الخطورة، ويعزز حوارًا أكثر موضوعيةً مع الجهة الخاضعة للرقابة وإدارتها بشأن إدارة المخاطر والرقابة الداخلية، مع مناقشة أمثلة واقعية.

وفي تونس تلجأ الجهات الرقابية إلى تقنية سلاسل الكتل (Blockchain) لتقدير مخاطر نقل الأموال عبر الحدود وممارسة الرقابة المستهدفة على المؤسسات. وأظهر تقييم المخاطر الوطني الذي تم إجراؤه في تونس عام 2017 أن النقل الدولي للأموال النقدية والتهريب يندرجان ضمن الأنشطة ذات المخاطر العالية. وبمبادرة من السلطات التونسية، وبمشاركة فاعلة من القطاع الخاص، تم إنجاز مشروع "هانيبال" وهو عبارة عن منصة وطنية تعتمد على تقنية سلاسل الكتل (البلوكشين) لجمع البيانات وتخزينها وتحليلها بشكل مشترك، وتضم هذه السلطات وحدات الاستخبارات المالية التونسية والبنك المركزي والجمارك ووزارة الداخلية، بينما يشمل القطاع الخاص البنوك ومكاتب الصرافة.

وتُقدم المنصة حلولًا مبتكرة لإنشاء لوحات معلومات ديناميكية تُسهل عملية تحليل مخاطر غسل الأموال وتمويل الإرهاب المرتبطة بنقل الأموال النقدية عبر الحدود. ويلعب ذلك دورًا هامًا في تمكين وحدة الاستخبارات المالية، ووكالات إنفاذ القانون، والبنوك، ومكاتب الصرافة على تحديد وكشف شبكات نقل الأموال النقدية ورصدها.

تحتل عملية تطوير أنظمة أتمتة لتقييم مخاطر الكيانات الخاضعة لمساءلتها، بالإضافة إلى إنشاء خدمات إلكترونية للتواصل مع القطاع الخاص، مكانة بارزة على قائمة أولويات هيئة الرقابة المالية الروسية (روسفينمونتورينغ). من بين حلول التكنولوجيا التنظيمية (RegTech) التي تخدم أكثر من 60 ألف كيان خاضع للمساءلة (مؤسسة فردية) هناك "الحساب الشخصي" على موقع وزارة المالية الروسية. وأصبح الحساب الشخصي الآن أكثر من مجرد قناة لإرسال الرسائل إلى الخدمة وتقديم معلومات حول الأشخاص المتورطين في الأنشطة الإرهابية وتمويل انتشار أسلحة الدمار الشامل، بل أصبح آلية فعالة تمكن من حل مجموعة واسعة من المهام الرامية لرفع مستوى الوعي بمتطلبات القانون والمخاطر المحتملة.

ويُشكل نظام التصحيح عن بُعد لسلوك الكيانات في نظام مكافحة غسل الأموال وتمويل الإرهاب عنصرًا محوريًا في هذه الآلية، حيث يتم إيصال تقييم المخاطر الذي تُصدره هيئة الرقابة المالية الروسية (روسفينمونتورينغ) إليهم، والذي يتم استخلاصه من نتائج المراقبة عن بُعد. وتتمتع هذه التدابير التصحيحية بكفاءة عالية، وتتميز بقدرتها على التكيف مع التغييرات، وانخفاض التكاليف من حيث الإدارة، وإمكانية تخصيصها باختيار معايير تقييم المخاطر بشكل مرن. ويؤدي هذا التفاعل إلى تخفيض مخاطر عدم الامتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب لدى آلاف الكيانات الخاضعة للمساءلة على أساس سنوي. ولا يقتصر عمل هذا النظام على تخفيض العبء الإداري على الجهات الخاضعة للرقابة، بل يسمح أيضًا بإعادة تخصيص موارد الجهة الرقابية لحل المهام التحليلية المعقدة التي تتطلب مهارات وخبرات مهنية.

وتهدف وظيفة الحساب الشخصي إلى زيادة وعي الكيانات المشاركة في مكافحة غسل الأموال وتمويل الإرهاب بالقوانين واللوائح ذات الصلة، وتزويدها بمعلومات حول نتائج التقييم الوطني للمخاطر، والتطورات والأنواع الجديدة من العمليات المشبوهة.

يحتوي الحساب الشخصي حاليًا على وصف لأكثر من 60 نوعًا، بما في ذلك علامات التعرف عليها.

يوفر الحساب الشخصي إمكانية التعلم عن بعد من خلال مجموعة من البرامج التعليمية المتاحة، وعقب إتمام دراسة هذه المواد يستطيع للمستخدمين تقييم معرفتهم المكتسبة من خلال الاختبارات. بالإضافة إلى ذلك، تتوفر إمكانية تقديم تفسيرات تلقائية لأحكام القانون بشأن القضايا الشائعة.

وضمن مساعي تطوير آليات التواصل مع القطاع الخاص، تم إطلاق الحساب الشخصي للمجتمع المهني (الجمعيات والنقابات) في العام 2022. وتتيح وظائفه، على سبيل المثال لا الحصر، نقل المواد المتعلقة بالتزام المؤسسات الخاضعة للمساءلة بمتطلبات التشريعات لمكافحة غسل الأموال وتمويل الإرهاب، وإبلاغهم بالفعاليات المُنظمة لتنسيق مشاركة أعضاء المجتمعات المهنية ذات الصلة وغير ذلك.

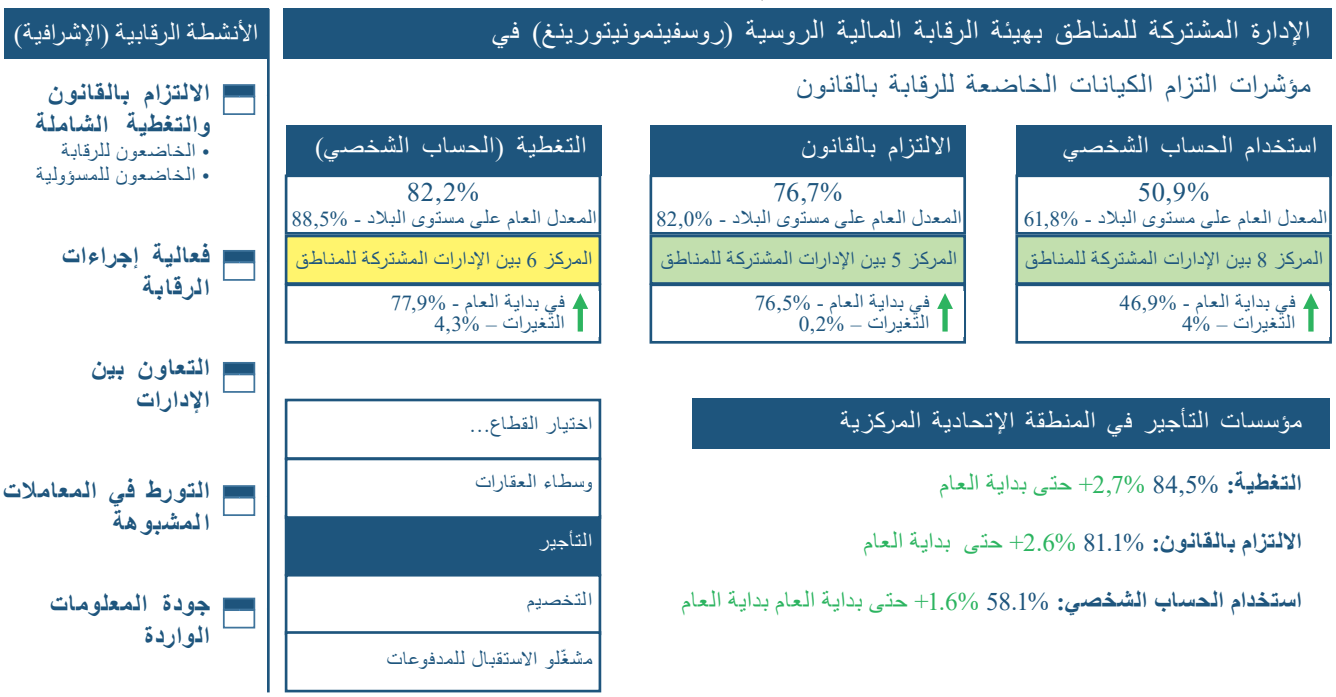
وبهدف تعزيز كفاءة استخدام الحساب الشخصي في عمليات التحقق من هوية العملاء، تم تصميم مُجمِّع معلومات عن العميل المُراد التحقق منه بجمع البيانات من جميع المصادر المتاحة وتقديمها في نموذج موحد مُجمَّع.

من خلال الحساب الشخصي للسلطة الإشرافية، يمكن الاطلاع إلكترونياً على نتائج المراقبة عن بعد التي تقوم بها Rosfinmonitoring، مما يضمن سرعة استجابة سلطات الرقابة (الإشراف) في مجال مكافحة غسل الأموال وتمويل الإرهاب للمخاطر في أنشطة الكيانات الخاضعة للإشراف، ويشجع استخدام أساليب موحدة عند التخطيط لأنشطة الرقابة. بالإضافة إلى ذلك، يتم توفير التحليلات الكلية عبر الإنترنت من خلال هذا المورد، مما يسمح للسلطة الإشرافية برؤية ليس فقط ديناميكيات معايير الالتزام بالقانون في القطاع وتورط ممثليه في المعاملات المشبوهة، ولكن أيضًا تعرضه لمخاطر محددة. ومن مهام المستقبل القريب دمج لوحة رئيس هيئة الإشراف في الحساب الشخصي.

توفر هذه اللجنة، التي تم تطويرها لأول مرة لرؤساء الهيئات الإقليمية لـ Ros-finmonitoring (الشكل 1)، بيانات تحليلية إضافية، بما في ذلك حول فعالية تدابير الاستجابة الإشرافية المطبقة في الأقسام التحليلية المختلفة (من حيث أدوات التحكم والمناطق الفردية وأنواع أنشطة). يتيح لك ذلك ضبط عمل الوحدة الإشرافية واختيار الأساليب الأكثر فعالية لتنفيذ أنشطة المراقبة.

ويُؤدي الحساب الشخصي أيضًا وظيفةَ "تقديمِ الملاحظات". وابتداءً من عام 2019، يتم إبلاغ الجهات الخاضعة للمساءلة بنتائج تقييم المعلومات المُرسلة من قبل المؤسسات الائتمانية حول العمليات المشبوهة، من خلال الحساب الشخصي على موقع الويب الخاص بهيئة الرقابة المالية (روسفينمونتورينغ)، وذلك في صورة "مؤشر جودة تدفق المعلومات" (الشكل 2) من خلال تطبيق خوارزميات محددة، يتم إجراء تقييم لمدى فعالية التفاعل المعلوماتي بين الكيانات الخاضعة للمساءلة وهيئة الرقابة المالية (روسفينمونتورينغ) وذلك بناءً على مجموعة من أهم المعايير. وفي الوقت الحالي تخضع معايير التفاعل التالية للتقييم: - سرعة الإبلاغ عن المعاملات المشبوهة، وتركيز الإبلاغ عن المعاملات المشبوهة على المخاطر الحالية، وخصائص التفاعل مع وحدة الاستخبارات المالية (إرسال معلومات حول المخاطر، والاستجابة لطلبات وحدة الاستخبارات المالية، وانتهاك المواعيد النهائية لتقديم المعلومات إلى وحدة الاستخبارات المالية).

الشكل رقم -1 منصة المدير



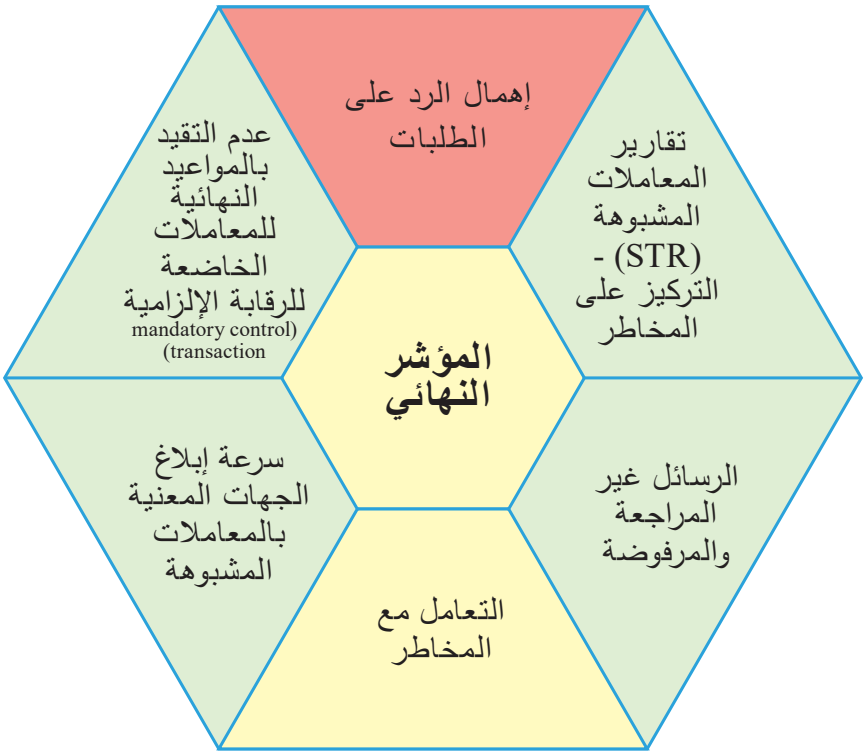
وبناءً على هذه المعايير، يتم تقييم مدى كفاءة تفاعل الكيان مع وحدة الاستخبارات المالية بشكل شامل. وتتمثل نتائج استخدام هذا الشكل من عمليات التقييم في: زيادة سرعة اكتشاف المعاملات المشبوهة، ورفع مستوى جودة أنظمة منع الاحتيال، وتوجيه تركيزها نحو المخاطر.

أحد الشروط المهمة لتحسين جودة تدفق المعلومات من الكيانات المبلغة هو التوجيه في الوقت المناسب لموضوعات المراقبة المالية للمخاطر والاتجاهات الحالية في المجال الائتماني والمالي.

أحد الأمثلة على هذه الممارسة هو توصيل نماذج وعلامات المعاملات المشكوك فيها إلى مؤسسات الائتمان من خلال وظيفة الحساب الشخصي. في سياق مكافحة غسل الأموال وتمويل الإرهاب، يشير التصنيف إلى ظهور أنماط مختلفة من المعاملات المشبوهة باستخدام البنية التحتية للمؤسسات المالية التي تكون منهجية أو متكررة. ترتبط الطبيعة المنهجية لمظاهرها، كقاعدة عامة، بنقاط الضعف المختلفة لأنظمة الرقابة الداخلية لموضوعات المراقبة المالية الأولية.

يمكن أن تكون مصادر المعلومات حول النماذج الجديدة هي نتائج التحليل المالي لكل من صندوق المعاشات التقاعدية وموضوعات المراقبة المالية. على سبيل المثال، تقوم هيئة الرقابة المالية (روسفينمونتورينغ)، بالتعاون مع المؤسسات الائتمانية - أعضاء مجلس الامتثال (هيئة استشارية تابعة للجنة المشتركة بين الإدارات المعنية بمكافحة غسل الأموال وتمويل الإرهاب)، بمراجعة أمثلة التحليل المالي بانتظام،

◄ الشكل رقم -2 مؤشر جودة تدفق المعلومات



والتي غالبًا ما تشكل الأساس للنماذج المقدمة من خلال وظيفة التحليل الشخصي حساب. وتجدر الإشارة إلى أن الإبلاغ عن المخاطر بهذا التنسيق يؤخذ بعين الاعتبار أيضًا عند حساب مؤشر جودة تدفق المعلومات.

تحليل المعلومات الواردة، بما في ذلك الإشارة إلى معرف النماذج (يتم تخصيص رقم فريد لكل منها لإرسال تقرير المعاملات المشبوهة في حالة تحديد معاملة مشبوهة تندرج ضمن المعايير المناسبة) يسمح لـ هيئة الرقابة المالية (روسفينمونتورينغ)، بإجراء اختيارات مواضيعية مختلفة عبر الإنترنت مما يبسط تحليل تدفق المعاملات.

بشكل عام، يتيح تطوير البنية التحتية لتكنولوجيا المعلومات للسلطات الإشرافية الوصول إلى مستوى جديد نوعيًا من العمل، وتوسيع المعرفة المتخصصة وسرعة اتخاذ القرار.

يُنظر إلى الهدف الرئيسي لتطوير التقنيات الرقمية في الأنشطة الإشرافية في المستقبل القريب على أنه تعزيز تنفيذ المعايير التي تركز على العميل، مما يضمن ليس فقط تقليل العبء التنظيمي، ولكن أيضًا تشكيل، من خلال اتصالات أكثر استهدافًا، جو فريد من الشراكة والثقة بين الدولة والقطاع الخاص

سجلّ المُستفيدين الفعليين. تجربة كازاخستان

عملاً بأحكام المادة 6-1 من قانون جمهورية كازاخستان "مكافحة غسل الأموال وتمويل الإرهاب"، تُناط بوكالة جمهورية كازاخستان للراقبة المالية مسؤولية إدارة سجلّ المستفيدين الفعليين للشخصيات الاعتبارية (يشار إليه فيما يلي باسم - "السجل").

دينارا موسينا -
رئيس قسم التحليل العملياتي في وكالة الرقابة المالية لجمهورية كازاخستان

يُمنح الوصول إلى المعلومات والبيانات المُستقاة من السجّل الخاص بالمستفيد الحقيقي للشركة إلى:

1) الجهات الحكومية في جمهورية كازاخستان المُكلفة، ضمن نطاق اختصاصها، بمراقبة التزام الكيانات الخاضعة لرقابة مكافحة غسل الأموال (تبييض الأموال) وتمويل الإرهاب بتشريعات جمهورية كازاخستان في هذا الشأن، وذلك فيما يتعلق بالكيانات الخاضعة لرقابتها.
2) جهات إنفاذ القانون والوكالات الحكومية المختصة.
3) الجهات المُكلفة بمراقبة العمليات المالية.

في هذه المقالة، سنناقش الأساليب التي وضعتها وكالة الرقابة المالية لإنشاء وإدارة السجل، بالإضافة إلى وظائفها المتاحة في الحساب الشخصي للجهات التنظيمية الحكومية، ووكالات إنفاذ القانون، وكيانات الرقابة المالية.

تُبنى أساليب إنشاء السجل وإدارته على ثلاثة عوامل:

- نتائج تقييم المخاطر الذي تم إجراؤه على الكيانات القانونية، أي درجة انخراطها في الجرائم الأساسية وغسل الأموال.
- امتلاك الوكالة القدرة على الوصول إلى قواعد بيانات متنوعة واستخدام تقنيات المعلومات لتحليلها ومعالجتها.
- التوصيات المُحدّثة لمجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF).

آلية تسجيل المستفيدين الفعليين

وتماشيًا مع معايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) التي تنص على أن "معلومات المستفيدين النهائيين يجب أن تكون شاملة ودقيقة وحديثة"، فقد أصبح جمع المعلومات من مصادر متنوعة كأهم مرحلة في عملية العمل المُصممة لهذا الغرض.

وعليه، فإن بدء العملية التجارية يتطلب جمع معلومات حول المستفيدين الفعليين، وذلك حسب ما تُقدّمه الكيانات القانونية نفسها. وتستند المعلومات الواردة في هذه المقالة إلى المصادر التالية:

- وزارة العدل: الجهة المسؤولة عن توحيد جميع بيانات التسجيل في البلاد.
- الجهات الخاضعة لمتطلبات الرقابة المالية: الجهات الملزمة بتحديد هوية وتسجيل المستفيدين الفعليين لعملائها (سجل كبار المساهمين، وسجل المستفيدين الفعليين المُدار من قبل المركز المالي الدولي "أستانا").
- لجنة الإيرادات الحكومية: الجهة المخولة بفرض وتحصيل الضرائب، وتشمل ضمن مهامها استلام إقرارات مراقبة الشركات الأجنبية من قبل المقيمين كجزء من التزاماتهم الضريبية.
- وكالة المراقبة المالية: الجهة المُخولة بطلب وتلقي المعلومات عن المستفيدين الفعليين.
- وزارة الطاقة ووزارة الصناعة وتطوير البنية التحتية: الهيئات المعتمدة للحصول على المعلومات وتخزينها حول المالكين المستفيدين من مستغلي الثروات الطبيعية (المعيار الدولي للشفافية في قطاعات استخراج الموارد الباطنية).

لذا، تتمثل المرحلة الأولى في جمع كافة البيانات المتعلقة بالملكية المستفيدة من مصادر متعددة، بناءً على ما أعلنته الكيانات القانونية نفسها.

ويمكن لوكالة الرقابة المالية الوصول إلى معظم هذه المعلومات عبر الإنترنت. وبالتالي، يتم جمعها وتوحيدها بشكل تلقائي.

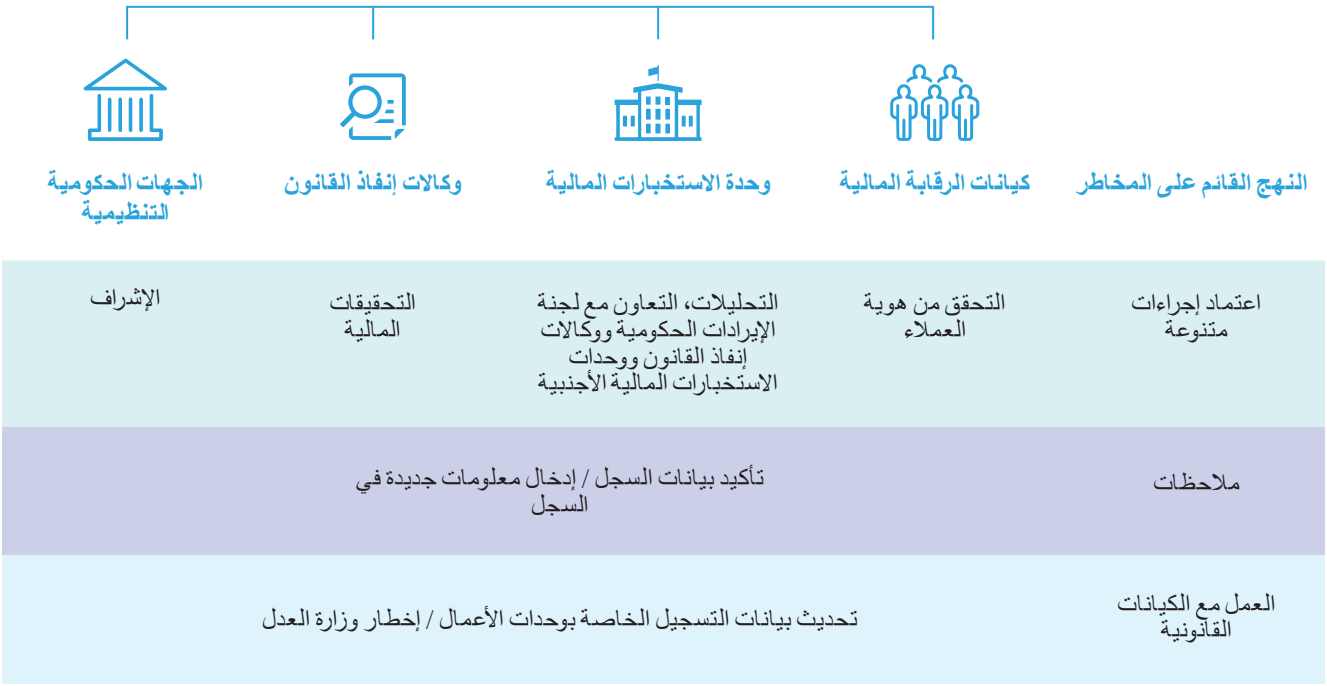
مصادر بيانات إضافية

وبعد ذلك يتم التحقق من صحة هذه المعلومات من خلال جمع بيانات إضافية من مصادر أخرى، بما في ذلك:

- تقارير حول المعاملات التي تقع فوق عتبات محددة أو المعاملات المشبوهة - من قبل الجهات الخاضعة لقواعد الرقابة المالية.
- الإقرارات الضريبية - من لجنة الإيرادات الحكومية.
- العلاقات الأسرية والشركات - من وزارة العدل.
- الفواتير الإلكترونية - من لجنة إيرادات الدولة.
- بيانات وحدات الاستخبارات المالية الأجنبية - سجل الاستعلامات.
- مصادر البيانات المفتوحة على الإنترنت.

حالات المالكين المستفيدين

تم تطوير منهجية شاملة لخوارزميات معالجة هذه البيانات لتحديد العلاقات المستفيدة، وذلك بناءً على مجموعة



البيانات المتاحة. وتكون خوارزميات معالجة البيانات مؤتمتة. في الوقت الحالي، يوجد 19 خوارزمية قيد التطبيق أثبتت فعاليتها.

نتيجة حسابات هذه الخوارزميات، يتم تعيين إحدى الحالات التالية للأفراد:

- "مالك مستفيد مسجل"
- "مالك مستفيد مُفترض"

تعتبر المعلومات المتعلقة بالمالكين والمقدمة لوزارة العدل، هي وحدها "المسجّلة" رسميًا، بينما تعتبر المعلومات الأخرى "مُفترضة".

تستند كل خوارزمية لتحديد "المالك المستفيد المحتمل" إلى تقنية منفصلة مصدرها معلومات مختلفة، ولكل منها وزنها الخاص ونقاط الثقة الخاصة بها. تخضع موثوقية المعلومات حاليًا للتقييم من قبل خبراء باستخدام نظام تقييم مُدرّج من 1 إلى 4، بحيث تُشير القيمة 1 إلى ضعف احتمالية الموثوقية، بينما تُشير القيمة 4 إلى قوتها.

وتعمل كل خوارزمية وفقًا لجدول زمني محدد. وتُخزن نتائج كل مرة يتم فيها تشغيل الخوارزميات.

مستخدمو السجل هم المشاركون في نظام مكافحة غسل الأموال: الجهات الحكومية التنظيمية، وكالات إنفاذ القانون، كيانات الرقابة المالية، وحدة الاستخبارات المالية.

في ضوء العمل المُنجز في هذا المجال، يُتيح السجل لمستخدميه إمكانية التعبير عن موقفهم الخاص فيما يتعلق بالمستفيدين المحتملين، وذلك من خلال:

1. تأكيد صحة فرضية وحدة الاستخبارات المالية أو دحضها.
2. طرح فرضية جديدة لمالك مستفيد إضافي مع شرح خوارزمية/ مخطط عمله.

إن كل ملاحظة من ملاحظات المشاركين في مكافحة غسل الأموال ذات قيمة كبيرة، حيث تُساهم في تحسين وتطوير الخوارزميات 19 المُطبّقة حاليًا وتوسيع نطاقها.

علاوة على ذلك فإن المستخدمين من خلال تفاعلهم مع العملاء والمعلومات التحليلية ومعايير الرقابة، يدفعون الكيانات القانونية لتحديث بياناتها المسجلة.

وعليه، فإنّ الاستخدام الفعّال لسجلّ المستفيدين الحقيقيين في إطار عمل مكافحة غسل الأموال من قبل جميع الأطراف المعنية يُسهم في تحقيق هدفنا المشترك المتمثل في منع ومكافحة انخراط الكيانات القانونية في الجرائم الأساسية وغسل الأموال.

الذكاء الاصطناعي في التقنيات المالية: نظرة على الحاضر والمستقبل

35 **سفيتلانا أورلوفا**
"المنتجات والحلول الرقمية هي ركيزة أساسية لتطوير المراجعة المالية الحكومية"

39 **ف. ل. دوستوف**
تقنيات الذكاء الاصطناعي في القطاع المالي وتأثيرها على بعض جوانب مكافحة غسل الأموال وتمويل الإرهاب

43 **ميخائيل سيرغيفيتش برونين**
توظيف الذكاء الاصطناعي في أعمال هيئة الرصد المالي

46 **أليكسي غيليتا**
"سوق التكنولوجيا المالية في روسيا هو أحد أكثر الأسواق ابتكارًا وتقدمًا في العالم من الناحية التقنية "

سفيتلانا أورلوفا-

"المنتجات والحلول الرقمية هي ركيزة أساسية لتطوير المراجعة المالية الحكومية"

عرضت الخبيرة في التدقيق لدى ديوان الرقابة المالية في روسيا الاتحادية السيدة/ سفيتلانا أورلوفا - خلال مقابلة مع مجلة "الأمن المالي"، مجموعة من الإجراءات المتعلقة بتطبيق تقنيات الذكاء الاصطناعي في مجال الرقابة الحكومية (التدقيق المحاسبي)، مع التركيز على إمكانيات التقنيات الجديدة لتحسين الإدارة الحكومية والحلول الرقمية الحديثة في المجال ذاته.

أودّ أن أعرب عن خالص شكري وتقديري لكم، السيدة/ سفيتلانا أورلوفا، على منحكم لي هذا الوقت الثمين من جدول أعمالكم المزدحم. يُسلط هذا العدد الضوء على التطورات المتسارعة في مجال الذكاء الاصطناعي. ما هي في رأيكم إمكانيات تطبيق الذكاء الاصطناعي في مجال الرقابة المالية الحكومية (التدقيق المحاسبي)؟

أودّ في البداية أن أُشدّد على أنّ عملنا ينسجم مع التوجيهات التي حدّدها الرئيس الروسيّ فلاديمير بوتين خلال منتدى سانت بطرسبرغ الاقتصاديّ الدوليّ في يونيو 2023. وتتمحور هذه التوجهات حول جعل "الأتمتة الفعّالة وإتقان تقنيات الذكاء الاصطناعي" حجر الزاوية للاقتصاد المبني على الابتكار. ومن الأهمية بمكان تبني واستخدام هذه الإنجازات بشكلٍ فعّال، ودعم تطوير البرامج المحلية في مجال البيانات الضخمة، وإطلاق مشاريع في مجال الذكاء الاصطناعي.

وفي شهر فبراير من عام 2024، قام رئيس روسيا الاتحادية بإدخال تعديلات جوهرية على الاستراتيجية الوطنية لتطوير الذكاء الاصطناعي للفترة حتى عام 2030. وعلى وجه الخصوص، تُلزم هذه الاستراتيجية السلطات التنفيذية الاتحادية بالاسترشاد بها عند صياغة وتنفيذ وثائق التخطيط الاستراتيجي القطاعي. وعليه، ستُصبح ممارسات أجهزة السلطة التنفيذية الاتحادية، بعد إدخال التعديلات، مُستندةً إلى حدٍّ ما إلى تقنيات الذكاء الاصطناعي.

كما تم التأكيد على استمرارية هذا النهج الاستراتيجي في خطاب الرئيس الروسي أمام الجمعية الاتحادية. خلال السنوات الماضية، بذل ديوان الرقابة المالية جهودًا حثيثة في سبيل تحقيق هذا الهدف. من خلال التركيز بشكل خاص على رقمنة أنشطة هيئة التفتيش.

من المؤكد أن بعض تقنيات الذكاء الاصطناعي تُستخدم حاليًا في العديد من القطاعات، بما في ذلك الهواتف الذكية والطب والتعليم وأنظمة المنازل الذكية والصناعة.

تعتمد تقنيات الذكاء الاصطناعي على ركيزتين أساسيتين: توافر كميات هائلة من البيانات وإمكانية معالجتها وتحليلها باستخدام تقنيات الشبكات العصبونية.

وفي مجال التدقيق المالي الحكومي (الرقابة)، تُعتبر جودة البيانات الضخمة، ولا سيما موثوقيتها، ذات أهمية قصوى بين مكونات الذكاء الاصطناعي المذكورة. وقد وجهنا اهتمامنا في البداية نحو تنظيم تحليل البيانات الضخمة. من خلال الحلول الرقمية التي تم تطويرها في ديوان الرقابة المالية باستخدام أدوات رقمية لجمع البيانات وتحليلها وتصورها (تحليلات البيانات)، تم حل هذه المهمة إلى حد كبير. وبحلول نهاية عام 2023، ضم سجل الحلول والمنتجات الرقمية لديوان الرقابة المالية بيانات عن أكثر من 300 حل ومنتج رقمي.

وتُتيح هذه الحلول نقلة نوعية في مجال إجراءات التدقيق المحاسبي من خلال الاستفادة من أحدث التقنيات والمنهجيات.

وعلاوة على ذلك، تُتيح الحلول الرقمية تخفيض مدة عمل مفتش تحليل بيانات كيان التدقيق (المراقبة) بنسبة الثلث كحد أدنى. ونظرًا لتقليل العامل البشري إلى أدنى حد، فإن خطر الأخطاء يكاد يكون معدومًا. وثالثًا، شهد نطاق المعلومات الخاضعة للتدقيق توسعًا ملحوظًا.

ومن المؤكد أن هذا الإنجاز لم يتأتى إلا بفضل العمل الدؤوب في مجال التحول الرقمي للتدقيق الذي ينفذه ديوان الرقابة المالية.

وبصفتي مديرًا لقسم تدقيق الإدارة الحكومية، أُشرف على جهودنا الحثيثة لدفع عجلة التحول الرقمي في جميع جوانب عملنا، بما في ذلك المؤسسات الخاضعة للتدقيق.

السيدة سفيتلانا أورلوفا، بِمَا أنّنا قد أحرزنا تقدمًا في هذا المجال، أرجو منكم التكرم بشرح هذه النتائج بشكلٍ أكثر تفصيلًا.

كمثال على ذلك، يمكنني الإشارة إلى العمل المشترك في مجال تطبيق تقنيات المعلومات الحديثة في إجراءات التقاضي.

خلال عام 2023، عقدنا أربع اجتماعات موسعة مع 15 وزارة ووكالة رائدة في مجال التحول الرقمي، بما في ذلك وزارة التنمية الرقمية والاتصالات والإعلام الجماهيري الروسية، ووزارة العدل الروسية، والخزينة الاتحادية، ومصلحة الضرائب الاتحادية، ودائرة تنفيذ الأحكام القضائية الاتحادية، ووكالة إدارة الممتلكات الاتحادية وغيرها من الوكالات الأخرى. وتناولت المباحثات معهم أفضل السبل لدمج التقنيات المعلوماتية الحديثة في إطار سير إجراءات التقاضي، وتعزيز التعاون بين مختلف أجهزة الدولة والمنظومة القضائية، بما في ذلك تحسين عمليات إدارة الحسابات المصرفية الوداعية للمحاكم التحكيمية.

وقد طرحنا هذه القضايا خلال اجتماع مع نظرائنا من حكومة روسيا الاتحادية، والمحكمة العليا لروسيا الاتحادية، ومجلس الاتحاد في الجمعية الاتحادية الروسية.

وبفضل جهودنا المشتركة، تم التوقيع على اتفاقية نوايا في أواخر عام 2023 بين الإدارة القضائية لدى المحكمة العليا لروسيا الاتحادية، ووزارة التنمية الرقمية والاتصالات والإعلام الجماهيري في روسيا الاتحادية والخزينة الاتحادية لوضع استراتيجية مشتركة لتطبيق تقنيات المعلومات والاتصالات الحديثة في جميع مراحل التقاضي وإدارة سجلات المحكمة.

وتسعى هذه المبادرة التعاونية إلى إرساء خدمة مُيسّرة للمواطنين والشركات على حد سواء، ودمجها في الإجراءات القضائية، والتي من شأنها تسهيل عملية تسديد الأموال من قبل أطراف الدعوى، وتعزيز وضوح مساراتها، ومنع أي احتمالية لسوء استخدام هذه الأموال.

يخضع المشروع حاليًا لمرحلة تصميم الحلول التقنية، ونتوقع بدء مرحلة التنفيذ التجريبي في المستقبل القريب، وذلك في مقر محكمة التحكيم التجاري لمدينة موسكو.

وفي حال أثبتت التجربة العملية نجاعة الإجراءات المنصوص عليها في الاتفاقية، سيتم تعميم تطبيقها على جميع المحاكم الاتحادية وإدارات الأقسام القضائية التابعة للمحكمة العليا لروسيا الاتحادية في جميع الكيانات المكونة لروسيا الاتحادية.

علاوة على ذلك، وبالتعاون مع ممثلي السلطة القضائية، وإدارة شؤون القضاء لدى المحكمة العليا لروسيا الاتحادية، وبالاشتراك مع الوزارات والوكالات الحكومية، يجري العمل على بلورة موقف موحد بشأن صياغة "خارطة طريق" لتنفيذ الحلول الرقمية في كل من الإجراءات القضائية والتفاعل بين الإدارات.

ومن المقرر الشروع في تنفيذ عدة مشاريع رائدة بمشاركة فاعلة من جانبنا:

- تبذل الجهات القضائية، بالتنسيق مع وزارة التنمية الرقمية والاتصالات والإعلام الجماهيري، ووزارة العدل، ووزارة المالية، ووزارة الخزانة، ومصلحة الضرائب الاتحادية، ومأموري التنفيذ القضائي، جهودًا حثيثةً لحلّ مشكلةٍ مُلحة تواجهها البلاد حاليًا، وهي **تخصيص معرفات فريدة للدفعات في الوثائق التنفيذية الصادرة عن المحاكم.** وعلى الرغم من التوصل إلى حل مؤقت، إلا أن هناك مهمة ضخمة وجادة تنتظرنا تتمثل في توحيد جهود جميع الجهات الفاعلة في هذا الاتجاه.

- تشارك الجهات القضائية والخزينة ودائرة التنفيذ القضائي في دراسة إمكانية تنفيذ مشروع مشترك ضخم وذو أهمية بالغة، وهو **إنشاء نموذج سجل لتنفيذ الأحكام القضائية.** ويركز هذا النموذج على ضمان الشفافية في إجراءات التنفيذ، ممّا سيُعزز كفاءة التواصل الإلكتروني بين الجهات الحكومية والمواطنين.

السيدة سفيتلانا أورلوفا، هل يمكنكم التفضل وتقديم أمثلة ملموسة على الحلول الرقمية وتأثيراتها الإيجابية على تحسين نظام الإدارة الحكومية؟

بفضل جهود القسم الذي أترأسه، تمّ إنجاز 18 حلًّا رقميًا (منتجًا) خلال عام 2023 فقط.

وهنا أودّ تسليط الضوء على أبرز هذه الحلول والتي أدت إلى تحسين نظام الإدارة الحكومية بشكلٍ نوعيّ.

وبالتالي، لتحقيق أهداف تنفيذ التوصيات المنهجية التي تم تطويرها من قبل الإدارة لمعرفة وتقييم مخاطر الفساد خلال الأنشطة الرقابية والتحليلية الخبيرة باستخدام تقنية الذكاء الاصطناعي، تم تطوير منتج رقمي يحمل الاسم - "كشف مخاطر مخالفات الفساد في عمليات الشراء من مورد واحد".

إذ يُمكن للمنتج إجراء تحليل تلقائي لمدى مطابقة العقد مع أحكام القانون الاتحادي "نظام العقود في مجال شراء السلع والخدمات والأعمال لتلبية احتياجات الدولة والبلديات"، حيث ينظم القانون قضايا الشراء من مورد واحد، وفي حال الكشف عن أي تناقض بين بنود العقد وأحكام القانون، يُصدر المنتج تنبيهًا بوجود مخاطر محتملة لحدوث مخالفات.

في إطار عملية تطوير المنتج، قام النموذج بدراسة وتحليل ما يقارب 100 ألف عقد تم نشرها على نظام المعلومات الموحد في مجال المشتريات وتقييم مختلف صياغاتها، والتي على أساسها، يتمكن النموذج من تحديد التباينات والمخاطر المحتملة.

يُعد المشروع جاهزًا للاستخدام اليوم وقد تم نشره على البوابة الداخلية لديوان الرقابة المالية.

كما تجدر الإشارة إلى أنه تم تصميم حل رقمي متميز خلال فعاليات التحليل الخبير "تحليل إدارة الحسابات الشخصية (الودائع) لتسجيل العمليات بالتحويلات المالية التي تخضع لتصرف المحاكم التحكيمية مؤقتًا في الفترة من 2012 إلى 2022 والفترة المنتهية في 2023".

ويهدف الحل الرقمي بشكل رئيسي إلى التحقق من توافق مستندات الدفع المتعلقة بالأموال المودعة مؤقتًا لدى محاكم التحكيم مع عدد القضايا التي تم قبولها للنظر فيها خلال 11 عامًا وضمان الالتزام بأحكام لائحة تنظيم عمل المحاكم الاتحادية والإدارات التابعة للأقسام القضائية في كيانات روسيا الاتحادية فيما يتعلق بالحسابات الشخصية (الودائع) لتسجيل العمليات المتعلقة بالتحويلات المالية التي تخضع للاستخدام المؤقت.

وتسعى هذه المبادرة التعاونية إلى إرساء خدمة مُيسّرة للمواطنين والشركات على حد سواء، ودمجها في الإجراءات القضائية، والتي من شأنها تسهيل عملية تسديد الأموال من قبل أطراف الدعوى، وتعزيز وضوح مساراتها، ومنع أي احتمالية لسوء استخدام هذه الأموال.

والآن لدينا البيانات الأولية التالية: عدد مستندات الدفع: حوالي 9 ملايين؛ عدد الدعاوى التحكيمية أكثر من 27 مليون دعوى.

ومن الصعب تصور العدد الهائل من المفتشين والوقت اللازم لمعالجة وتحليل هذا الكم الهائل من المعلومات والأرقام.

ومع ذلك، واجهت العملية بعض التحديات، تمثلت في عدم وضوح البيانات بشكل كبير: حيث تم إيداع الأموال من قبل أشخاص معينين، بينما تم سحبها من قبل أشخاص آخرين، بما في ذلك أشخاص ليسوا أطرافًا في الإجراءات القضائية، بالإضافة إلى ذلك، كانت البيانات المتعلقة بالأموال المودعة في حساب المحكمة غير مكتملة (حيث تم استخدام رقم التعريف الضريبي لإدارة الخزينة الاتحادية بدلاً من رقم التعريف الضريبي للمحكمة).

وقد أفضى تطوير حل رقمي إلى معالجة هذه المشكلة بفعالية.

والأهم من ذلك:

كشفت نتائج هذا الحدث عن الحاجة الماسة إلى إطلاق مشروع تجريبي لتعزيز وكفاءة عمليات معالجة الأموال الموجودة في الحسابات الجارية المُدارة من قبل أفرع الخزينة الاتحادية، والتي تم إيداعها من قبل الأفراد والكيانات بموجب التشريعات السارية.

هناك اقتراح بتعديل لائحة تنظيم عمل المحاكم الاتحادية وإدارات الأقسام القضائية في كيانات روسيا الاتحادية للتعامل مع الحسابات الشخصية (الودائع) لتسجيل العمليات المتعلقة بالتحويلات المالية التي تخضع للاستخدام المؤقت.

ما هي الحلول الرقمية المبتكرة التي يعمل عليها طاقمكم في الوقت الحالي؟

اليوم في ضوء التعليقات التي وردتنا من عدة دوائر في ديوان الرقابة المالية، نقوم حاليًا بوضع اللمسات الأخيرة على الحل الرقمي الذي تم تصميمه في إطار تنفيذ إرشاداتنا الخاصة بتحديد وتقييم مخاطر الفساد.

يجري العمل على تحسين الحل باستخدام تقنية جديدة تسمى "الذكاء الاصطناعي التوليدي".

وأود أن أُبين، لمن لم يسبق له التعامل مع هذه التقنية، أنها تتيح لنا برمجة خوارزمية بحث خاصة بنا تتماشى مع معايير محددة وتلبي احتياجاتنا.

بعد الانتهاء من تطوير الحل واختباره، ستعرض نتائج تحليل العقد الحكومي ليس فقط تحديدًا لمناطق المخاطر المحتملة، بل ستتضمن أيضًا شرحًا تفصيليًا للمخاطر، بما في ذلك مجموعة العوامل التي أدت إلى تحديد مخاطر حدوث مخالفات محتملة.

بالإضافة إلى ذلك، وبمجرد اكتمال المشروع، لن نقتصر على تحليل العقود بشكل انتقائي، بل نخطط لتحميل مجموعات من المستندات بأي تنسيق قابل للقراءة آليًا.

وستؤدي عملية أتمتة كشف المناطق ذات المخاطر إلى خفض زمن معالجة وتقييم المستندات بفعالية وكفاءة عالية.

ومن المهم الإشارة إلى أن الذكاء الاصطناعي، مهما كان متطورًا، لا يمكنه أن يحل محل المفتش، بل يمكن أن يكون أداة مساعدة قيّمة له.

ومن المهم الإشارة إلى أن الذكاء الاصطناعي، مهما كان متطورًا، لا يمكنه أن يحل محل المفتش، بل يمكن أن يكون أداة مساعدة قيّمة له.

تقنيات الذكاء الاصطناعي في القطاع المالي وتأثيرها على بعض جوانب مكافحة غسل الأموال وتمويل الإرهاب

لا شك أن الذكاء الاصطناعي أصبح أكثر التطورات التكنولوجية صخبًا في العامين الماضيين. ولا شك أن القفزة النوعية في تطوّره ستُتيح لنا إعادة النظر في الأساليب التقليدية لحلّ العديد من المهامّ الفكرية التي كانت تتطلّب في السابق تدخلًا بشريًا، وتوسيع نطاق المهامّ التي يمكن حلّها دون تدخّل بشري.

ف. ل. دوستوف -
رئيس مجلس إدارة جمعية "المال الإلكتروني"، دكتوراه في الفلسفة والعلوم الرياضية، أستاذ مشارك في الجامعة المالية.

وكشف تقرير استشاري حديث صادر عن البنك المركزي لروسيا[1] الاتحادية عن أن المجال المالي قد تبوأ مكانة الصدارة بين القطاعات الأكثر استهلاكًا للتكنولوجيا الجديدة. وفي هذه المقالة، نسعى إلى استعراض جوهر هذا التطور التكنولوجي بشكل موجز وتأثيره المحتمل على تطور القطاع مع التركيز بشكل خاص على جوانب مكافحة غسل الأموال وتمويل الإرهاب.

مقدمة في التكنولوجيا.

لا يتسع نطاق المقالة لتقديم عرض شامل لتكنولوجيا معقدة مثل الذكاء الاصطناعي، والتي تتمتع بتاريخ طويل من التطوير والتطبيق. ولكننا سنركز في هذه المقالة على صياغة النقاط الأساسية المتعلقة بالشبكات العصبونية الاصطناعية الرئيسية، وخاصة تلك المتعلقة بنماذج اللغة الكبيرة (LLM و Large Language Models) القائمة عليها، وذلك حسب ما وصلت إليه التطورات في هذا المجال حتى الآن. إذ لا ينبغي أن يُساء فهم مصطلح "لغوي" - فكل عنصر يُحوّل إلى سلسلة من الأصفار والآحاد، مثل الكتب والصور الرقمية وبيانات التقييم وشبكات دفع العملات المشفرة وتقلبات أسعارها ومقاطع الفيديو وما شابها، يُمثّل "بيانات" بلغة متخصصة من منظور الذكاء الاصطناعي.

وبتعبير أدق، تُمثل الشبكة العصبونية الاصطناعية سلسلة من العمليات الحسابية التي تُطبق على أعمدة البيانات الأولية (الناقلات) لتحويلها إلى ناقل النتيجة النهائي. على سبيل المثال، تقوم نماذج اللغة الكبيرة النموذجية (LLM) بمعالجة النص الأصلي، المقدم كسلسلة من الرموز الأبجدية (عادة ما تكون مرتبة في سطر أو عمود)، وتحويله إلى سلسلة جديدة من الرموز في المخرَج. ويكشف اختبار هذه المقالة بواسطة الذكاء الاصطناعي عن

[1] https://cbr.ru/press/event/?id=17177.

وجود عمود طويل من الحروف. ويمكن إدخال النص إلى نموذج الذكاء الاصطناعي مع إضافة عمود سؤال للحصول على إجابة بنعم أو لا أو إجابة مفصلة أو ترجمة إلى لغة أخرى. كما يمكن تمثيل مجموعة متنوعة من العناصر في شكل عمود من الرموز، مثل الصور ومقاطع الفيديو وبيانات التجارب العلمية ومجموعات المعاملات وغيرها الكثير.

وفي حد ذاته، يُعد التحويل بسيطًا بشكل مدهش (مع إمكانية إضافة صورة توضيحية). نأخذ العمود الأول ونحوله إلى العمود الثاني وفقًا لقاعدة بسيطة: تمثل كل خلية في العمود الناتج مجموع جميع القيم في العمود الأول مضروبة بمعاملات عشوائية Aij، والتي تشكل جدولًا (مصفوفة). في المرحلة التالية، تخضع القيم المستخرجة في كل خلية من العمود الثاني لعملية تحويل باستخدام معادلات بسيطة تعمل على تقليل القيم الصغيرة وزيادة القيم الكبيرة، مما يؤدي - إن صحّ التعبير - إلى تعزيز تباين النتائج. بعد ذلك، وباستخدام نفس القاعدة ومصفوفة Aij، يتم استخراج العمود الثالث من العمود الثاني، وتستمر العملية حتى الوصول إلى عمود الناتج. تشكل مصفوفة المعاملات، إلى جانب صيغة التحويل والعمود - طبقة واحدة، ويكون العدد المطلوب من الطبقات قليلًا على نحوٍ مدهش. وقدم روزنبلات في عام 1958 دليلاً على أن أي مهمة لتصنيف الصور (مثل التعرّف على الأرقام والحروف، وتمييز السيارات والمشاة، ومجموعة واسعة من المهام الأخرى) يمكن حلها باستخدام شبكة عصبونية اصطناعية مكونة من ثلاث طبقات.

ما هي المصادر التي يستقي منها الذكاء الاصطناعي مصفوفات Aij؟ الإجابة بسيطة: من خلال عملية التدريب. ويتميز هذا النهج ببساطته. في المرحلة الأولى، يتم تحديد المعاملات عشوائيًا، ثم يقوم الذكاء الاصطناعي بتقديم سلسلة الإدخال مع تزويدها بإجابة صحيحة معروفة مسبقًا، مثل طرح سؤالٍ تكون إجابته معروفةً مسبقاً بـ "نعم" أو "لا". ويعطي الذكاء الاصطناعي إجابة، قد تكون عشوائية في البداية. وفي حال نجاحه في تخمين الإجابة الصحيحة، يتم طرح السؤال اللاحق عليه. أما في حال عدم إعطاء الإجابة الصحيحة، تُعدّل المصفوفة بشكل طفيف ويُطرح السؤال مرة أخرى. ثم تُعدّل المصفوفة مرة أخرى ويُطرح السؤال من جديد، ويستمر ذلك حتى يتم الوصول إلى الإجابة الصحيحة. يُعاد تكرار عملية الاختيار المذكورة مرارًا وتكرارًا عددًا لا يحصى من المرات حتى يتم التوصل إلى الإجابة الصحيحة في معظم الحالات (أو في جميعها). وبمجرد استيفاء معايير الأداء المحددة، يعتبر الذكاء الاصطناعي قد اكتسب مهارات كافية ليتم دمجه في الحياة الواقعية للتعامل مع أسئلة جديدة.

ظلت فكرة إنشاء ذكاء اصطناعي تراود مخيلة البشر منذ القدم. وبالحديث عن نماذج اللغة، يعود الفضل إلى عالم الرياضيات الروسي ماركوف في طرح أولى الأفكار عام 1913. ومع ذلك، لم تتوفر الشروط الأساسية من برامج وأجهزة وقدرات سياقية لتمكين تدريب ذكاء اصطناعي قوي إلا مع حلول عام 2022 تقريبًا، وشهدنا بعد ذلك ظهورًا سريعًا لنماذج معالجة النصوص والصور.

وفي الوقت نفسه، أظهرت الدراسات أن نماذج اللغة الكبيرة (LLM) القائمة على الشبكات العصبونية الاصطناعية تتمتع بقدرات شاملة. وتاريخيًا، اتسمت أبحاث الذكاء الاصطناعي بالتعددية وتنوع المسارات المتبعة، دون وجود روابط وثيقة بينها. ولأغراض تحليل النصوص، تم توظيف خوارزميات مغايرة تمامًا لتلك المستخدمة في مجال الألعاب أو تشغيل الطائرات بدون طيار. وقد أثبتت الشبكات العصبونية الاصطناعية للتعلم العميق قدرتها على التكيف مع مختلف أنواع المهام، حيث حققت نتائج ممتازة في معالجة مختلف أنواع المهام بعد تحويلها بطريقة ما إلى ناقلات بيانات. وساعد ذلك على تجنب تشتت الموارد والتركيز على اتجاه واحد ذا أهمية استراتيجية. وشهد استخدام الذكاء الاصطناعي انتشارًا سريعًا في مختلف مجالات العمل البشري، بدءًا من الفن الرقمي وصولًا إلى المجال الطبي. وكما كان متوقعًا، لم يبقَ المجال المالي بمعزل عن التطورات.

تطبيقات الذكاء الاصطناعي في القطاع المالي

نظرًا للتركيز الأساسي على نماذج اللغة في البداية، فقد تم تبني هذه النماذج بشكل أسرع في مجال التواصل مع العملاء. تشمل بعض الأمثلة على هذه التطبيقات روبوتات الدردشة للدعم الفني، ونظام تحليل الطلبات، ونظام مراقبة أداء موظفي مراكز الاتصال وغيرها الكثير. ويمثل تحسين أوصاف المنتجات أحد الأمثلة على هذا النوع من الأنشطة. في هذا الإطار، تُستخدم نماذج لغوية عامة، بينما تقتصر التطبيقات ذات الصلة بالمجال المالي على سياقات محددة.

يستند استخدام الذكاء الاصطناعي في تحسين المنتجات ذاتها إلى تحليل سلوكيات العملاء. يتم تدريب الذكاء الاصطناعي في هذه الحالة على مجموعة من متغيرات المنتج المختلفة، مثل مبلغ الوديعة، ويتعلم الذكاء الاصطناعي كيفية تحسين هذه المتغيرات لتحقيق النتيجة المرجوة، مثل زيادة مبيعات المنتج. وقد بُذلت محاولات أكثر طموحًا لتحليل سلوك العميل وتحسينه بشكل عام، لكن وبشكل غير متوقع، تبين أن سلوك العملاء يصعب التحكم به.

يُعد التقييم الائتماني مجالاً هامًا يُمكن من خلاله الاستفادة من قدرات الذكاء الاصطناعي. إذ يُتيح الذكاء الاصطناعي تحليل البيانات وتقييم العملاء باستخدام أساليب مبتكرة تربط بين مختلف المعايير، مما يُتيح على سبيل المثال، تحسين عملية منح القروض بشكل أكثر فعالية.

وتُراهن البنوك بشكل كبير على توظيف الذكاء الاصطناعي لحماية أنظمتها المعلوماتية. إذ يخضع أي طلب خارجي يتم إرساله إلى نظام الصراف الآلي لتحليل

الذكاء الاصطناعي لتحديد ما إذا كان ناتجًا عن عميل مُعتمد أو محاولة اختراق إلكتروني. وتعتمد عملية التدريب على تحليل مجموعات بيانات ضخمة من السجلات، لتحديد أنماط الطلبات المشروعة ومحاولات الهجوم.

وهذه ليست سوى أمثلة قليلة، إلا أنها تمثل مجرد غيض من فيض من إمكانات التطبيق المتنوعة التي تتوسع باستمرار.

تقنيات الذكاء الاصطناعي في مكافحة غسل الأموال وتمويل الإرهاب

وقد أدرك المختصون منذ فترة طويلة الأهمية العملية لاستخدام الذكاء الاصطناعي في مكافحة غسل الأموال وتمويل الإرهاب. في عام 2018، نوهت شركة "كيه بي إم جي" الدولية المحدودة (KPGM) إلى جانب رابطة أخصائيي مكافحة غسل الأموال المعتمدين (ACAMS) إلى تسارع ملحوظ في تبني تقنيات الذكاء الاصطناعي لمكافحة غسل الأموال. وشددت هيئة العمل المالي المعنية بمكافحة غسل الأموال وتمويل الإرهاب وانتشار التسلح (FATF) على هذا الأمر بشكل خاص في ورقتها التحليلية.[2] وفي هذه المرحلة، نحدد الاتجاهات المحورية التالية:

1. تحليل مخاطر العملاء عند التقدم بطلب للحصول على الخدمة.

في هذه الحالة، يعتمد تدريب الذكاء الاصطناعي على مجموعة بيانات ضخمة تضم معلومات عن العملاء السابقين للمصارف (شركات وأفراد) مع إمكانية تقييم جودة كل عميل لاحقًا. إذ يُتيح التدريب تصنيف العملاء بشكل أكثر كفاءة من حيث المخاطر، مما يساهم بشكل كبير في حل مشكلة التحوط من المخاطر. وتشير بيانات بنك "Sber" وبنك "HSBC" إلى أن هذا النهج يُمكن من توفير الخدمات لعدد كبير من العملاء الذين كانوا يتعرضون لرفض غير مبرر عند اتباع عملية المراجعة التقليدية لدراسة الطلبات.

2. تحليل العمليات الجارية.

يعتمد التحليل الكلاسيكي للعمليات على أنماط محددة مسبقًا، مثل تقسيم المدفوعات، ودمجها، واستخدام وسطاء مشبوهين وما إلى ذلك. بيد أن المخططات العملية غالبًا ما تكون أكثر تعقيدًا ولا يمكن تحليلها باستخدام أساليب التحليل الرسمي. إذ يوفر الذكاء الاصطناعي أدوات متقدمة للتحرر من قيود المعايير الرسمية وتحسين عملية تتبع العمليات المشبوهة والإبلاغ عنها بشكل أكثر فعالية. كما تلجأ العديد من المؤسسات المالية البارزة، بما في ذلك بنك VTB و Sber و Standard Chattered و JPMorgan Chase و Danske Bank إلى استخدام هذه الأساليب كجزء من استراتيجياتها المالية. وتجدر الإشارة إلى أن هذه الآليات فعالة أيضًا ليس فقط في التحكم بأنظمة الدفع التقليدية، بل أيضًا في أنظمة الدفع الموزعة. وعلى وجه الخصوص، كشفت هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) النقاب في أغسطس 2020 عن نموذج أولي لنظام تحليل معاملات العملات المشفرة يعتمد على تقنية الذكاء الاصطناعي. وقد أطلق على النظام اسم "البلوكشين الشفاف" وبدأ العمل به في فبراير 2021.

3. تحليل الانتماءات باستخدام الرسوم البيانية

تتمثل المهمة التقنية الأكثر أهمية لمكافحة غسل الأموال وتمويل الإرهاب في الكشف عن العلاقات المستفيدة والارتباطية المخفية بين أطراف هياكل الدفع المعقدة. ويُتيح الذكاء الاصطناعي تحليل كل من المعاملات المالية والبيانات الخارجية (مثل البيانات المدونة في سجلات الشركات والمعلومات حول الملكية المُستمدة من مصادر خارجية وما إلى ذلك) لإنشاء رسوم بيانية توضح العلاقات بين الشركات والأفراد، حيث تمثل العُقد في هذه المخططات الكيانات، بينما تعكس الروابط بين العُقد درجة الارتباط بين هذه الكيانات. ومن خلال هذه الطريقة، يتم تحديد العلاقات الرسمية وغير الرسمية بين الأطراف المستقلة ظاهريًا في معاملات الدفع بشكل فعال.

4. مراقبة الامتثال البشري

شهد هذا النموذج أول تطبيق له في مجال مراكز الاتصال التي يديرها "بشر" (مثل حلول JustAI). وهناك جملة من التحديات التي يواجهها العملاء والتي لا يمكن للذكاء الاصطناعي في مراحله الحالية معالجتها. ومع ذلك، يُتيح تحليل الحوارات النصية والصوتية للنظام تقييم جودة عمل الموظفين

[2] Opportunities and challenges of new technologies for AML/CFT https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

البشريين وتقديم توصيات لتحسينها. وعلى نحو مماثل، يستطيع الذكاء الاصطناعي ممارسة الرقابة على عمل الامتثال "البشري" من خلال استخلاص الأخطاء الشائعة، وتقييم أداء الموظفين من حيث الجودة، وتقديم التوصيات المناسبة.

5. تحليل التغييرات في الأنظمة القانونية

تُعلق آمال عريضة على توظيف الذكاء الاصطناعي في مجال المعالجة الآلية للوثائق التنظيمية. إذ يمنح ذلك فرصة لتحسين سياسات البنك الداخلية بفاعلية تماشيًا مع التغييرات في متطلبات الجهة التنظيمية.

6. تحليل العقود

في أنشطة الامتثال، يقضي موظفو الامتثال وقتًا طويلاً في مراجعة المستندات المقدمة للتأكد من مصدر الأموال وأهداف تحويلها. وتُشكل هذه العملية عبئًا كبيرًا نظرًا لخصوصية بيانات هذه الوثائق وتنوعها. وهنا يبرز دور الذكاء الاصطناعي الذي يتميز بقدرته على تحليل البيانات المستمدة من الوثائق للتأكد من صحتها ومطابقتها لأهداف المعاملة.

7. إنشاء المؤشرات الأساسية.

وكما هو مذكور أعلاه، يمكن للذكاء الاصطناعي أن يُحدث نقلة نوعية في نموذج الامتثال من خلال الانتقال من اعتماد مجموعة محددة من المعايير إلى تحليل شامل لكافة العمليات. ومن الممكن أيضًا تطبيق نهجٍ معاكس، حيث يمكن تدريب الذكاء الاصطناعي على مجموعة من العمليات المشبوهة، مع تكليفه باختيار مجموعة محدودة من المعايير ذات الفعالية العالية لتحليلها بسرعة.

8. تحديد الهوية

تُشكل مهمة تحديد هوية العميل حجر الزاوية في مجموعة من المهام المنفصلة. وتتخطى هذه المهام حدود المجال المالي لتشمل عملية تحديد هوية الشخص بشكل عام. وتتضمن إجراءات التحقق من الهوية تحليل صور العميل ووثائقه، وتحليل الكلام والتسجيلات المرئية، وأي أساليب أخرى تُحسّن من دقة التحقق من هوية الشخص، سواء عن بُعد أو في وضع الحضور الشخصي.

نقاط ضعف الذكاء الاصطناعي في مجال مكافحة غسل الأموال وتمويل الإرهاب

على الرغم من جميع مزايا الذكاء الاصطناعي، إلا أنه يتميز بخصائص فريدة تشكل تهديدًا محتملًا في أي مجال من مجالات التطبيق، خاصة في المجال المالي. وعلى النقيض من الأساليب الخوارزمية التي تُمكّن من تحليل آلية اتخاذ قرارات الذكاء الاصطناعي، فإن الشبكات العصبونية لا تُتيح، بشكلٍ مُطلق، تفسير تلك القرارات من خلال مفاهيم الخوارزميات. على سبيل المثال، من التحديات التي نواجهها في تحليل العمليات المشبوهة عدم القدرة على عزل أقسام مصفوفات Aij المسؤولة عن البحث عن التجزئة والتوحيد، وغيرها من العمليات. بالتالي، لا يمكننا التحقق من موثوقية أداء الخوارزمية إلا بطريقة إحصائية من خلال إسناد كمية كبيرة من المهام إليها وتقييم جودة النتائج الحاصلة. وعلى الرغم من ذلك، لا تزال هناك بعض المشكلات الشائعة، مثل:

- تشوهات الذكاء الاصطناعي، عندما ينتج الذكاء الاصطناعي بناءً على بيانات صحيحة نتائج لا تمت للواقع بصلة. وقد شهدنا حالات قام فيها الذكاء الاصطناعي بوضع سوابق قضائية جديدة أو اقتراح عروض خصم غير حقيقية.
- مناطق عدم اليقين، عندما يعطي الذكاء الاصطناعي نتائج خاطئة تمامًا عند إجراء تغييرات بسيطة على بيانات المدخلات. ولا تزال طبيعة هذه الظاهرة غامضة تمامًا، مما يُشكل عقبة أمام السيطرة عليها.
- الإفراط في التعلّم، مع ازدياد حجم البيانات المدخلة وجودتها، قد تحدث ظاهرة غريبة تتمثل في تراجع جودة الاستجابات وظهور العديد من المشكلات الأخرى.

ويُعدّ استخدام أنظمة متعددة المكونات، حيث تقوم شبكة عصبونية اصطناعية واحدة بمراجعة نتائج شبكة أخرى، من بين الوسائل ذات الفعالية النسبية. وعلى هذا النحو، لا تزال هذه المشكلات تفتقر إلى حلول نهائية في الوقت الحالي.

استخدام الذكاء الاصطناعي لأغراض مكافحة غسل الأموال وتمويل الإرهاب

لم يكن مفاجئًا أن تثير أداة كهذه ذات قدرات هائلة اهتمام المجرمين وسعْيهم للاستفادة منها بشكلٍ غير قانوني. لا تتوفر لدينا حاليًا نماذج محددة لاستخدام الذكاء الاصطناعي في عمليات غسل الأموال أو تمويل الإرهاب، ولكن يمكننا استعراض بعض الاحتمالات الواردة بشكل كافٍ على النحو التالي: استخدام الروبوتات للتواصل مع البنوك خلال عمليات التسجيل، وتصنيع هويات شخصية مزيفة، ومحاكاة الشخصية في عمليات التعريف عن بُعد، وتحسين نصوص الهندسة الاجتماعية، وتحسين مخططات المعاملات الإجرامية وما إلى ذلك. وتُمثل هذه المسألة موضوعًا شائكًا يتطلب تحليلًا عميقًا في مقالٍ مستقل.

من المؤكد أن الذكاء الاصطناعي سيُوظف بكفاءة في المجال المصرفي بشكل عام وفي مجالات مكافحة غسل الأموال وتمويل الإرهاب بشكل خاص. ويرى الكاتب أن التوقعات الحالية حول قدرات الذكاء الاصطناعي مبالغ فيها، وأن هذه التوقعات ستواجه مراجعة نقدية صارمة في المستقبل القريب. على الرغم من ذلك، لا بد من جعل تحليل قدرات الذكاء الاصطناعي وتطوير منهجية لمكافحة الاستخدامات الإجرامية للذكاء الاصطناعي من بين أهم أولويات المحللين والممارسين في مجال مكافحة غسل الأموال وتمويل الإرهاب.

توظيف الذكاء الاصطناعي في أعمال هيئة الرصد المالي

لقد شهد استخدام الذكاء الاصطناعي في الآونة الأخيرة ازديادًا ملحوظًا في مختلف مجالات العمل، ليصبح موضوعًا رئيسيًا في جميع قطاعات العمل. في هذا السياق، تلعب المصارف دورًا رائدًا في تبني المنتجات والحلول التقنية المتطورة في مجال تكنولوجيا المعلومات، مما يجعلها بمثابة محرك رئيسي للتقدم في هذا المجال.

ميخائيل سيرغيفيتش برونين،
نائب رئيس مجلس إدارة بنك "بي اس بي" - مدير إدارة الرقابة المالية، حائز على درجة دكتوراه في العلوم الاقتصادية.

ونلاحظ وجود العديد من الحلول الناجحة في مجال تمويل العملاء وخدمات المعاملات، خاصةً في المجالات التي تعتمد بشكل كبير على التحليل الآلي لبيانات العملاء وسلوكهم.

ومن خلال تحليل هذه المنطقية، يتضح أن مجال مُكافحة الأنشطة غير القانونية، الذي يُركّز على رصد النشاط المشبوه للعملاء، يوفر بيئة مثالية لاستخدام أدوات التعلم الآلي، أحد مجالات الذكاء الاصطناعي.

في إطار العمل التحليلي لوحدة الرقابة المالية في بنك "بي اس بي"، شرعنا بإطلاق تجارب باستخدام أدوات التعلم الآلي في عام 2020. تركزت جهودنا بشكل رئيسي على نماذج رياضية متنوعة للكشف عن السلوكيات الشاذة في عمليات الدفع التي يقوم بها عملاؤنا.

واستطاعت خوارزمية هجينة تجمع بين شجرة القرار والانحدار اللوجستي تحقيق نتائج نوعية متميزة. إلا أنه على الرغم من ذلك، واجهنا صعوبات في تحقيق تحسينات جوهرية في الأداء، حيث لم تتفوق فعالية هذا النموذج بشكل كبير على أداء المحللين الخبراء.

وفي المقابل، حققنا تجربة ثمينة ساعدتنا في وقت لاحق على بلورة استراتيجية محددة لأعمالنا.

في المقام الأول، تمكنا من رصد ظاهرة جديرة بالملاحظة. ففي معظم الحالات، لا يُظهر سلوك الدفع الخاص بالعملاء المشتبه بهم أيّ انحراف عن سلوك قاعدة العملاء ككل. ويُعزى ذلك إلى أن العملاء المشتبه بهم، وحرصًا منهم على عدم كشفهم، يُضطرون إلى "المحاكاة" بشكل مستمر.

إنّ هذا التكيّف والتقليد للسلوك الطبيعي للعملاء الملتزمين يُؤدّي إلى أن تُصنّف النماذج الرياضية السلوك غير القياسي لبعض العملاء الملتزمين على أنه سلوك مشبوه، بدلاً من تصنيف سلوك العملاء المشبوهين أنفسهم. وتنتشر هذه السمة بشكل خاص بين فئات محددة، مثل أصحاب المشاريع الطموحين من الشباب أو في المجالات التجارية النادرة، حيث تُفسر السلوكيات غير النمطية في سداد المدفوعات بخصائص طبيعة عمل هذه المجالات نفسها.

ثانيًا، يؤدي التكيّف المستمر لسلوك العملاء ذوي المخاطر العالية مع السلوك الطبيعي المُعتاد، الذي لاحظناه، إلى تغييرات مستمرة في البيانات التحليلية نفسها. وعلى إثر ذلك، تفقد النماذج التي كانت تتمتع بفعالية ممتازة بالأمس كفاءتها بسرعة وتصبح بحاجة إلى استبدالها بأخرى جديدة. وإلى جانب ذلك، كلما زادت كثافة مراقبتنا لهذا

المجال باستخدام أدوات التعلم الآلي ونماذج التحليل المعقدة، كلما بدأت في التغيير بشكل أسرع.

وهذا يجعل استخدام أدوات الذكاء الاصطناعي في مجال الرقابة المالية يختلف اختلافًا كبيرًا عن استخدامها في المجالات الأخرى. على سبيل المثال، في سياق البيع بالتجزئة، تُظهر نماذج السلوك العام للمستهلكين داخل المتجر دقة عالية ومتسقة عند تحليلها باستخدام مجموعات بيانات كبيرة. وبفضل هذه المعلومات، يصبح من السهل التنبؤ بسلوك المشتري داخل المتجر.

ومن خلال تقييمنا لمستوى التعقيد المرتبط بمهمة دمج الذكاء الاصطناعي في عمليات الرقابة المالية، تأكدنا من كفاءتنا في مجال تقييم مخاطر غسل الأموال وتمويل الإرهاب، إلا أننا واجهنا نقصًا في الخبرة الداخلية المتعلقة بتطبيق أدوات التعلم الآلي. ونتيجة لذلك، اتخذنا قرارًا في عام 2022 ببدء توظيف محللي بيانات متخصصين ضمن وحدة مكافحة غسل الأموال وتمويل الإرهاب.

وينبغي التمييز بوضوح بين محلل البيانات ومحلل العملاء المعتاد الذي يتولى مهام التحقيقات المتعلقة بمكافحة الأنشطة غير القانونية، حيث تتباين مهامهم بشكل كبير. إذ يُمثّل هذا الموظف حالة مختلفة تمامًا، ويستدعي تواصلًا فرديًا مُخصّصًا وأدوات مهنية متخصصة. ونتيجة لذلك، ظهرت في سياق عملنا "بيئات اختبار" مخصصة للبيانات، مدعومة بأجهزة كمبيوتر قوية، وبرامج مكتوبة بلغة بايثون (Pyton)، وأدوات تحليلات الأعمال (BI) لتصور البيانات.

وبعد ذلك، قمنا بإنشاء بيئة عمل تشاركية حيث تمكن محللو العملاء من طرح فرضيات بحثية مفتوحة حول طرق جديدة محتملة للكشف عن العملاء المشبوهين، بينما قام محللو البيانات بتحويل هذه الفرضيات إلى نماذج رياضية مناسبة. تمّ إدخال النماذج المُستخرجة في نظام التشغيل المُعتاد، وتم إرسال نتائجها مرة أخرى إلى محللي العملاء للتحقق من صحتها. وفي حال تراجع كفاءة نماذج العمل، يضع محلل العملاء فرضية لتحسينها، أو فرضية جديدة كليًا ضمن نطاق المخاطر ذاته، والتي يتم تحويلها وفقًا للخطوات المذكورة سابقًا إلى محلل البيانات لتنفيذها.

لقد أثمرت عملية تشكيل بيئة تواصلية مشتركة تضم محللي العملاء ومحللي البيانات عن تحقيق نتائج تآزرية ناتجة عن العمل الجماعي، بالإضافة إلى تبادل سريع لرفع مستوى مهارات الموظفين وتطوير كفاءات جديدة لديهم. كما أصبح محللو البيانات أكثر دراية بالمجالات ذات الصلة. وهنا نود التأكيد على أن الهدف من ذلك لم يكن تحويلهم إلى محللي عملاء، حيث لدينا بالفعل متخصصون مؤهلون في هذا المجال. ولكن أدى التقارب بينهم إلى إدراكهم لأهمية أساليب العمل على البيانات في مجال مكافحة غسل الأموال، حيث ساعدهم ذلك على فهم كيفية تطبيق هذه الأساليب بشكل فعال. واستنادًا إلى تحليلهم، لجأ محللو البيانات إلى استخدام أدوات معالجة بيانات مختلفة تناسب كل فرضية على حدة.

وبالمثل، قام محللو العملاء بنفس الخطوة. في الماضي، كانت القضايا المتعلقة بتكنولوجيا المعلومات تبدو معقدة وبعيدة المنال بالنسبة لهم، ولكن بعد التعرف على كيفية عملها، أصبحوا قادرين على تولي مهام محددة من وظائف محلل البيانات. علاوة على ذلك، سمح التعرف على أدوات تحليلات البيانات لمحللي العملاء التقليديين بالبدء في وضع فرضيات أكثر تطورًا للكشف عن المخاطر.

وبشكل عام، تمثل هذه تجربة مثيرة للاهتمام إلى حد ما، تم تحديدها من قبلنا على أنها تعاون بين الذكاء الطبيعي والذكاء الاصطناعي.

تمّ تحويل سير العمل المذكور إلى نظام إنتاج مستمر من خلال دمجه في خط تجميع فعال، ممّا يُتيح:

1. الاستجابة الفورية للمخاطر الجديدة وأنواع الأنشطة المشبوهة للعملاء، والتي نتلقى معلومات عنها من قبل البنك المركزي الروسي وهيئة الرقابة المالية الروسية (روسفينمونيتورينغ). ولا تتجاوز مدة اختبار نماذج المخاطر الجديدة يومي عمل.

2. الارتقاء المتواصل بكفاءة قواعد التحليل المُستخدمة لمراقبة عمليات العملاء عبر الإنترنت وغير المتصلة بالإنترنت. وبالتالي، يمكننا الحفاظ على كفاءة العمليات دون الحاجة إلى زيادة عدد الموظفين مع استمرار نمو قاعدة العملاء.

ومن خلال تقييمنا لمستوى التعقيد المرتبط بمهمة دمج الذكاء الاصطناعي في عمليات الرقابة المالية، تأكدنا من كفاءتنا في مجال تقييم مخاطر غسل الأموال وتمويل الإرهاب، إلا أننا واجهنا نقصًا في الخبرة الداخلية المتعلقة بتطبيق أدوات التعلم الآلي.

▲ النقاش المفتوح في ختام الدورة الثالثة للأولمبياد الدولي للأمن المالي

3. اختبار كمية كبيرة من الفرضيات الداخلية لاكتشاف أنواع جديدة ومتغيرات محدثة لأنماط المعاملات المشبوهة. ويتم تحويل ما لا يقل عن 10 فرضيات من مجرد أفكار إلى خوارزميات قابلة للتنفيذ كل ربع سنة.

أودّ أن أُشارككم ملاحظة أخرى لفتت انتباهي. ففي شهر أكتوبر من عام 2023، وبمناسبة الأولمبياد الذي رعته هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) حول الأمن المالي، قدّمنا ورشة عمل للطلاب تناولت مشروعنا التحليلي المسمى "أنماط". وهذا مشروع داخلي لتطوير أداة جديدة عالية الكفاءة للكشف عن المعاملات المشبوهة في أنشطة العملاء.

وفي الواقع، أصبحت مشاركتنا في هذا المشروع ممكنة بفضل التقدم الذي أحرزناه في مجال تعلم الآلة بالتعاون مع محللي البيانات، ومهارات صياغة الفرضيات التحليلية التي طورها محللو العملاء لدينا.

ونحن نقف أمام الطلاب ونشاركهم هذا الانطباع حول التعاون المثمر ونُفكر بكيفية روعة تجسيد هذه المهارات في المستقبل في موظف واحد يقوم بتحليل العملاء وتركيب الفرضيات ثم برمجتها بنفسه وتطبيقها لكشف العمليات عالية المخاطر.

ونُواجه استفسارات من الجمهور حول تأخر تطبيق هذه المبادرات حتى الآن. تصوروا أن طلابنا المشاركين في أولمبياد مكافحة غسل الأموال الذي ترعاه هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) يتطلعون لأن يكونوا من هذا النوع من المتخصصين في المستقبل. لا يقتصر الأمر على تخيلهم هذا فحسب، بل إنهم يعدون أنفسهم بشكل منهجي لمثل هذا الشكل من العمل، من خلال تراكم المعرفة وتطوير المهارات اللازمة لهذا الغرض.

ومع جيل شاب كهذا، ستشهد مراقبة مُكافحة الأنشطة غير القانونية قفزة نوعية نحو مستقبل مشرق. مستقبل يتعاون فيه الذكاء الطبيعي والذكاء الاصطناعي بشكل فعال ويتطور.

أليكسي غيليتا-

"سوق التكنولوجيا المالية في روسيا هو أحد أكثر الأسواق ابتكارًا وتقدمًا في العالم من الناحية التقنية "

تخضع مبادرات التكنولوجيا المالية لتقييم مستقل من قبل خبراء قبل تنفيذها. ويتم تقييم مشاريع التكنولوجيا المالية من منظور المخاطر والتهديدات المحتملة، مع الأخذ في الاعتبار فوائدها للمواطنين والدولة والشركات. ويُجري مركز التحليل التابع للحكومة الروسية هذه التقييمات، من خلال مجموعة الامتثال الرقمي. ولتوسيع نطاق فهمنا لدور هذه المجموعة وأهمية الوعي المالي في أيامنا هذه، أجرى فريق تحرير المجلة حوارًا حصريًا مع السيد أليكسي غيليتا، رئيس مجموعة الامتثال الرقمي.

1. ترتبط هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) بعلاقات تعاون وثيقة مع المركز التحليلي التابع للحكومة الروسية في مجالات شتى. وشمل ذلك تنفيذ مشاريع مع مجموعة الامتثال الرقمي التي تترأسها. هلّا أخبرتنا المزيد عن مهام هذه المجموعة وكيفية تعرّفك شخصيًا على هذا المجال.

انطلاقًا من مبادرة حكومة روسيا الاتحادية، شهد عام 2020 تأسيس قطاع "الامتثال الرقمي" كمسار متخصص جديد للقطاع العام، وذلك تحت مظلة المركز التحليلي التابع لحكومة روسيا الاتحادية. وتتمثل مهامه الرئيسية في التنسيق بين الإدارات المختلفة عند دراسة مبادرات التكنولوجيا المالية وتوفير الخبرة التحليلية والقانونية الشاملة والمستقلة، مع مراعاة أفضل الممارسات والتجارب الدولية في هذا المجال. ونحن نُركز في عملنا على مجالات تتضمن اكتشاف المخاطر والتهديدات، إلى جانب تعزيز سوق التكنولوجيا المالية بما يتوافق مع احتياجات الدولة والشركات والأفراد.

أما فيما يتعلق بأول اتصال لي مع نظام "الامتثال" فكان خلال فترة دراستي الجامعية. فأنا خريج القسم التخصصي في معهد الأمن المالي والاقتصادي التابع لجامعة موسكو للهندسة الفيزيائية، والذي تم إنشاؤه بدعم من هيئة الرقابة المالية الروسية (روسفينمونيتورينغ). وقد تولى التدريس موظفون متفرغون في الوكالة، مما أتاح تلقي المعرفة النظرية والتطبيقية على حدٍ سواء، بما في ذلك من خلال خضوع المتدربين لتدريب عملي في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ). كما أنني اكتسبت مهارات واسعة ومعرفة عميقة في مجال الامتثال خلال عملي في القطاع المصرفي. فقد لعبتُ دورًا هامًا في إنشاء نظام إدارة المخاطر التنظيمية (الامتثال) على مستوى المصرف الرئيسي، وقمتُ بتنسيق جهود المؤسسات المالية الروسية والأجنبية التابعة لمجموعة المصرف في مجال مكافحة غسل الأموال وتمويل الإرهاب، وإدارة المخاطر التنظيمية (الامتثال). وكان من الأهمية بمكان ضمان الالتزام

بالمعايير الموحدة للمجموعة المصرفية، مع الأخذ بعين الاعتبار الخصوصيات التشريعية المحلية للبلاد في مجال الامتثال.

2. على ماذا تركز جهود مجموعة الامتثال الرقمي في هذه المرحلة؟

يمكننا هنا تحديد ثلاثة محاور رئيسية:

1. المجالات الواقعة في "المنطقة الرمادية" والتي تتطلب تكوين خبرات وتوصيات شاملة لاتخاذ القرارات الإدارية لاحقًا على المستويين الاتحادي والإقليمي. وتشمل هذه المجالات، على سبيل المثال لا الحصر، استخراج العملات الرقمية وتداولها. كما تتطلب طبيعة العمل الانخراط في مشاريع ملموسة، يُبادر بها ممثلو الأعمال، تهدف إلى تحسين أنظمة الأتمتة، وتطبيقات سلسلة الكتل (بلوكشين)، وحلول الدفع.

2. الكشف عن المخاطر والتهديدات التي تتعرض لها المنظومة المالية الوطنية والمجال الاجتماعي والاقتصادي. تمت دراسة الأنشطة المتعلقة بالكشف عن المعاملات المصرفية غير القانونية (التشفير الخاطئ)، والاحتيال تحت ستار المدفوعات الاجتماعية واسترداد النقود، والموارد غير القانونية خلال COV-ID-19 والعديد من الأنشطة الأخرى. ودون التعمق في تفاصيل سير العمل والنتائج، تطلبت مهمتنا فهمًا دقيقًا للأسباب الرئيسية لظهور التهديدات، وتصميم مسارات العملاء وعمليات العمل، وتحديد أكثر المناطق ضعفًا، وإنشاء تدفقات بيانات، وبناء لوحات تحكم تحليلية، والمشاركة في الأنشطة المشتركة بين الإدارات، وإعداد تقارير تحليلية تتضمن توصيات لتقليل أو القضاء على التهديدات التي تم تحديدها.

3. المساهمة في تطوير آليات الدفع. ويُمكن القول بثقة أن سوق التكنولوجيا المالية في روسيا يُعدّ من بين أكثر الأسواق ابتكارًا وتقدمًا تقنيًا في العالم، وذلك على الرغم من التحديات التي يواجهها نتيجة للضغوط الخارجية.

وعلى الرغم من ذلك، تُواجه بعض التحديات التي تتطلب تحديث الاستراتيجيات المُتبعة أو وضع أنظمة تنظيمية جديدة لتطوير البنية المالية. وفي سياق معالجة مهام كهذه، تُصبح ضرورة التواصل الدائم والفهم المتبادل بين ممثلي الجهات الفاعلة في عالم الأعمال، الذين يُطرحون مُقترحاتٍ جديدة لتطوير النظام المالي الوطني، وبين الجهات الحكومية المُختصة بضمان أمن هذا النظام، أمرًا لا غنى عنه.

ويُقدم مركز التنسيق التابع لحكومة روسيا الاتحادية منصة مثالية لتعزيز التفاهم بين جميع المشاركين في العملية، بما في ذلك تجاوز العقبات البيروقراطية وتحقيق تقدم هام في معالجة القضايا ذات الأهمية.

3. ما هي الممارسات في مجال التكنولوجيا المالية التي يمكنك تصنيفها على أنها محافظة؟

إجراءات التحقق من هوية العملاء، خاصة عند فتح حساب مصرفي. نلاحظ انتشارًا واسعًا للتحول الرقمي في مختلف القطاعات الاجتماعية والاقتصادية، مما أدى إلى تسهيل وتسريع إنجاز المهام الحياتية والمهنية للأفراد من خلال الاستفادة من الخدمات عن بعد، بينما لا يزال فتح حساب مصرفي يواجه عقبات كبيرة ويفتقر إلى نفس مستوى السلاسة والسرعة.

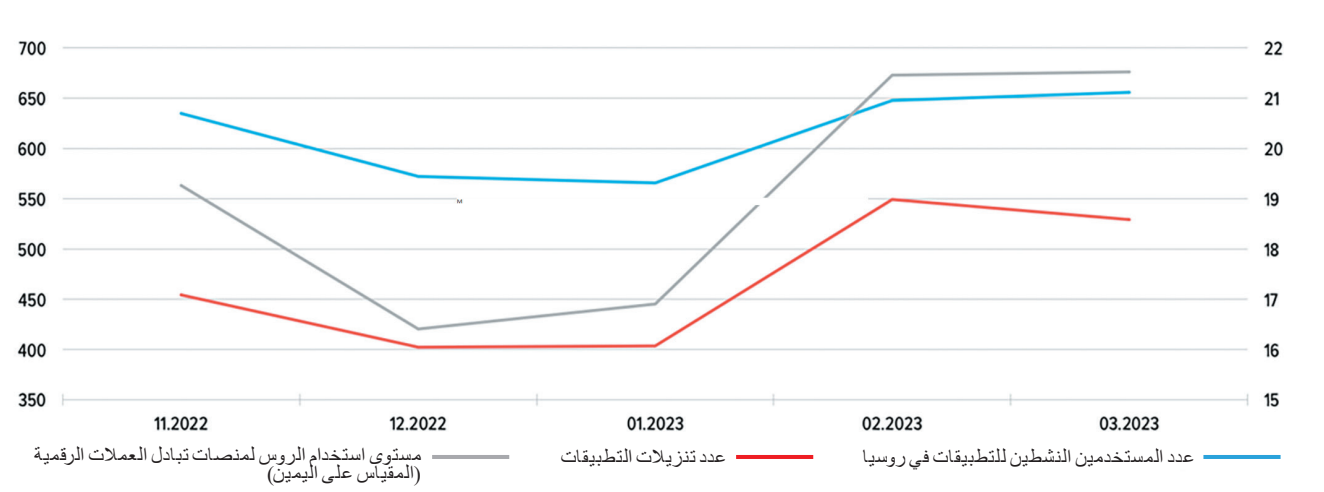
ورغم الصعوبات، فقد تمكنّا من إنجاز بعض التقدم في هذا المجال. بناءً على طلبات ممثلي القطاع المصرفي، تمّ من خلال المركز التنسيقي وبالتعاون مع البنك المركزي الروسي، وهيئة الرقابة المالية الروسية (روسفينمونيتورينغ)، والجهات المعنية الأخرى ذات الصلة، البدء في دراسة آليات تحديد الهوية عن بعد للمواطنين الأجانب عند فتح حساب مصرفي في مؤسسة ائتمانية روسية، ويُعرف هذا المشروع شعبيًا باسم "بطاقة السائح". ومن خلال الجهود المشتركة، تم إدخال التعديلات الضرورية على القوانين الوطنية المتعلقة بمكافحة الأنشطة غير القانونية. والآن بات بإمكان المواطنين الأجانب، عند استيفاء شروط ومعايير محددة، فتح حساب مصرفي عن بعد في مؤسسة ائتمانية روسية، والحصول على بطاقة "مير" افتراضية، وبدء تنفيذ المعاملات المالية قبل وصولهم إلى روسيا. وفي الوقت نفسه، تواصل المؤسسات الائتمانية إبلاغنا بالمخاوف التي تواجهها، والتي تتطلب جهدًا مشتركًا لحلها.

لا تزال مسألة تنظيم تعدين العملات الرقمية وتداولها موضع جدل ساخن منذ سنوات عديدة. وعلى الرغم من إدراك جميع الهيئات الحكومية للمخاطر والتهديدات التي تنطوي عليها العملات المشفرة، إلا أن الجدل لا يزال قائمًا حول كيفية التعامل معها. في الواقع، انقسمت الآراء حول التعامل مع العملات المشفرة ضمن النظام المالي الروسي إلى معسكرين: أحدهما ينادي بمنع تداولها للتقليل من المخاطر والتهديدات، بينما يدافع الثاني عن ضرورة وضع إطار تنظيمي واضح لجميع الفاعلين في السوق الروسية للعملات المشفرة. ومن وجهة نظري كخبير، ونظرًا لازدياد اهتمام* الناس بهذا المنتج الرقمي، أميل أكثر إلى نهج تنظيم سوق العملات الرقمية القائم على المخاطر، والذي يميز بين المشاركين الملتزمين بالقانون وغير الملتزمين. وفي حين أنّ حظر كل شيء يُعدّ أبسط الحلول، إلّا أنّ التحدّي الأكبر يكمن في كيفية ضمان امتثال السلطات والمؤسسات الائتمانية لهذا الحظر بشكلٍ فعّال على المدى الطويل، فقد يُفضي ذلك إلى فرض غرامات على المؤسسات الائتمانية وجعل التشريعات "غير قابلة للتنفيذ".

4. هل ترى أن التكنولوجيا الحديثة قادرة على تعزيز حماية مستخدمي الخدمات المالية من جرائم الاحتيال؟ أم أنها على العكس تمامًا، تُشكل أداةً جديدةً يستغلّها المجرمون لتنفيذ مخططاتهم؟

تُظهر هذه العبارة تناقضًا جليًا: فمن ناحية، قد تُساهم التقنيات الحديثة في تعزيز الأمن، بينما قد تُصبح من ناحية

تفاعل المستخدمين الروس مع منصات تداول العملات الرقمية



المصدر: https://www.cbr.ru/Collection/Collection/File/44007/4q_2022_1q_2023.pdf

أخرى أدوات إضافية يستخدمها المجرمون. كما تبين الممارسات العملية أن المُحتالين يتبنّون التقنيات الجديدة بشكل أسرع متجاوزين بذلك قدرة الأجهزة الأمنية على مُواكبة التطورات. وتأكيدًا لما سبق، نستعرض بعض الحالات الواقعية لجرائم الاحتيال التي استخدمت تقنيات "التزييف العميق" وتقنيات استبدال الصوت. ويتسم الوضع الحالي باتجاه سلبي، ومن المتوقع أن يستمر هذا الاتجاه في النمو.

5. ما هو دور الثقافة المالية في ظل التحول الرقمي؟ هل أجرى المركز التحليلي دراسات موضوعية في هذا المجال؟ وما هي المشاريع الواعدة في هذا المجال من وجهة نظرك؟

تعطي الإحصائيات الراهنة صورة مقلقة، حيث تُبيّن تزايدًا مُستمرًا في خسائر المواطنين عامًا بعد عام جراء عمليات الاحتيال الإلكتروني. ووفقًا لبيانات بنك روسيا، فقد قام المجرمون الإلكترونيون في عام 2023 باختلاس 15.8 مليار روبل من المواطنين الروس، وذلك حسب "استعراض العمليات التي تم تنفيذها دون موافقة عملاء المؤسسات المالية". وقد سجلت العمليات المصرفية التي نُفذت دون موافقة العملاء في عام 2023 زيادة ملحوظة بنسبة 11.48% عن عام 2022.

ونتيجة لجهود متضافرة من قبل مختلف الهيئات، باتت روسيا تمتلك قاعدة معرفية غنية لتعزيز الوعي المالي. في سياق الجهود المبذولة لتعزيز الأمن المالي، تُسجل هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) إنجازًا هامًا من خلال تنظيم الأولمبياد الدولي للأمن المالي، حيث تم تراكم خبرات عملية واسعة النطاق ستُفيد المواطنين في ظل التوجه المتزايد نحو التحول الرقمي. يمكن تنفيذ التدريب من خلال ألعاب الإنترنت والاختبارات وغيرها من الأشكال الرقمية التي يمكن التوصية بتطبيقها في المؤسسات التعليمية والحكومية والشركات والمؤسسات الأخرى.

6. الامتثال الرقمي في روسيا: هل هناك خصائص استثنائية؟

إذا كنت تسأل عن وظيفة الامتثال الرقمي في المؤسسات المصرفية الروسية، فإن أقسام الامتثال في هذه البنوك نفسها هي أفضل من يمكنهم شرحها لك. من الممكن مناقشة هذا الموضوع بشكل مفصل في إطار مجلس الامتثال الذي تنظمه هيئة الرقابة المالية الروسية (روسفينمونيتورينغ). وسأكون سعيدًا بالمشاركة في هذه المناقشة.

فيما يتعلق بالوحدة التي أترأسها، يمكن إبراز السمات الفريدة التالية: تعمل مجموعة الامتثال الرقمي ضمن منصة مركز التنسيق التابع لحكومة روسيا الاتحادية وتُشكل مركزًا خبيرًا مستقلًا لحكومة روسيا الاتحادية عند اتخاذ القرارات الإدارية.

لا تزال مسألة تنظيم تعدين العملات الرقمية وتداولها موضوع جدل ساخن منذ سنوات عديدة. وعلى الرغم من إدراك جميع الهيئات الحكومية للمخاطر والتهديدات التي تنطوي عليها العملات المشفرة، إلا أن الجدل لا يزال قائمًا حول كيفية التعامل معها

كشف الجرائم الإلكترونية وقمعها

50 **بوغدان ألكساندروفيتش شابليا**
مكافحة "المُتواطئين في الاحتيال" والعمليات عالية المخاطر بين الأفراد (P2P) تمثل أولوية قصوى في مجال الرقابة المالية

53 **فاديم ألكسندروفيتش أوفاروف،**
الأمن المعلوماتي في السوق المالية: مكافحة الاحتيال الإلكتروني في عمليات تحويل الأموال

57 **نيكولايفيتش راستاشينوف**
تقييد الوصول إلى المعلومات الممنوع نشرها في روسيا الاتحادية قبل الحصول على أمر قضائي

60 **رومان فياتشيسلافوفيتش موخلينوف**
"الاتجاهات الحالية في سوق مقدمي الخدمات المالية غير الشرعيين"

63 **أوليغ فياتشيسلافوفيتش كيبكايف**
توظيف التكنولوجيا الرقمية في عملية جمع المعلومات والبيانات التحليلية وغيرها، ومعالجتها وتحليلها، وغيرها من البيانات المستخدمة في أنشطة الادعاء: دراسة حالة لنظام المعلومات والتحليل "المكتب الإلكتروني للمدعي العام"

مكافحة "المُتواطئين في الاحتيال" والعمليات عالية المخاطر بين الأفراد (P2P) تمثل أولوية قصوى في مجال الرقابة المالية

بوغدان ألكساندروفيتش شابليا -
مدير قسم الرقابة المالية ومراقبة العملات في بنك روسيا

يعرب بنك روسيا عن قلقه من مخاطر متزايدة مرتبطة باستغلال القطاع المصرفي الروسي لإجراء عمليات P2P بين الأفراد، مما يُتيح السبل لإتمام المعاملات المالية بين المواطنين والكيانات التي تُمارس أعمالًا غير مشروعة. وتُعزى هذه المخاطر بشكل رئيسي إلى تعامل البنوك مع أفراد وهميين، أو ما يعرف باسم - "المُتواطئين في الاحتيال"، حيث يتم استخدام حساباتهم لتنفيذ معاملات الدفع من شخص إلى شخص (P2P). يعمل بنك روسيا جنبًا إلى جنب مع البنوك الأخرى على وضع وتنفيذ استراتيجيات لمكافحة مثل هذه العمليات، تتضمن إجراءات لتعزيز سرعة اكتشاف حسابات الأفراد "المُتواطئين في الاحتيال" والتعامل مع المخاطر المُكتشفة.

تشير ممارسات الأنشطة الإشرافية ومراقبة عمليات المؤسسات المالية إلى لجوء بعض جهات P2P غير الملتزمة بمعايير السلوك المهني إلى استخدام خدمات المؤسسات المالية لإجراء معاملات تنطوي على مخاطر عالية. وتفتح هذه العمليات بوابة أمام الشركات التي تمارس أنشطة غير مشروعة، والتي لا يُسمح لها بالتعامل مع البنوك المرخصة، لقبول المدفوعات. ويشير مصطلح "الأعمال غير القانونية" إلى مجموعة واسعة من الأنشطة التجارية غير القانونية أو غير الأخلاقية التي تتم عبر الإنترنت، وتشمل هذه الأنشطة: ألعاب الكازينو ومكاتب المراهنات عبر الإنترنت والمخططات المالية الهرمية وبائعو السلع المحظورة ومبادلات العملات المشفرة وخدمات P2P لتبادل العملات المشفرة التي تستخدم "المُتواطئين في الاحتيال".

ونحن نُشدد على أن مشاركة المواطنين في مثل هذه العمليات تُعرضهم لمخاطر جسيمة، ليس فقط من ناحية فقدان مدخراتهم بسبب الاحتيال بأنواعه المختلفة، بل أيضًا من حيث مخاطر التورط في أنشطة غير قانونية قد تُفضي إلى ملاحقتهم جنائيًا. وقد تُشكل هذه المعاملات، نظرًا لحجمها الكبير في مجال الأعمال غير المشروعة، تهديدًا لمصالح الدائنين والمدخرين في حال قامت البنوك بمعالجتها وإجرائها.

وخلال الفترة من عامي 2020 إلى 2022، تم تنفيذ هذه العمليات باستخدام خدمات الدفع غير النقدي في القطاع المصرفي، مع التركيز بشكل أساسي على المؤسسات الائتمانية الصغيرة المتخصصة في تقديم الخدمات المصرفية غير المشروعة. وفي معظم الأحيان، كانت تتم عمليات الدفع من خلال حسابات مقدّمي خدمات الدفع الأجانب، والشركات

المسجلة، وأصحاب المشاريع الفردية المُنشأة خصيصًا لتنفيذ مثل هذه المعاملات، والمؤسسات المالية غير الملتزمة بمعايير السلوك المهني والتي تمارس أنشطة غير مشروعة تحت غطاء تقديم خدمات مثل القروض الصغيرة.

وفي إطار سعيه لتعزيز سلامة واستقرار القطاع المصرفي، عَمِلَ بنك روسيا خلال هذه الفترة على القضاء على العمليات عالية المخاطر وإخراج المؤسسات المالية التي تشارك بشكل منهجي في تنفيذها من القطاع المصرفي.

وشكل إطلاق البنك لمنصة "اعرف عميلك" عقبةً كبيرة أمام استخدام حسابات الشركات والأفراد لتنفيذ مثل هذه العمليات. وقد أدى خروج أنظمة الدفع الدولية من روسيا، والتي كانت تُنفذ في السابق معاملات عالية المخاطر عبر بنوك المعاملات الأجنبية، إلى حدوث تحولات جوهرية في سوق الدفع الموازي.

ونتيجةً لذلك، شهد عام 2023 ازديادًا ملحوظًا في حجم العمليات عالية المخاطر نحو نظام الدفع المباشر من شخص إلى شخص - P2P باستخدام بطاقات الدفع وحسابات "المُتواطئين في الاحتيال" الذين يفتحون حسابات أو بطاقات بنكية باسمهم ثم يسلمونها إلى المشاركين في الأنشطة التجارية غير الشرعية. وتشمل الأمثلة على معاملات P2P تحويل الأموال "من بطاقة إلى أخرى" و "من محفظة إلى أخرى" و "من حساب مشترك في شركة الاتصالات إلى محفظة أو بطاقة والعكس صحيح".

ونحن نُقدّر أن حجم عمليات P2P عالية المخاطر في القطاع المصرفي، وكذلك عدد "المُتواطئين في الاحتيال"

المشاركين في تنفيذها، مرتفع حاليًا، ويتطلب منّا اتخاذ إجراءات استجابة شاملة. ووضعت إدارة بنك روسيا هذا المجال من العمل ضمن قائمة المهام ذات الأولوية القصوى.

من ناحية أخرى، نرى أن استخدام مخططات P2P لإجراء المدفوعات بين الأفراد لأغراض الأعمال غير الشرعية أكثر تعقيدًا وتكلفة مقارنة بعمليات الدفع غير النقدي، وذلك لعدة أسباب، منها: الحاجة إلى الحفاظ على بنية تحتية معقدة لتكنولوجيا المعلومات لإدارة وتسجيل المعاملات تلقائيًا، والحاجة إلى إنشاء العديد من الحسابات المصرفية باسم أشخاص وهميين "المُتواطئين في الاحتيال". وفي المقابل، لعبت عدة عوامل دورًا في إعادة توجيه المشاركين في الأنشطة التجارية غير المشروعة إلى اعتماد المخطط المشار إليه، نذكر منها:

- سهولة ويسر فتح الحسابات المصرفية والمحافظ الإلكترونية، مما يسمح بإجراء عمليات P2P بأحجام كبيرة عمليًا ودون قيود تذكر وبأقل التكاليف. من ناحية، هذا يجعل المنتجات المصرفية جذابة لكل من الأفراد والشركات على حد سواء. ومن ناحية أخرى، يسعى المشاركون في الأنشطة المصرفية غير الشرعية إلى استغلال سهولة "الدخول" وتوافر المنتجات المصرفية لتحقيق أهدافهم. على سبيل المثال، هناك ما يُعرف باسم - "المُتواطئين في الاحتيال" الذين يقومون بفتح حسابات مصرفية نيابة عن أصحاب هذه الأعمال. إذ يستهدفون الأشخاص ذوي الوعي المحدود، ويستغلون عدم إدراكهم لجميع العواقب المترتبة على تسليم حساب (محفظة) تم فتحه حديثًا إلى شخص غريب لإدارته. حيث تُتيح بعض الحسابات ربط عشرات البطاقات الافتراضية، والتي تُستخدم لإنفاق مبالغ كبيرة في غضون أيام قليلة.
- إمكانية التعرف على هوية الأفراد عند فتح المحافظ الإلكترونية مع إشراك جهات خارجية (مثل وكلاء الدفع المصرفيين، ومشغلي الاتصالات)، والتي قد تتخذ أحيانًا نهجًا شكليًا في الامتثال لمتطلبات التعرف على الهوية، نظرًا لأن حجم دخلهم يعتمد على عدد المحافظ الإلكترونية التي يفتحونها للأفراد. إذ تُتيح التشريعات النافذة إمكانية التحقق من صحة المعلومات المقدمة لاستصدار المحافظ الإلكترونية عبر أنظمة المعلومات الحكومية، وذلك في إطار عملية التحقق من الهوية

(تحديد الهوية المبسط) دون الحاجة إلى الحضور الشخصي أو تقديم النسخ الأصلية من المستندات. وقد كشفنا عن حالات قامت فيها مؤسسات ائتمانية بإنشاء محافظ إلكترونية مرتبطة ببيانات شخصية لأفراد دون علمهم أو موافقتهم، واستخدام هذه المحافظ لإجراء عمليات مالية، مما أدى إلى مخاطر جسيمة على أصحاب هذه البيانات.

- تم اكتشاف ثغرات تقنية في بعض خدمات P2P للمؤسسات الائتمانية المتاحة للجمهور على الإنترنت. إذ يلجأ منظمو الأنشطة غير المشروعة على مواقعهم الإلكترونية على شبكة الإنترنت إلى استخدام نماذج دفع P2P وهمية، حيث "تجمع البرامج الآلية" معلومات بطاقات العملاء المصرفية وتعيد توجيهها تلقائيًا إلى صفحة الويب الفعلية للمؤسسة الائتمانية لإجراء عملية P2P.

وبهدف تجنب المخاطر المشار إليها، أصدر بنك روسيا توصيات منهجية بتاريخ 6 سبتمبر 2021 برقم 16-MR[1] وتاريخ 12 أكتوبر 2023 برقم 13-MR[2].

تُشدد التوصيات المنهجية رقم 16-MR على ضرورة قيام المؤسسات الائتمانية بتحديد عمليات تحويل الأموال (الأموال الإلكترونية) بين الأفراد باستخدام وسائل الدفع الإلكترونية (على وجه الخصوص بطاقات الدفع والمحافظ الإلكترونية) التي تُظهر خصائص غير معتادة للمعاملات العادية، كما تُلزم هذه التوصيات بتطبيق تدابير مكافحة غسل الأموال، وضمان حماية المعلومات الكافية لخدمات P2P الخاصة بالمؤسسات من الاستخدام الآلي.

وللحد من مخاطر استخدام خدمات الدفع غير النقدي للتحايل على التعليمات المنهجية رقم 16-MR، أصدر بنك روسيا التوصيات المنهجية رقم 13-MR، وتتضمن هذه التوصيات توجيهات للمؤسسات الائتمانية التي تعمل كجهات دفع غير نقدي، بما في ذلك: مراقبة تحويل الأموال إلى حسابات المنشأة التجارية أو الخدمية التي تمت فيها عملية الشراء، إذ يهدف ذلك إلى مكافحة ما يطلق عليه اسم "مخطط المطعم"، والتدقيق المكثف على عمليات التحويل المريبة لصالح المنشآت التجارية أو الخدمية التي لا تمارس نشاطًا تجاريًا حقيقيًا.

ونعمل حاليًا بشكل وثيق مع البنوك على تطوير وتطبيق حلول مبتكرة جديدة لمكافحة معاملات P2P عالية المخاطر. وتتضمن هذه الحلول تحسين سرعة اكتشاف الحسابات والمعاملات الخاصة بالأفراد الذين يعملون كوكلاء أو ما يسمى "المُتواطئين في الاحتيال"، بما في ذلك الكشف الفوري عبر الإنترنت، وإجراءات مراقبة إضافية عند إصدار بطاقات الائتمان واستخدام بعض المنتجات المصرفية.

تُركز هذه الحلول إلى تحقيق غرضين رئيسيين: الأول هو عرقلة الأنشطة غير المشروعة من خلال جعل الاعتماد على القطاع المصرفي وتحويلات الأموال من شخص لآخر (P2P) أكثر صعوبة وباهظ التكلفة.

والثاني هو غرس مبدأ عدم التسامح المطلق تجاه أنشطة "المُتواطئين في الاحتيال" لدى المؤسسات المالية والسكان. ولتحقيق ذلك، ينبغي تعزيز إجراءات الامتثال في القطاع المصرفي لمنع فتح حسابات باسم أشخاص وهميين، بالإضافة إلى تكثيف الجهود التوعوية التي يبذلها كل من بنك روسيا والمؤسسات الائتمانية بالتعاون مع أجهزة إنفاذ القانون، بهدف توعية الجمهور بعواقب مثل هذه الأنشطة وتعزيز الرفض المجتمعي لها.

ونعمل حاليًا بشكل وثيق مع البنوك على تطوير وتطبيق حلول مبتكرة جديدة لمكافحة معاملات P2P عالية المخاطر. وتتضمن هذه الحلول تحسين سرعة اكتشاف الحسابات والمعاملات الخاصة بالأفراد الذين يعملون كوكلاء أو ما يسمى "المُتواطئين في الاحتيال"، بما في ذلك الكشف الفوري عبر الإنترنت، وإجراءات مراقبة إضافية عند إصدار بطاقات الائتمان واستخدام بعض المنتجات المصرفية.

[1] تعزيز يقظة المؤسسات الائتمانية تجاه معاملات محددة للعملاء- الأفراد.
[2] بخصوص أنشطة المؤسسات الائتمانية ووكلاء الدفع في معالجة الحسابات مع مؤسسات السلع (الخدمات) للعمليات التي تتم باستخدام وسائل الدفع الإلكترونية.

الأمن المعلوماتي في السوق المالية: مكافحة الاحتيال الإلكتروني في عمليات تحويل الأموال

شكل الانتشار الواسع لتقنيات الدفع الرقمية نقطة تحول رئيسية في موقف المجتمع تجاه قضية ضمان الأمن المعلوماتي. وفي ظل النمو المُطّرد للخدمات المصرفية عن بُعد، يُشكل غياب الإجراءات الوقائية الكافية لحماية عملاء البنوك من جرائم الاحتيال الإلكتروني خطرًا يهدد بتبعات سلبية ذات أبعاد اجتماعية واسعة[1]. وعلى هذا النحو، فإنّ التصدي بفعالية لمخاطر سرقة الأموال من حسابات المواطنين يُمثّل اليوم أحد أهمّ العوامل في حماية حقوق المستهلكين في الخدمات المالية ورفع مستوى الثقة في التكنولوجيا الرقمية.

فاديم ألكسندروفيتش أوفاروف،
مدير إدارة أمن المعلومات في بنك روسيا

وتتصدّر مكافحة الاحتيال الإلكتروني في القطاع الائتماني والمالي قائمة أولويات عمل بنك روسيا. ونتيجة للجهود المنهجية التي تبذلها الجهة التنظيمية بالتعاون مع ممثلي القطاع، تمكنت البنوك في عام 2023 من صدّ ما يقارب 34.8 مليون محاولة لتنفيذ عمليات احتيالية. وبفضل هذه الإجراءات، تمّ إحباط سرقة 5.8 تريليون روبل من أموال عملاء المؤسسات الائتمانية.

ومع ذلك، لاحظ بنك روسيا على مدار السنوات القليلة الماضية زيادة سنوية في حجم المعاملات الناجحة التي تم تنفيذها دون موافقة عملاء البنوك. ففي عام 2023، تمكن المجرمون من سرقة 15.8 مليار روبل. وبالمقارنة مع العام السابق، ارتفع حجم الأموال المسروقة بنسبة 11.5%. وسجلت العمليات الاحتيالية ارتفاعًا بنسبة 33% لتصل إلى أكثر من 1.1 مليون حالة[2].

ومن بين العوامل التي تحول دون حدوث تغيير جذري في مكافحة الاحتيال والهندسة الاجتماعية هو التحسين المستمر للمحتالين في خططهم وسيناريوهات التأثير على المواطنين. وتشهد الفترة الحالية ازديادًا في اعتماد المحتالين على شن هجمات مخصصة، والتي يسبق تنفيذها دراسة شاملة للمعلومات الشخصية للضحايا المستهدفين، بما في ذلك تلك التي ينشروها المواطنون طوعًا على موارد الإنترنت المختلفة.

وفي إطار جهوده لمكافحة جرائم الاحتيال عبر الهاتف والإنترنت، يُنفذ بنك روسيا حزمة من الإجراءات المتكاملة. تشمل منظومة الإجراءات المتخذة تحسين التشريعات المنظمة لنشاط المؤسسات المالية، والعمل توعية

[1] كشفت إحصائيات رسمية صادرة عن وزارة الداخلية الروسية أن ثلث الجرائم في البلاد خلال عام 2023 ارتُكبت باستخدام تقنيات المعلومات والاتصالات. وارتفع عدد الجرائم المُسجلة في هذا المجال بنسبة 29.7% عما كان عليه في عام 2022. (https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/).

[2] يمكن الاطلاع على المراجعات السنوية للمعاملات التي تتم دون موافقة عملاء المؤسسات المالية على الموقع الإلكتروني الرسمي لبنك روسيا: (http://www.cbr.ru/analytics/ib/operations_survey/2023/).

المواطنين وتثقيفهم، إلى جانب التعاون مع جهات إنفاذ القانون والهيئات الرقابية وسجلات أسماء النطاقات ومشغلي شركات الاتصالات.

وفي شهر يوليو من العام 2024، سيدخل حيز التنفيذ قانون تمّت صياغته بمشاركة البنك المركزي الروسي، يهدف إلى تحسين آليات مكافحة سرقة الأموال من عملاء المصارف[3]. وهو ينص على:

- تطبيق "مهلة زمنية" إلزامية مدتها يومان - إجراء إلزامي على البنك لتعليق التحويلات المالية إلى الحسابات المدرجة في قاعدة بيانات بنك روسيا "بشأن حالات ومحاولات تحويل الأموال دون موافقة العميل" (المشار إليها فيما يلي باسم - "قاعدة بيانات بنك روسيا"). وسيكون بمقدور الشخص خلال مدة لا تتجاوز يومين مراجعة وتقييم الإجراءات التي يُقدم على اتخاذها ورفض تحويل الأموال إلى حساب مشبوه.

- تقع على عاتق البنك مسؤولية تعطيل الوصول إلى وسائل الدفع الإلكترونية للمُتواطئين في الاحتيال، في حال تم إرسال معلومات حول ممارستهم لأعمال غير قانونية إلى قاعدة بيانات بنك روسيا من قبل وزارة الشؤون الداخلية الروسية. أما إذا تم إرسال المعلومات إلى قاعدة بيانات بنك روسيا من قبل مؤسسة مالية أخرى، فإن قطع الوصول إلى أدوات الدفع الإلكترونية للمستخدم يصبح خيارًا متاحًا للبنك.

- يلتزم البنك بإرجاع الأموال للعميل في غضون 30 يومًا في حال قام البنك بتحويل الأموال إلى حساب احتيالي مدرج في قاعدة بيانات بنك روسيا دون اتخاذ الإجراءات الوقائية الإلزامية لحماية العميل.

وقد بيّنت نتائج استطلاع أجراه بنك روسيا عام 2023 حول درجة رضا السكان عن أمن الخدمات المالية أن 62% من ضحايا الاحتيال قد اتخذوا خطوات للإبلاغ عن الحادث، إما إلى البنك أو إلى الشرطة أو كليهما. وتكتسب عملية تبادل المعلومات حول العمليات الاحتيالية بين البنوك والأجهزة الأمنية أهمية قصوى في سبيل التصدي لهذه الظاهرة.

وفي شهر أكتوبر من عام 2023، دخل قانون التفاعل المعلوماتي بين بنك روسيا ووزارة الشؤون الداخلية في روسيا حيز التنفيذ[4]، مما خلق ظروفًا للتبادل الآلي لبيانات المعاملات بين المؤسستين دون موافقة العملاء. وبذلك أصبح بإمكان أجهزة إنفاذ القانون الآن الوصول إلى المعلومات الضرورية للتحقيق في جرائم الاحتيال والقضايا الجنائية من قاعدة بيانات بنك روسيا بكفاءة وسرعة فائقتين. في المقابل، يُمكن للمصارف الاستفادة من المعلومات التي يتلقاها بنك روسيا من وزارة الشؤون الداخلية الروسية، وذلك في إطار أنظمة مكافحة الاحتيال الخاصة بها، بهدف منع حدوث عمليات احتيال جديدة.

وفي إطار مكافحة الجرائم الإلكترونية، ينسّق بنك روسيا مع النيابة العامة لروسيا الاتحادية[5] والجهات المسؤولة عن تسجيل أسماء النطاقات. وفي إطار

عمليات الاحتيال المصرفية: إحصائيات

ممارسات احتيالية بقي **5,8** تريليون روبل

التي تمّ إحباطها من قبل البنوك **34,8** مليون

المختلس

عدد العمليات، وحدة **+33,0%**

2023	1 165 992
2022	876 589

حجم المبالغ المالية **+11,5%**

2023	15,8
2022	14,2

كانت بطاقات الائتمان الهدف الأكثر شيوعًا للسرقات المالية

سمات الضحية

تعيش في المدينة

المبلغ المختلس أقل من 20 ألف روبل

امرأة عاملة ذات مستوى دخل متوسط ومستوى تعليمي متوسط

العمر من 25 إلى 44 سنة

يُقدم حوالي ثلث ضحايا عمليات الاحتيال المالي بلاغات عن اختلاس أموالهم إلى بنوكهم

[3] القانون الاتحادي رقم -369ف ز الصادر بتاريخ 24 يوليو 2023 "تعديلات القانون الاتحادي "نظام الدفع الوطني".
[4] عملاً بأحكام القانون الاتحادي المُعدل رقم -408ف ز الصادر بتاريخ 20 أكتوبر 2022 "تعديل المادة 26 من القانون الاتحادي "البنوك والأنشطة المصرفية" والمادة 27 من القانون الاتحادي "نظام المدفوعات الوطني".
[5] عملاً بالصلاحيات المنصوص عليها في المادة 6.2 من القانون الاتحادي الصادر في 10 يوليو 2002 رقم -86ف ز "البنك المركزي لروسيا (بنك روسيا)".

جهودها لمكافحة الأنشطة غير القانونية، عمدت الجهة التنظيمية في عام 2023 إلى إرسال أكثر من 38.3 ألف مورد إلكتروني إلى عناوينها بهدف حجبها. وتُشكّل مواقع التصيد الاحتيالي (55%) النسبة الأكبر من هذه الموارد، حيث تهدف بشكل أساسي إلى سرقة بيانات عملاء المؤسسات المالية. وعطفًا على ما سبق، تمّ حظر الوصول إلى 4500 صفحة (مجموعة) على مواقع التواصل الاجتماعي و35 تطبيقًا، والتي كان يستخدمها المجرمون بشكل رئيسي لممارسة الأنشطة غير القانونية وعمليات التصيد الاحتيالي من خلال انتحال صفة مؤسسات الائتمان المرخصة.

وبناءً على رصده استخدامها من قبل المحتالين لسرقة الأموال من المواطنين، قام البنك المركزي الروسي بإرسال 575.7 ألف رقم هاتف إلى شركات الاتصالات ليتم حظرها.

وفي ضوء نتائج الرصد الذي أجراه بنك روسيا هذا العام، تركز الهيئة التنظيمية على اتجاهين لهما تداعيات اجتماعية سلبية على المواطنين: حجم هائل لعمليات الاحتيال في الائتمان وجذب المواطنين، خاصة الشباب، لممارسة عمليات مشاركة المواطنين في سحب الأموال التي سرقها المحتالون.

يُشكل الاحتيال الائتماني تهديدًا خطيرًا يتجاوز مجرد الزيادة في متوسط مبلغ عمليات الاحتيال. فالضحايا الذين يُغريهم المحتالون بالحصول على قروض ثم يسلمونهم الأموال المقترضة بأنفسهم يجدون أنفسهم محاصرين في "فخ الديون" لسنوات طويلة. وانطلاقًا من التزامه بحماية المواطنين وتعزيز مسؤولية المؤسسات المالية، يضع بنك روسيا مبادرات ملموسة قيد التطوير. وتشمل الإجراءات الوقائية "مهلة زمنية" إلزامية بين الموافقة على القرض وصرف الأموال للمقترض: وينبغي تطبيق هذا الإجراء بشكل أساسي في الحالات التي يتقدم فيها المقترض بطلب للحصول على قرض بمبلغ كبير. إن دمج إجراءات مكافحة الاحتيال في عملية منح القروض أمر بالغ الأهمية، حيث يُمكّن ذلك البنك من تقييم ما إذا كان المقترض يتصرف بإرادته الحرة أو تحت تأثير جهات خارجية.

كما يبذل بنك روسيا جهودًا حثيثة لمكافحة ظاهرة "مشاركة المواطنين في سحب الأموال التي سرقها المحتالون"، وهي عملية سحب الأموال وتحويلها إلى نقود تم الحصول عليها بطرق غير مشروعة، بما في ذلك استخدام وسائل الدفع الإلكترونية من قبل الأشخاص المتورطين في هذه العملية. هناك العديد من الخيارات لمشاركة المواطنين في سحب الأموال التي سرقها المحتالون. وتتنوع دوافع مشاركة الأشخاص في هذه الأنشطة، فمنهم من يشاركون بوعيٍ تامٍ، بينما قد يجهل البعض الآخر العواقب التي قد تترتب على ذلك. وفي حالات أخرى، لا يدركون أنهم متورطون في ممارسة أنشطة غير قانونية: من خلال مشاركة بياناتهم مع شخص آخر أو نشرها علنًا، على سبيل المثال على منصات التواصل الاجتماعي، وبهذا

يمكن أن يصبحوا متورطين دون قصد في ارتكاب جرائم معينة. والفئات العمرية الأكثر عرضة للخطر هي المراهقون والشباب (الأعمار الأساسية للمُتواطئين في الاحتيال هي 19-17 سنة).

وحرصًا على مكافحة هذه الظاهرة، أوصى بنك روسيا في أبريل 2022 المؤسسات المالية بتعطيل أدوات الدفع الإلكترونية للأفراد الذين تُستخدم بطاقاتهم المصرفية في عمليات سحب الأموال المسروقة وصرفها[6]. لذلك، تتمتع البنوك حاليًا بالصلاحية لتعليق الوصول عبر الإنترنت لإدارة الحسابات مؤقتًا في حال قيام العميل بعمليات مشبوهة.

وبعد إقرار قانون تحسين آليات مكافحة سرقة الأموال من عملاء البنوك في يوليو 2024، ستصبح إجراءات مكافحة غسل الأموال أكثر صرامة، خاصة فيما يتعلق بالعمليات المصرفية عن بعد التي يقوم بها "المتواطؤن في الاحتيال". وستكون البنوك ملزمة بتعليق استخدام العميل للأدوات الإلكترونية للدفع في حال تلقي معلومات حول ممارسته لأعمال غير قانونية إلى قاعدة بيانات بنك روسيا من قبل وزارة الشؤون الداخلية الروسية. بالنظر إلى أن هذه المعلومات يتم إرسالها إلى جميع المؤسسات الائتمانية، سيتم إيقاف العمليات عن بعد ذات الصلة بحسابات المتواطئين في الاحتيال في جميع البنوك.

ومن خلال هذه الخطوة، سيتم خلق بيئة تُثبط المجرمين عن ممارسة أنشطتهم غير القانونية بسبب عدم جدواها الاقتصادية.

وفي إطار تعزيز التواصل المعلوماتي بين المؤسسات الائتمانية وعملائها، قام بنك روسيا بإعداد وتنسيق "توصيات منهجية" بالتعاون مع وزارة الداخلية الروسية[7]. وتحدد هذه المعلومات تدابير عملية لزيادة وعي العملاء من أجل التصدي لمخاطر توريطهم في عمليات سحب الأموال التي سرقها المحتالون. وتتمثل الأهداف الرئيسية للعمل الإعلامي والتوعوي في الإبلاغ عن مسؤولية وعواقب المشاركة في عمليات سحب الأموال التي سرقها المحتالون، وتعزيز وعي المواطنين بكون هذه الأنشطة غير قانونية وتُلحق ضررًا بسمعة المشاركين في تنفيذها.

تعتمد استراتيجية مكافحة الاحتيال الإلكتروني في القطاع المصرفي، والتي تشمل الاحتيال الائتماني وسحب الأموال التي يسرقها المحتالون، بشكل كبير على دقة البيانات حول المعاملات المشبوهة التي يتم تبادلها بين البنوك وبنك روسيا، إذ يقوم بنك روسيا بدوره بتوزيع هذه البيانات على جميع الجهات المشاركة في تبادل المعلومات. وترتبط سرعة وكفاءة مكافحة المحتالين، فضلًا عن جودة أنظمة مكافحة الاحتيال في البنوك، ارتباطًا وثيقًا بمدى اكتمال وموثوقية المعلومات المقدمة وسرعة توفرها. وعليه، فإن ضمان تقديم تقارير بيانات كافية لبنك روسيا يعتبر اليوم من أهم أولويات عمل الجهة المُنظّمة، بما في ذلك مهامها الرقابية. وهناك أمر بالغ الأهمية بأن تضمن آليات مكافحة اختلاس الأموال، المنصوص عليها في القوانين المُعتمدة، حماية حقوق المواطنين ومصالحهم بصفتهم مستخدمين للخدمات المالية.

[6] خطاب إعلامي صادر عن بنك روسيا بتاريخ 15 أبريل 2022 برقم 3143/5-56-01 يطلب من جميع المؤسسات الائتمانية اتخاذ خطوات لمكافحة عمليات تحويل الأموال دون موافقة العملاء.

[7] التوجيهات المنهجية رقم MP-3 الصادرة في 28 فبراير 2024 بشأن تعزيز الجهود الإعلامية للمنظمات الائتمانية مع العملاء لمكافحة التحويلات المالية دون موافقة العميل الصريحة، وإبرام عقود الحصول على الأموال الائتمانية (القروض) تحت تأثير الخداع أو إساءة استخدام الثقة، وإجراء المعاملات باستخدام هذه الأموال، وإشراك المواطنين في أنشطة سحب وصرف الأموال التي تم الحصول عليها بوسائل إجرامية.

تقييد الوصول إلى المعلومات الممنوع نشرها في روسيا الاتحادية قبل الحصول على أمر قضائي

ظلت مشكلة الجرائم المرتكبة باستخدام تقنيات المعلومات والاتصالات، خلال السنوات الأخيرة، واحدة من أكثر القضايا إلحاحًا وتشكل تهديدًا خطيرًا للأمن القومي لروسيا الاتحادية.

نيكولايفيتش راستاشينوف
مدير وحدة منع تداول المحتوى المُضر والمُحظور عبر الإنترنت
إدارة تنظيم مكافحة الاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات التابعة لوزارة الشؤون الداخلية في روسيا
عقيد شرطة أنطون

ويرجع ذلك إلى التبني المتسارع لابتكارات تكنولوجيا المعلومات في الحياة اليومية للمجتمع، مما يسمح للمجرمين بالبقاء بعيدًا عن أعين وكالات إنفاذ القانون.

وتشير الإحصاءات الرسمية إلى أن أجهزة إنفاذ القانون سجلت 677 ألف جريمة ارتكبت باستخدام تقنيات المعلومات والاتصالات في الفترة من يناير إلى ديسمبر 2023، بزيادة قدرها 29.7% عن العام السابق.

ويُؤكد الازدياد المتواصل في جرائم هذه الفئة على الحاجة الملحة للبحث عن أفضل الأشكال والطرق والوسائل المثلى والفعالة لبيان ماهيتها والوقاية منها ومكافحتها وكشفها والتحقيق فيها.

وتحتل الإجراءات الوقائية مكانةً محوريةً في منظومة مكافحة الجرائم الإلكترونية، وذلك من خلال مكافحة موارد المعلومات غير القانونية التي يُوظّفها المجرمون كمنصات لنشر الدعاية والإعلانات، وكأدواتٍ لغسل الأموال وتمويل الأنشطة الإجرامية.

وعملًا بالأحكام القانونية النافذة، تتولى وزارة الشؤون الداخلية الروسية، بالتعاون مع هيئة الرقابة على الاتصالات (روسكومنادزور)، مهمة تقييد الوصول إلى موارد الإنترنت التي تتضمن معلومات محظورة، وتشمل تلك المتعلقة بالمخدرات والأسلحة، فضلًا عن نشر المواد المتطرفة.

وفي عام 2023، وبفضل الجهود المشتركة للوكالات المذكورة، تم تقييد الوصول إلى أكثر من 330 ألف موقع وصفحة تحتوي على معلومات من هذا النوع.

وعادةً ما يتم نشر المعلومات المحظورة من خلال موارد مخصصة تم إنشاؤها على الإنترنت، مثل المواقع الإلكترونية وصفحات المنتديات المتخصصة، بالإضافة إلى المجموعات ذات الاهتمامات المحددة على مواقع التواصل الاجتماعي. وعلاوة على ذلك، قد يكون الأشخاص الذين ساهموا في إنشاء المنصات المذكورة أعلاه موجودين خارج البلاد، مستخدمين أدوات وموارد لإدارة عملياتها.

يحدد القانون الاتحادي رقم -149ف ز[1]، الصادر بتاريخ 27 يوليو 2006، القواعد التي تحكم العلاقات المرتبطة بممارسة الحق في البحث عن المعلومات والحصول عليها ونقلها وإنتاجها ونشرها، وتطبيق تقنيات المعلومات، وضمان حماية المعلومات.

وتنصّ المادة 15.1 من القانون الاتحادي رقم -149ف ز، والذي دخل حيز التنفيذ في 1 نوفمبر 2012، على تحديد آلية حظر المواقع الإلكترونية، والتي تُعرّف بأنها مجموعة من التدابير التنظيمية والفنية المُتّخذة للحد من إمكانية الوصول إلى المعلومات المحظورة على شبكة الإنترنت.

ووفقًا للجزء 2 من المادة 15.1 من القانون الاتحادي رقم -149ف ز على أن نظام المعلومات الآلي الموحد "السجل الموحد لأسماء النطاقات وعناوين المواقع الإلكترونية على الإنترنت" وعناوين الشبكة التي تحدد المواقع على الإنترنت التي تحتوي على معلومات يحظر نشرها في روسيا الاتحادية" [2]يتضمن أسماء النطاقات أو عناوين المواقع الإلكترونية على الإنترنت أو كليهما، بالإضافة إلى عناوين الشبكة التي تسمح بتحديد المواقع على الإنترنت التي تحتوي على معلومات يحظر نشرها في روسيا الاتحادية.

ووفقًا للجزء 5 من المادة 15.1 من القانون الاتحادي رقم -149ف ز، فإنّ الأسس لإدراج موارد الإنترنت في نظام المعلومات الآلي الموحد "السجل الموحد" لموارد الإنترنت هذه هي قرارات السلطات التنفيذية الاتحادية المخولة من قبل حكومة روسيا الاتحادية، المعتمدة وفقا لاختصاصها بموجب للإجراءات التي تحددها حكومة روسيا الاتحادية[3]، كما يتم إدراج موارد الإنترنت بناءً على قرارات قضائية تُحظر نشر معلومات عبر شبكة الإنترنت في روسيا الاتحادية.

كما وضعت قائمة شاملة للمعلومات المحظورة بموجب البنود الفرعية (أ) إلى (م) من البند 1

من الجزء 5 من المادة 15.1 من القانون الاتحادي رقم -149ف ز، وتقوم السلطات التنفيذية الفيدرالية المخولة من قبل حكومة روسيا الاتحادية، في حدود اختصاصاتها، باتخاذ القرارات المناسبة بشأن هذه المعلومات.

وعلى وجه الخصوص، تحدد البنود الفرعية "ب" و"ك" من البند 1 من الجزء 5 من المادة 15.1 من القانون الاتحادي رقم -149ف ز الأساس لإدراجها في نظام المعلومات الآلي الموحد "السجل الموحد" والذي يوزع المعلومات:

- بخصوص الأساليب والطرق المتبعة في تطوير وتصنيع واستخدام المواد المخدرة والمؤثرات العقلية ومشتقاتها، وأماكن الحصول على هذه العقاقير والمواد ومشتقاتها، وحول طرق وأماكن زراعة النباتات التي تحتوي على مواد مخدرة.

- بخصوص أساليب وطرق التصنيع الذاتي للمتفجرات والأجهزة المتفجرة، والتصنيع أو التعديل غير القانوني للأسلحة، والأجزاء الرئيسية للأسلحة النارية، وكذلك التصنيع غير القانوني للذخائر، باستثناء المعلومات المتعلقة بطرق وأساليب ملء خراطيش الأسلحة النارية المدنية ذات الماسورة الطويلة بشكل مستقل.

ووفقًا لاستراتيجية الأمن القومي لروسيا الاتحادية، التي تم إقرارها بموجب مرسوم رئيس روسيا الاتحادية رقم 683 بتاريخ 31 ديسمبر 2015، تُعتبر الأنشطة المتعلقة باستخدام تقنيات المعلومات والاتصالات لنشر ودعاية أيديولوجية الفاشية والتطرف والإرهاب والانفصالية من بين التهديدات الرئيسية للأمن القومي والمجتمعي.

وفي هذا الصدد، فإن أحد الاتجاهات الرئيسية لضمان أمن المعلومات هو مكافحة استخدام تكنولوجيا المعلومات لتعزيز الأيديولوجية المتطرفة ونشر كراهية الأجانب وأفكار التعصب القومي.

بموجب القانون الاتحادي رقم -398ف ز الصادر بتاريخ 28 ديسمبر[4] 2013 والقانون الاتحادي رقم -327ف ز[5] الصادر بتاريخ 25 نوفمبر 2017، تم تعديل القانون الاتحادي رقم -149 ف ز بإضافة المادة 15.3، والتي تحدد قواعد تقييد الوصول إلى المعلومات التي يتم اكتشافها على شبكات المعلومات والاتصالات، بما في ذلك شبكة "الإنترنت"، والتي تحتوي على دعوات للقيام باضطرابات جماعية، والانخراط في ممارسة الأنشطة المتطرفة، والمشاركة في فعاليات جماهيرية (عامة) تُنظم مع انتهاك النظام المعمول به، بالإضافة إلى المواد الإعلامية لمؤسسات غير حكومية أجنبية أو دولية تم الاعتراف بأن نشاطها غير مرغوب فيه على أراضي روسيا الاتحادية، علاوةً على

[1] بناءً على أحكام القانون الاتحادي رقم -149ف ز "المعلومات وتكنولوجيا المعلومات وحماية المعلومات" الصادر بتاريخ 27 يوليو 2006. المشار لإليه فيما يلي باسم - القانون الاتحادي رقم -149ف ز.

[2] المشار إليه لاحقًا باسم - نظام المعلومات الآلي الموحد "السجل الموحد".

[3] مرسوم حكومي صادر عن حكومة روسيا الاتحادية رقم 1101 صادر بتاريخ 26 أكتوبر 2012 "نظام المعلومات الآلي الموحد "السجل الموحد لأسماء النطاقات وعناوين المواقع الإلكترونية في شبكة المعلومات والاتصالات العالمية "الإنترنت" والعناوين الشبكية التي تسمح بتحديد المواقع الإلكترونية على شبكة المعلومات والاتصالات العالمية "الإنترنت" التي تحتوي على معلومات يحظر نشرها في روسيا الاتحادية. يُشار إليه فيما يلي باسم - المرسوم رقم 1101.

[4] "التعديلات على القانون الاتحادي "المعلومات وتكنولوجيا المعلومات وحماية المعلومات".

[5] "المعلومات وتكنولوجيا المعلومات وحماية المعلومات" والمادة 6 من قانون روسيا الاتحادية "وسائل الإعلام".

البيانات التي تسمح بإمكانية الوصول إلى المعلومات أو المواد المذكورة.

بناءً على أحكام الجزء 1 من المادة 15.3 من القانون الاتحادي رقم -149 ف ز، يحق للنائب العام لروسيا الاتحادية أو نوابه، عند تلقي إخطارات من الهيئات الاتحادية للسلطة التنفيذية، أو سلطات الدولة في الكيانات المكونة لروسيا الاتحادية، أو الهيئات المحلية للحكم الذاتي، أو المنظمات، أو المواطنين، بشأن نشر معلومات ذات طبيعة محددة في شبكات المعلومات والاتصالات، بما في ذلك شبكة "الإنترنت"، إرسال طلب إلى الهيئة الاتحادية للرقابة في مجال الاتصالات وتقنيات المعلومات والاتصالات الجماهيرية (روسكومنادزور) لاتخاذ تدابير لتقييد الوصول إلى الموارد المعلوماتية التي تنشر هذه المعلومات.

وبناءً على تعليمات من النائب العام لروسيا الاتحادية أو نوابه، ترسل الهيئة الاتحادية للرقابة في مجال الاتصالات وتقنيات المعلومات والاتصالات الجماهيرية (روسكومنادزور)، عبر نظام التفاعل، إخطارًا عاجلاً إلى مشغلي الاتصالات يطالبهم باتخاذ خطوات لتقييد الوصول إلى مورد إعلامي أو إلى المعلومات المنشورة عليه، وبعد تلقي هذا الإخطار، يتعين على مشغل الاتصالات الذي يقدم خدمات الوصول إلى شبكة المعلومات والاتصالات "الإنترنت" حظر الوصول إلى هذا المورد الإعلامي دون تأخير. وتقوم الهيئة الاتحادية للرقابة في مجال

الاتصالات وتقنيات المعلومات والاتصالات الجماهيرية (روسكومنادزور) بتسجيل بيانات المورد الإلكتروني في سجل خاص.

وتسمح الآلية المنصوص عليها برد فعل سريع على حالات انتشار المعلومات المماثلة على شبكة الإنترنت، وذلك من خلال اشتراط تضمين اسم نطاق الموقع الإلكتروني في طلب الهيئة الاتحادية للرقابة في مجال الاتصالات وتقنيات المعلومات والاتصالات الجماهيرية (روسكومنادزور) وعنوانه على شبكة "الإنترنت" وروابط صفحات الموقع الإلكتروني التي تُتيح التعرف على هذه المعلومات بشكل دقيق في طلباتها.

"الاتجاهات الحالية في سوق مقدمي الخدمات المالية غير الشرعيين"

تأتي مهمة ضمان سلامة مداخيل السكان وحماية المستهلكين من الانخراط في أنشطة غير قانونية في السوق المالية على رأس أولويات الجهات التنظيمية المالية.

رومان فياتشيسلافوفيتش موخلينوف،
نائب مدير إدارة الإقراض غير المصرفي في البنك المركزي لروسيا الاتحادية

وفي إطار سعيه لحماية مدخرات المواطنين وتعزيز الثقة في القطاع المالي، يقوم بنك روسيا باتخاذ خطوات لتوحيد جهود جميع الأطراف المعنية، لمكافحة عمليات الاحتيال والتصدي للممارسات غير الأخلاقية وغير القانونية التي قد تُعرّض مدخرات المواطنين للخطر.

وفي عام 2023، كشف بنك روسيا عن 5735 كيانًا (شركات، مشاريع، رواد أعمال فرديين، وغيرهم) تظهر علامات على ممارسات غير مشروعة، بما في ذلك علامات على وجود مخططات هرمية (مخططات بونزي) وهذا يمثل زيادة بنسبة 15.5% عن العام السابق، بينما أصبح "عمر" هذه المشاريع أقصر وانخفض "متوسط الاستثمار" فيها. تُرسل جميع البيانات المُكتشفة حول الأنشطة غير القانونية إلى جهات الاختصاص، مثل وكالات إنفاذ القانون، وهيئة الرقابة المالية الروسية (روسفينمونيتورينغ)، وهيئة مكافحة الاحتكار الاتحادية الروسية (فاس)، والوكالة الاتحادية للرقابة في مجال الاتصالات وتكنولوجيا المعلومات والاتصالات الجماهيرية (روسكومنادزور)، وذلك بهدف وقف الأنشطة. مع ذلك، يلجأ المحتالون كل عام إلى استخدام أساليب وأدوات جديدة، مما يتطلب اليقظة الشديدة للكشف عن مثل هذه الممارسات، سواء من قبل الجهات التنظيمية أو جهات إنفاذ القانون أو المنظمات المجتمعية أو المؤسسات المالية.

شهدت السنوات الماضية ظاهرة بارزة تمثلت في الانتقال المكثف إلى التفاعل عبر الإنترنت، الأمر الذي استغله المحتالون والموردون غير الشرعيين للخدمات المالية لتعزيز مخططاتهم الاحتيالية من خلال الاستفادة من تقنيات التشفير. وقد حذر بنك روسيا مرارًا وتكرارًا من مخاطر انتشار العملات المشفرة في روسيا الاتحادية، مشيرًا إلى تأثيرها السلبي الذي ينعكس على رفاهية المواطنين واستقرار النظام المالي، فضلًا عن ازدياد احتمالية تورط عملاء المؤسسات المالية في الأنشطة غير القانونية، مثل غسل الأموال وتمويل الإرهاب[1]. وسعيًا لتجنب تفاقم هذا الوضع، أصدر البنك توصيات تهدف إلى تقليل مخاطر كهذه على عملاء البنوك والمؤسسات المالية الأخرى[2].

ولا يقل خطورة عن ذلك تنامي عدد المشاركين غير القانونيين في السوق المالية الذين يجذبون الاستثمارات في العملات المشفرة. وقد شهد العام 2022

[1] يُمكن الاطلاع على المعلومات المُفصلة حول المخاطر والتحديات المُرتبطة بانتشار الأصول المشفرة ("العملات الافتراضية"، العملات المشفرة) على الموقع الرسمي لبنك روسيا على شبكة الإنترنت، وتشمل هذه المعلومات بيانات مُستمدة من بيانات صحفية صادرة عن البنك في 27 يناير 2014 بعنوان "استخدام العملات الافتراضية، وعلى وجه الخصوص، البيتكوين، في المعاملات"؛ وبيان صحفي صادر في 4 سبتمبر 2017 بعنوان "استخدام العملات الافتراضية الخاصة (العملات المشفرة)"؛ وتقرير للاستشارات العامة صادر في 20 يناير 2022 بعنوان "العملات المشفرة: الاتجاهات والمخاطر والتدابير".

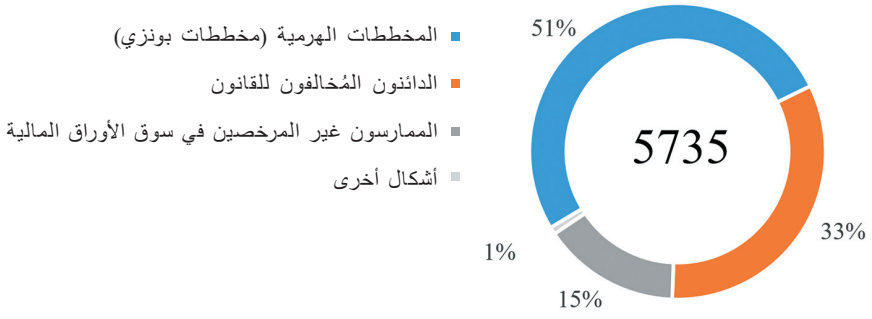
[2] مذكرة إعلامية صادرة عن بنك روسيا بشأن مخاطر التعامل بالعملات الرقمية وتوصياته للمؤسسات المالية بوقف تقديم الخدمات المتعلقة بمثل هذه المعاملات بتاريخ 29 فبراير 2024 رقم إي ان18/12-08-.

تضمين العملات المشفرة في نصف مشاريع الاستثمار الوهمية على الأقل، بينما برز العام 2023 باعتماد جميع المخططات الهرمية (مخططات بونزي) ونوادي الفوركس غير القانونية تقريبًا على الاستثمار في الرموز المميزة الداخلية أو قبول المدفوعات بالعملات المشفرة.

ويُشكل استخدام العملات المشفرة في الأنشطة غير القانونية مخاطر جسيمة، وذلك نظرًا لصعوبة تتبع المعاملات المرتبطة بها، مما قد يعيق عملية تحديد المستفيد النهائي من المخطط الإجرامي. يُظهر المجرمون قدرة استثنائية على التكيف مع المتغيرات الجديدة، ويُبتكرون باستمرار طرقًا أكثر تعقيدًا لتحويل الأموال من المشاريع الاحتيالية القائمة على العملات المشفرة. وقد كشفت دراسة حول 2944 مخططًا هرميًا تمّ الكشف عنها عام 2023، أن أكثر من 45% من تلك المخططات قد اعتمدت على أنظمة مقدّمي خدمات الدفع الأجنبية كوسيلة لتحويل الأموال من قبل "المستثمرين". وتشير التقديرات إلى أن ما يقارب من 1500 عملية احتيال قد تلقت تمويلها من خلال العملات المشفرة، مما يُسهل على منظمي هذه المخططات والمستفيدين منها الحفاظ على سرية هوياتهم.

ومع ازدياد إقبال المستهلكين على الخدمات المالية الإلكترونية وتزايد ثقتهم بالمعلومات المُتاحة على مواقع التواصل الاجتماعي، اتجهت غالبية المخططات الهرمية (مخططات بونزي)، والسماسرة الوهميين، وحتى المُقرضين غير الشرعيين إلى ممارسة أنشطتها عبر الإنترنت، مما يُعرّض عددًا متزايدًا من المستهلكين لخطر الوقوع ضحية للممارسات غير النزيهة والاحتيالية.

توزيع الكيانات ذات الخصائص الأنشطة غير القانونية، في العام 2023

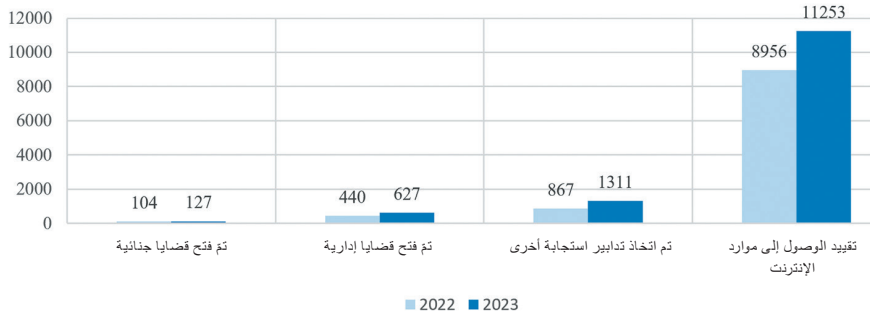


ومما لا شك أن بنك روسيا يعمل وبلا هوادة على تطوير إعدادات نظام مراقبة الفضاء المعلوماتي، سعيًا لتحسين كفاءته وفعاليته. فقد شهد العام الماضي إدخال نظام تقييم آلي للمحتوى المنشور، بينما تم دمج مواقع التواصل الاجتماعي وتطبيقات المراسلة الفورية في نظام الرصد خلال العام الذي سبقه. وقد أدى ذلك إلى تحسين نوعية وسرعة الكشف عن مقدمي الخدمات المالية غير القانونيين. وبناءً على مبادرة من بنك روسيا، تُحظر الموارد غير القانونية، لكن مُنظمو هذه المشاريع يردون بإنشاء موارد جديدة. ومن الممارسات الشائعة لدى المحتالين إنشاء مواقع إلكترونية جديدة بنفس المحتوى بعد حظر الموقع الرئيسي. ومع سعي بنك روسيا لتعزيز كفاءة عمليات الحجب وجعلها أكثر شمولًا، اتخذ البنك، بدءًا من عام 2023، خطوات تسمح بفرض قيود شاملة على الوصول إلى كل من النطاقات الأساسية ونطاقاتها الفرعية المرتبطة بكيانات ضالعة في الأنشطة غير القانونية.

إذ أنه وبتوجيه من بنك روسيا، تم خلال عام 2023 حظر الوصول إلى أكثر من 11.2 ألف موقع إلكتروني، بما في ذلك صفحات على مواقع التواصل الاجتماعي مثل فكونتاكتي وأودنوكلاسنيكي، وتطبيق تيليجرام (أكثر من 3000 صفحة وقناة وروبوت دردشة وما إلى ذلك) التي تم استخدامها من قبل جهات فاعلة غير قانونية في السوق المالية والمخططات المالية الهرمية (مخططات بونزي). وتُشير التقديرات إلى أن عدد مستخدمي الإنترنت الذين لا يمكنهم الوصول إلى المواقع المحجوبة يتجاوز 230 مليون مستخدم.

علاوةً على ذلك، نعمل منذ العام 2022 على تضمين بيانات حول الشركات المخالفة للقانون (الكيانات القانونية وأصحاب المشاريع الفردية) في منصة "اعرف عميلك، إذ تهدف هذه الخطوة إلى مساعدة البنوك على أخذ هذه المعلومات بعين الاعتبار وبشكل فوري عند تقييم المخاطر المتعلقة بعملائها وشركائهم، واتخاذ الإجراءات اللازمة لمُكافحة الأنشطة غير القانونية ضد مقدمي الخدمات المالية غير القانونيين. وحتى الآن، تم إدراج بيانات حول 2300 كيان على المنصة، تشمل المخططات المالية الهرمية (مخططات بونزي)، والمقرضين غير

التدابير المتخذة ضد المؤسسات غير القانونية والمخططات الهرمية المالية (مخططات بونزي) بناءً على طلبات بنك روسيا



المرخص لهم، ونوادي الفوركس غير القانونية وما إلى ذلك.

بالإضافة إلى ذلك، في عام 2023، حث[3] بنك روسيا المؤسسات الائتمانية على تطبيق تدابير "مكافحة غسل الأموال"، بما في ذلك تقييد إجراء المعاملات في الحسابات، على جميع المؤسسات المدرجة في "قائمة الشركات ذات مؤشرات النشاط غير القانوني" المنشورة على الموقع الرسمي لبنك روسيا، وكذلك وسطاء هذه الكيانات وذلك في حال وجود أدلة تشير إلى ذلك. ومن شأن ذلك أن يُساهم في تقليص عمر المخططات المالية الهرمية (مخططات بونزي)، ويُصعّب على مقدمي الخدمات المالية غير الشرعيين جمع الأموال، ويُخفف من حدة الضرر الذي يلحق بالمواطنين من جراء المخططات غير القانونية.

على سبيل المثال، تُشير الإحصائيات إلى ازدياد الطلب على القروض عبر الإنترنت في سوق مؤسسات التمويل الأصغر، حيث تُبرم 75% من عقود القروض مع مقدمي هذه الخدمات عبر الإنترنت، مقارنة بنسبة 66% في عام 2022. وعليه، فقد شهدت مؤسسات التمويل الأصغر ارتفاعًا ملحوظًا في حالات الاحتيال، حيث يتنكر المحتالون في صورة المقترضين للحصول على قروض ثم يمتنعون عن السداد. وفي مثل هذه المخططات، هناك طرفان متضرران.

أولاً، المواطنون حيث يتم الاحتيال عليهم من خلال قروض تُسجل بأسمائهم، مما يُدمر سجلهم الائتماني ويُلزمهم ببذل جهود وموارد كبيرة لتصحيح وتسوية العواقب. ثانيًا، مؤسسات التمويل الأصغر نفسها - حيث تتحمل الخسائر المالية الناجمة عن القروض المُقدمة للمحتالين والتي لا يتم سدادها، بالإضافة إلى مخاطرٍ جسيمة على سمعتها والتي قد تؤثر على قدرتها على الاستمرار في العمل. وتُسجّل عمليات الاحتيال المشابهة نطاقًا واسعًا، حيث ارتفع حجمها بشكل ملحوظ منذ عام 2022. وشهدت الفترة ما بين 2022 و2023 ذروة محاولات الاحتيال للحصول على قروض، حيث سجلت واحدة من كبريات مؤسسات التمويل الأصغر ما يقارب 700-350 ألف عملية من حيث عدد عمليات الاحتيال وما يقارب 4-2 مليار روبل من حيث حجم القروض. وتُشير هذه الأرقام إلى كثافة عالية لمحاولات الاحتيال وإمكانية تعرض الشركات لخسائر كبيرة. ومع ذلك، تمكنت الشركة من إحباط أكثر من 98% من هذه العمليات. ولكن يتطلب الأمر من مؤسسات التمويل الأصغر في المستقبل القريب تحسين إجراءات التحقق من الهوية ومكافحة الاحتيال بشكل أكثر فعالية عند منح القروض عبر الإنترنت. ويعمل بنك روسيا على تبادل المعلومات والأفكار بشكل فعّال مع مجتمع المهنيين بخصوص هذه المسائل.

في إطار سعيها لتعزيز حماية المستهلكين والحد من مخاطر الاحتيال المرتبطة بطلبات القروض الإلكترونية، قامت الحكومة بسن قانون[4] يرفع المسؤولية المالية للمصارف عن المعاملات الاحتيالية. وابتداءً من يوليو 2024، سيتم تطبيق إجراء جديد يُعرف باسم "المهلة الزمنية" مدتها يومان، يمنع خلالها البنك من تحويل الأموال إلى أي حساب مشبوه مدرج في قاعدة بيانات الجهة التنظيمية.

. تتيح هذه الفترة للعميل، خلال يومين، فرصة إعادة تقييم قراره، والتأكد من عدم التعامل مع محتالين، وإلغاء التحويل إن لزم الأمر. وفي حال قيام البنك بإجراء تحويل من هذا القبيل قبل انتهاء المهلة الزمنية، فسيكون ملزمًا بتعويض العميل عن الخسائر التي يتكبدها. بالإضافة إلى ذلك، يلزم القانون البنوك بقطع الوصول إلى خدماتها عن بعد للأشخاص الذين يثبت تورطهم في عمليات تحويل وسحب الأموال المسروقة، وذلك في حال تلقي البنك معلومات من وزارة الشؤون الداخلية الروسية تفيد بتورطهم في أنشطة غير قانونية. من ناحية أخرى، يُمكن للمواطنين اتخاذ خطوة استباقية لمنع عمليات الاحتيال المتعلقة بالقروض. وذلك من خلال التقدم بطلب رسمي لرفض إبرام أي عقود تتعلق بالقروض أو القروض الشخصية. وسيصبح القانون المذكور نافذًا اعتبارًا من 1 مارس 2025، وبدءًا من هذا التاريخ، سيصبح بالإمكان فرض أو إلغاء حظر ذاتي على استخدام خدمات الإنترنت من خلال بوابة "الخدمات الحكومية". وعليه، إذا قام المقرض بإبرام عقد على الرغم من وجود منع صريح، فلا يجوز له المطالبة بتنفيذ التزامات المقترض الناشئة عن ذلك العقد. ويُمكن التراجع عن قرار حظر الحصول على القروض في أي وقت إذا اقتضت الحاجة حصول الشخص على قرض أو تمويل.

ونظرًا لتزايد سرعة انتشار التفاعل عن بعد ودمجه في الحياة اليومية لمستهلكي الخدمات المالية، إلى جانب التركيز الإعلامي الكبير على العملات المشفرة والرقمية، من المرجح أن ينتقل التصدي للممارسات غير القانونية بشكل شبه كامل إلى الفضاء الإلكتروني لسوق المال.

[3] مذكرة إعلامية صادرة عن بنك روسيا تحث المؤسسات المالية على توخي الحذر بشأن المعاملات التي تتضمن كيانات تُظهر أدلة على الانخراط في أنشطة غير قانونية في السوق المالية، بتاريخ 27 ديسمبر 2023، رقم ИН-08-12/69.

[4] القانون الاتحادي المؤرخ 26 فبراير 2024 برقم 31 "تعديل القانون الاتحادي "السجلات الائتمانية" والقانون الاتحادي "القروض (الديون) الاستهلاكية"

الموضوع: توظيف التكنولوجيا الرقمية في عملية جمع المعلومات والبيانات التحليلية وغيرها، ومعالجتها وتحليلها، وغيرها من البيانات المستخدمة في أنشطة الادعاء:

دراسة حالة لنظام المعلومات والتحليل "المكتب الإلكتروني للمدعي العام".

سعيًا لتقليل الجهود غير المجدية لوكلاء النيابة العامة المرتبطة بجمع كمية هائلة من البيانات ومعالجتها، من خلال دمج التكنولوجيا الرقمية الحديثة في ممارساتهم، تعمل النيابة العامة لروسيا الاتحادية على إنشاء مشروع نظام معلوماتي تحليلي يُعرف باسم "المكتب الإلكتروني لوكيل النيابة العامة" (المشار إليه فيما يلي باسم - "نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام").

أوليغ فياتشيسلافوفيتش كيبكايف -
رئيس قسم الرقابة على تنفيذ القوانين في مجال تقنية المعلومات وحماية المعلومات في الإدارة الرئيسية للرقابة على تنفيذ التشريعات الفيدرالية

يُصبح تطوير المنتج المذكور ضرورة ملحة استجابة للاحتياجات الموضوعية المُلحّة لإعادة صياغة الأساليب التقليدية لتنظيم عمل النيابة العامة في ظل التحول الرقمي المُتسارع للعلاقات المجتمعية، والذي يتطلب تبني أدوات جديدة أكثر كفاءة وفعالية لأداء كل من المهام التحليلية والمهام المُناطة بأدوات الرقابة القضائية. وتشمل العوامل الرئيسية التي تتطلب حلولًا برمجية وتقنية مبتكرة ما يلي:

1) البيانات - يواجه المدعون العامون صعوبات متزايدة في ظل ازدياد حجم البيانات التي يتم تحليلها بشكلٍ مستمر، مما يُشكل تحدياتٍ جمةً قد لا يمكن التغلب عليها بدون استخدام أدوات أتمتة سير العمل.

2) التحليلات - إنّ إعداد التقارير والملخصات يستهلك وقتًا كبيرًا من زمن العمل المباشر للنيابة العامة، مما يُعيق إنجاز المهام الأساسية المنوطة بها. ومع ازدياد حجم المعلومات بشكل مطرد، يصبح تحليلها وتقييمها مهمةً أكثر تعقيدًا عامًا بعد عام.

3) البيانات الضخمة - تفتقر أجهزة النيابة العامة في الوقت الحالي إلى إمكانية الوصول إلى جميع المعلومات التي يمتلكها كل وكيل من وكلاء النيابة على حدة. وفي الواقع، تُستخدم هذه الأداة في إعداد وثائق محددة، لكن نادرًا ما يتم استغلال إمكانياتها الكاملة.

4) التحكم - يتطلب عمل المدعين العامين الاطلاع على معلومات مرئية واضحة حول المواعيد النهائية الحالية للتحكم، بينما قد لا يكون الاعتماد على قوائم التحكم عمليًا في جميع الأحيان.

تركز فكرة المنتج على استخدام أدوات برمجية قد تتضمن تقنيات الذكاء

الذكاء الاصطناعي

التبسيط والتوحيد

لا يلزم وجود موظف لإنشاء قاعدة البيانات
سيتم تخزين جميع أفعال الاستجابة في مجلد واحد يسهل الوصول إليه من قبل الشخص المسؤول، وستتم معالجتها تلقائيًا باستخدام أنظمة ذكية.

إعداد تقارير قابلة للتخصيص حول مواضيع محددة بنقرة زر واحدة
بناءً على نتائج إيجابية في معالجة الوثائق الفردية وتكوين قاعدة بيانات شاملة، يمكن الشروع في المرحلة التالية، وهي تدريب الذكاء الاصطناعي على إنشاء وثائق تحليلية.

إعداد تحضير ملخصات سريعة ودقيقة
توحيد وصف المخالفات وتسهيل الوصول إليها.

تحليلات بخصوص انتهاكات محددة
للحصول على جميع المعلومات المتعلقة بمعالجة انتهاكات قانون أو لائحة معينة في جميع أنحاء البلاد، لا يتطلب الأمر سوى صياغة طلب استعلام دقيق.

الاصطناعي في المستقبل، لتحقيق أتمتة عمليات جمع البيانات المتعلقة بحالة القانون والنظام العام ومعالجتها وتخزينها وتحليلها، بالإضافة إلى ممارسات النشاط الرقابي وغيره من مهام هيئات النيابة العامة.

ومن المقرر استخدام الوثائق التالية كبيانات أساسية: محاضر استجابة النيابة العامة، والمذكرات التوضيحية لتنفيذ المهام، وغيرها من الوثائق المناسبة للمعالجة بواسطة الشبكات العصبونية التوليدية، بما في ذلك استخلاص الخصائص الأساسية من ملفات النصوص ذات الصلة. ويُفترض أن يتم استخراج تقارير إحصائية وتحليلية مُلخّصة تلقائيًا من مجموعة البيانات المُحمّلة على النظام، وذلك وفقًا لمعايير محددة، مع إمكانية مراجعة هذه التقارير وتعديلها يدويًا.

على سبيل المثال، لتقييم حالة الرقابة في مجال الإسكان والمرافق العامة، سيتمكن نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام" من استخراج جميع العروض والاحتجاجات والدعاوى والأعمال الأخرى ذات الصلة بناءً على معايير محددة، والتي تتضمن إشارات إلى مخالفات للقانون في المجال المذكور، وإصدار تقرير تحليلي جاهز مع أمثلة لكل من منطقة محددة والبلاد ككل.

ومع ذلك، تُطرح بعض التساؤلات أثناء تنفيذ المهام المُوكلّة، وذلك فيما يتعلق بخصائص معالجة النصوص آليًا، مما يتطلب البحث عن حلول جوهرية.

غالبًا ما تختلف بنية ومحتوى قرارات النيابة العامة اختلافًا جذريًا بين مكاتب المدعي العام المختلفة، وذلك تبعًا

لخصائص الممارسة الإقليمية، وتراكم أسلوب نمطي لعرض المعلومات في تلك المناطق، وكثرة اقتباسات القوانين في الوثائق، بما في ذلك تلك التي لا تنطبق بشكل مباشر على المخالفات المكتشفة.

إن ما سبق يُشكل عقبة أمام المعالجة الآلية لبيانات الوثائق باستخدام تقنية المعلومات المُستندة إلى خوارزميات التعلم الآلي والتي تمت برمجتها للعمل مع البيانات المنظمة الموحدة في منطق عرض المعلومات، مما يتطلب إعادة النظر في متطلبات هذه الوثائق.

وعلى المدى الطويل، سيؤدي استخدام نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام" إلى إمكانية إعداد قرارات المدعي العام بشكل موحد في جميع مكاتب المدعي العام، مع معالجتها لاحقًا آليًا واستخراج النتائج التحليلية، بما في ذلك التنبؤية.

وقد دخلت وحدات النظام الفردية التي تُعالج البيانات المُهَيّأة التي لا تستدعي معالجة مُعقّدة مرحلة التشغيل التجريبي ومرحلة الاختبار.

وفي الواقع، تم تطبيق وظيفة تلخيص المؤشرات الرقمية بالفعل (بنقرة واحدة، مع التحقق من التحكم المنطقي)، وقد تم استخدامها عند جمع الجداول لمهام محددة، مما أدى إلى إثبات تبسيط المهام الروتينية النموذجية بشكل فعلي وتقليل وقتها بشكل كبير. بالإضافة إلى ذلك، فإن استخدام أدوات إلكترونية متقدمة مستقبلًا لمعالجة البيانات سيعزز سرعة وفعالية إبلاغ قيادة مكتب المدعي العام عن الحالة الراهنة والتطورات في أنشطة الرقابة وغيرها، خاصة في حالة عدم وجود بيانات تقريرية، مما سيؤثر إيجابًا على جودة صنع القرار الإداري.

علاوة على ذلك، يتم تشغيل مكون نظام المعلومات التحليلية "التقويم الإلكتروني للمهام"، والذي لا يقتصر فقط على مراقبة تنفيذ المهام في الوقت المحدد والبحث الفوري عن مصدرها الأصلي، ولكن يهدف أيضًا إلى أن يصبح السجل الإلكتروني الرسمي لجميع المهام الجارية مع اعتبار الوثائق غير المدرجة فيه على أنها غير قابلة للتنفيذ. وتهدف هذه الوظيفة أيضًا إلى تخفيف العبء الإداري، وبالتالي إتاحة المجال للموارد البشرية للتركيز على أداء المهام الرقابية المباشرة المنوطة بالنيابة العامة.

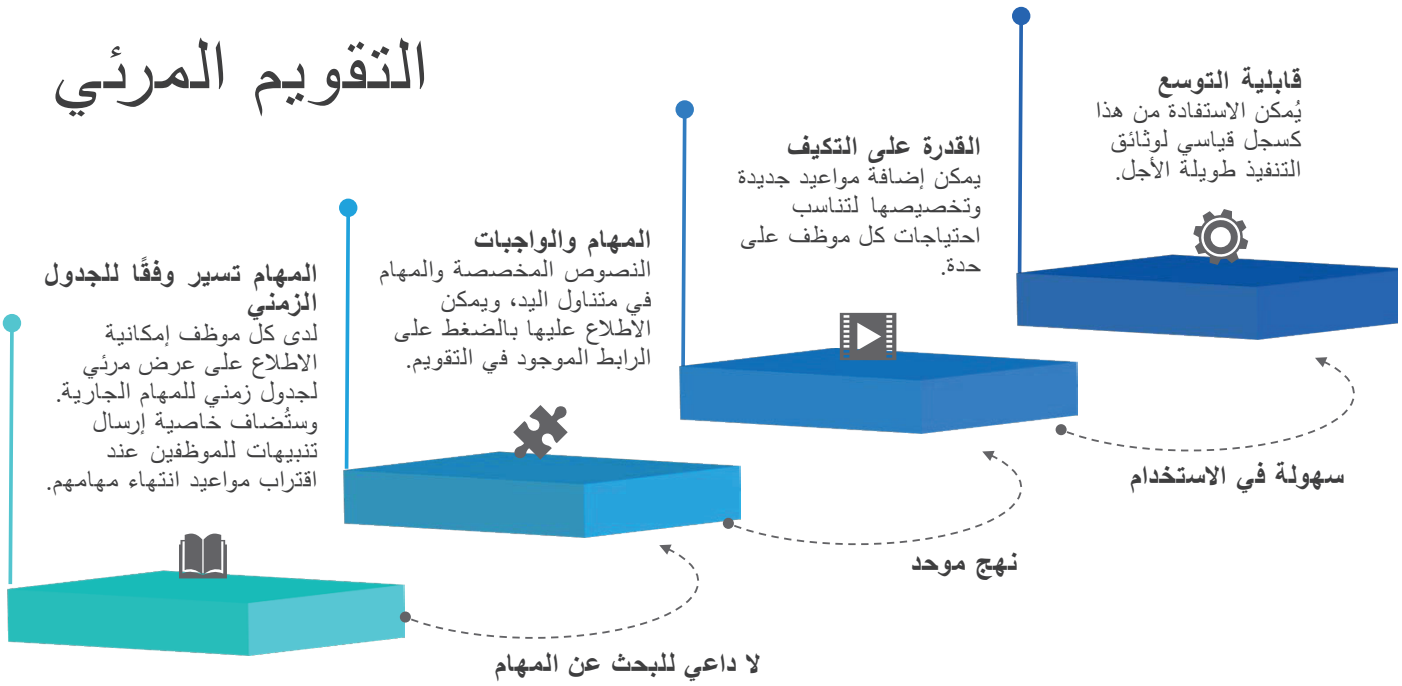
يُتيح التقويم إمكانية إدارته في كافة أفرع النيابة العامة.

وكانت مقاطعة كورغان هي السبّاقة في تطبيق هذا التوجه. إذ استفاد موظفو النيابة العامة المعنية من ميزة الروابط التشعبية المتاحة للوصول إلى المستندات المسجلة في نظام المعلومات الآلي "الرقابة الإلكترونية". وبفضل هذه الطريقة، لا يقتصر الأمر على الاطلاع على معلومات تاريخ الاستحقاق، بل يتيح الوصول السريع إلى الوثيقة التي تحدده.

أما بخصوص المذكرات التوضيحية المتعلقة بمجالات العمل، يجري اختبار إنشاء قالب إلكتروني لها، مُنظم وفقًا للتقسيم المنطقي والموضوعي للمهمة أو التكليف، مع تقييد ملئها بحد معين من الحروف المطبوعة لضمان الإيجاز، كما تم وضع معايير أخرى لملء المخطط النموذجي بهدف تحسين كفاءة البحث عن المعلومات ومعالجتها.

وسيُساعد هذا النهج على:

1) توفير تخزين آمن مع إمكانية الاستفادة من ميزات التحليل، مع إمكانية استخدام البيانات المُجمّعة لاحقًا لتدريب الذكاء الاصطناعي (يتم تخزين المعلومات في قاعدة بيانات).



2) تنفيذ بحث فوري في المذكرات التوضيحية التي تم جمعها، ورفع كفاءة استخدام البيانات المُتراكمة، مع تعزيز عملية جمعها (البحث الشامل).

3) ضمان استمرارية العمل التحليلي من خلال الاحتفاظ بسجلات جميع التقارير والمذكرات المتعلقة بنطاق الإشراف، حتى عند تغيير الموظفين، بحيث تظل جميع المعلومات متاحة للموظف الجديد.

4) دمج بيانات المذكرات التوضيحية حسب الفئات الموضوعية وفقًا للبنية المُعتمدة، مما يُساهم في تسهيل معالجة المعلومات تبعًا لحجم مهمة التحليل (تبسيط تلخيص التقارير حسب المعايير المحددة).

يتضمن نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام" وحدات متخصصة قيد الاستخدام الفعال، تُقدم مساعدة جوهرية في أنشطة النيابة العامة، وتشمل هذه الوحدات على وجه الخصوص: "سجل المواقع الإلكترونية التي تنشر محتوى غير قانوني" (المشار إليه فيما يلي باسم - السجل، سجل المواقع الإلكترونية التي تنشر محتوى غير قانوني).

وعملًا بخطاب نائب المدعي العام الأول لروسيا الاتحادية المؤرخ 12 أبريل 2023، بعنوان "تعزيز فعالية العمل في إعداد التقارير والبيانات الادعائية الإدارية بهدف حجب المعلومات المنشورة على شبكة الإنترنت التي تنتهك القانون"، تم توجيه المدعين العامين إلى الاستفادة من السجل المذكور لمقارنة عناوين الموارد الإلكترونية وتجنب تكرار تدابير الرد عليها.

قبل تبني استخدام السجل في إعداد التقارير الموجهة إلى النيابة العامة لروسيا الاتحادية بشأن الموارد الإلكترونية التي تحتوي على عروض لشراء المستندات المزيفة التي تمنح الحقوق أو تعفي من الالتزامات، كانت فعالية تدخل النيابة العامة منخفضة للغاية، حيث لم تتجاوز 15%. ويُعزى ذلك إلى تكرار المواقع المقترحة من قبلهم لإدراجها في طلب اتخاذ الإجراءات اللازمة لتقييد الوصول إلى الموارد الإعلامية.

على سبيل المثال، يمكن أن يقوم 10 مدعين عامين بالإبلاغ عن نفس المورد الإلكتروني: diplom.com. وفي الوقت نفسه، تم تخصيص وقت في كل منطقة للتحقق من المورد وإعداد حزمة الوثائق المطلوبة.

وبفضل الاستعانة بسجلّ المواقع الإلكترونية التي تنشر محتوى غير قانوني، ارتفع مستوى كفاءة عمل المدّعين العامّين في المنطقة المحدّدة بشكلٍ ملحوظٍ، إذ تراوحت النسبة بين 50 و70%. وفي حال قيام جميع المدعين العامين باستخدام المورد المناسب، من المتوقع أن يرتفع هذا المؤشر بشكل ملحوظ ليصل إلى 95%.

يلعب سجل العقود الحكومية المبرمة في إطار المشروع الوطني "الاقتصاد الرقمي" دورًا محوريًا في الارتقاء بجودة الأنشطة الرقابية.

يتيح هذا السجل، المُدرج في نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام"، للمدعين العامين الحصول على معلومات حول العقود الحكومية المبرمة في المنطقة الخاضعة لمساءلتهم في إطار هذا المشروع الوطني دون الحاجة إلى طلبات إضافية. ومصدر المعلومات هو هيئة الرقابة المالية الروسية (روسفينمونيتورينغ) وتتم عملية تحديثها بشكل دوري كل ثلاثة أشهر.

تم إبلاغ النيابة العامة على المستوى المحلي بمعلومات حول إمكانيات السجل المذكور من خلال خطاب إعلامي صادر عن النائب الأول للمدعي العام لروسيا الاتحادية مؤرخ 31 يوليو 2023 بعنوان "تنشيط إشراف النيابة العامة على إنفاذ القانون عند تنفيذ المشروع الوطني "الاقتصاد الرقمي".

وعليه، يمكن اعتبار منصة نظام المعلومات التحليلية "المكتب الإلكتروني للمدعي العام" بالفعل مساعدًا إلكترونيًا فعالًا للمدعين العامين على جميع المستويات، وفي المستقبل، يمكن أن يؤدي تطوير هذا المنتج إلى الكشف عن كامل إمكانياته، مما قد يُحدث تغييرًا جذريًا في الأساليب التقليدية لتنظيم عمل النيابة العامة، ونقل التركيز بشكل كبير من تنفيذ المهام الفنية البحتة إلى معالجة البيانات بشكل ذكي، مما سيؤدي بدوره إلى تحسين جودة الإشراف وضمان حقوق المواطنين وحرياتهم.

العملات الرقمية: رحلة البحث عن حلول

68 **أولغا تيسن**
التنظيم القانوني لتداول الأصول الافتراضية ومكافحة استخدامها لأغراض غسل الأموال وتمويل الإرهاب في بلدان محددة من مجموعة العمل الأوراسية

73 **ديمتري سيرغيفيتش ماتشيخين**
تحقيقات AML في قطاع Web-3

77 **شون منير**
إدارة الأصول الرقمية: العملات المشفرة، والرموز غير القابلة للاستبدال (NFT)، وتعزيز الأمن المالي

التنظيم القانوني لتداول الأصول الافتراضية ومكافحة استخدامها لأغراض غسل الأموال وتمويل الإرهاب في بلدان محددة من مجموعة العمل الأوراسية

شهدت تقنية السجل الموزع، على مدار ما يقرب من 15 عامًا من وجودها، تحولات جوهرية على صعيد العلاقات في هذا المجال. وقد برزت أدوات جديدة مثل الخلاطات والمفاتيح والخدمات المجهولة التي تُمكّن من إخفاء هوية صاحب المعاملات، كما ظهرت بنية تحتية متطورة لمقدمي خدمات الأصول الافتراضية (يُشار إليهم لاحقًا باسم "مقدمي خدمات الأصول الافتراضية")[1]، بما في ذلك مقدمو الخدمات الذين يعملون في السوق الموازي، كما شهدنا ازديادًا هائلاً في عدد العملات المشفرة.

أولغا تيسن -
رئيس القسم القانوني في هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)
الرئيس المشارك لفريق التقييمات والشؤون القانونية لدى مجموعة العمل الأوراسية المعنية بمكافحة غسل الأموال وتمويل الإرهاب، دكتوراه في القانون.

مثّل تقرير "العملات الافتراضية" الذي أصدرته مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) في يونيو 2014 أول وثيقة دولية رسمية تتناول موضوع الكيانات الرقمية الجديدة المخصصة للمعاملات المالية.[2] وتضمنت هذه الوثيقة التعاريف الأساسية والضرورية لفهم كيفية عمل الأصول الافتراضية، والتي تم تحديدها في ذلك الوقت، مع التركيز على المخاطر الناتجة عن استخدامها. وفي هذا السياق، تم تأكيد فرضية تم تكرارها لاحقًا مرات عديدة، وهي أن العملات الافتراضية في أيدي المجرمين تصبح أداة جديدة وقوية لنقل وتخزين الأموال بطريقة تجعلها خارج نطاق وصول وكالات إنفاذ القانون وغيرها من الهيئات المختصة الأخرى.

في شهر يونيو 2015، بعد مرور عام، أصدرت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) إرشادات حول تطبيق نهج قائم على المخاطر على الأصول الافتراضية. ويهدف هذا الدليل إلى تفصيل الطرق الأساسية للحد من مخاطر استخدام العملات الرقمية لأغراض غسل الأموال وتمويل الإرهاب.

وسّعت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) نطاق تطبيق معاييرها في أكتوبر 2018 لتشمل الأنشطة المالية المرتبطة بالأصول الافتراضية. كما تُصدر مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) تحديثات سنوية لتوصياتها منذ عام 2021. وقد نشرت مجموعة العمل المالي المعنية بمكافحة غسل الأموال

[1] مُقدمو خدمات الأصول الرقمية: مقدمو الخدمات في مجال الأصول الافتراضية هم أي شخص طبيعي أو اعتباري يقوم، في إطار نشاطه التجاري، بإجراء واحد أو أكثر من العمليات التالية نيابة عن شخص طبيعي أو اعتباري آخر أو لصالحه: تبادل الأصول الافتراضية بالعملات الورقية؛ تبادل نوع أو أكثر من الأصول الافتراضية؛ تحويل الأصول الافتراضية؛ حفظ أو إدارة الأصول الرقمية أو الأدوات أو كليهما والتي تسمح بالتحكم في الأصول الافتراضية؛ المشاركة وتقديم الخدمات المالية المرتبطة بعرض أو بيع الأصول الافتراضية // العملات الافتراضية. المصطلحات الرئيسية والمخاطر المحتملة في مجال مكافحة غسل الأموال وتمويل الإرهاب: تقرير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF)، يونيو 2014.

[2] العملات الافتراضية. المصطلحات الرئيسية والمخاطر المحتملة في مجال مكافحة غسل الأموال وتمويل الإرهاب: تقرير مجموعة العمل المالي المعنية بمكافحة غسل الأموال، يونيو 2014 // www.fatf-gafi.org

(FATF) في عام 2020 تقريرًا يحدد المؤشرات الحمراء لعمليات غسل الأموال وتمويل الإرهاب المرتبطة بتداول الأصول الافتراضية، كما أصدرت المجموعة نفسها تقريرًا منفصلاً موجهًا إلى وزراء المالية والبنوك المركزية للدول الأعضاء في مجموعة العشرين حول العملات المستقرة[3].

ومع اعتماد هذه الوثائق، تشكلت قاعدة قانونية دولية لتنظيم تداول الأصول الافتراضية في الدول بهدف مكافحة التهديدات الأمنية، بما في ذلك استخدام العملات المشفرة[4] من قبل جماعات الجريمة المنظمة العابرة للحدود، بما في ذلك لأغراض غسل الأموال أو تمويل الإرهاب[5].

وبات من الجليّ أنّ التنظيم القانوني لعمل مقدمي خدمات الأصول الافتراضية من خلال فرض متطلبات المعايير الدولية لمكافحة غسل الأموال وتمويل الإرهاب عليهم، أو حتى حظر هذه الأصول الافتراضية بشكل كامل، أصبح أمرًا لا مفر منه بالنسبة لجميع الدول.

تشمل المتطلبات الأساسية لمعايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) فيما يتعلق بتداول الأصول الافتراضية ما يلي:

- تقع على عاتق الدول مسؤولية تحديد وتقييم وتخفيف مخاطر مكافحة غسل الأموال وتمويل الإرهاب الناشئة عن معاملات الأصول الافتراضية (المشار إليها فيما يلي باسم - "الأصول الافتراضية").
- تنص معايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) على ضرورة تصنيف الأصول الافتراضية ضمن فئة الممتلكات، مما يجعلها عرضة للمساءلة القانونية في سياق الجرائم، بما في ذلك جرائم غسل الأموال وتمويل الإرهاب. وتخضع الأصول الافتراضية، بوصفها ممتلكات، لإجراءات الحظر (التجميد) والحجز والمصادرة.
- يجب إخضاع أنشطة مقدمي خدمات الأصول الافتراضية الذين يقومون بعمليات تبادل "الأصول الافتراضية" ونقلها وتخزينها لرقابة صارمة، بما في ذلك تسجيل/ ترخيص هذه الكيانات ومراقبتها. وينبغي تحميل مقدمي خدمات الأصول الافتراضية مسؤولية التحقق من هوية العملاء، وتحديد أصحابهم الحقيقيين، وإبلاغ وحدة الاستخبارات المالية عن أي عمليات مشبوهة، والاحتفاظ بالسجلات.

ينص دليل تطبيق النهج القائم على المخاطر على الأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، الصادر عن مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) في أكتوبر 2021، على أنّه يحق للدول حظر أو تقييد التعاملات بالأصول الافتراضية أو عمل مقدمي خدماتها، ويعتمد ذلك على تقييم المخاطر والتشريعات الوطنية السارية، بالإضافة إلى تحقيق أهداف سياسية أخرى، مثل حماية المستهلكين، وتعزيز الأمن والاستقرار، والحفاظ على النظام النقدي[6]. وفي حال اتخاذ قرار بمنع أو تقييد الأنشطة المتعلقة بالأصول الافتراضية داخل نطاق الدولة، فلن تنطبق أحكام التوصية 15 لمجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) في هذا الجزء، لكن ستكون الولايات القضائية ملزمة بتقييم المخاطر الناشئة. وفي حال خرق حظر تداول الأصول الافتراضية، يتعين على الدول التي فرضت هذا الحظر اتخاذ الإجراءات اللازمة ضد المخالفين (وفقًا للفقرات 108 و109 من الدليل)، بالإضافة إلى تحديد الأفراد والكيانات القانونية الذين يمارسون الأنشطة في هذا المجال دون تسجيل أو ترخيص.

وشدّد قرار مجلس الأمن التابع للأمم المتحدة رقم 1617 على أهمية التزام جميع الدول الأعضاء بمعايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) والمعايير الدولية الخاصة بمكافحة غسل الأموال وتمويل الإرهاب، الواردة في التوصيات الأربعين الصادرة عن مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) والتوصيات التسع الخاصة بمكافحة تمويل الإرهاب.

وفيما يتعلق بالنهج المتبع في تنفيذ التوصية 15 لمجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF)، هناك 3 نماذج للتنظيم القانوني لتداول الأصول الافتراضية:

1) منع تداول الأصول الافتراضية داخل نطاق الدولة وجعلها غير مقبولة كوسيلة للدفع.
2) النهج التصريحي: تقنين تداول العملات الافتراضية داخل الدولة، بما في ذلك كوسيلة للدفع، وإنشاء سوق وبنية تحتية مناسبة.
3) تنظيم تداول الأصول الافتراضية مع فرض قيود تشريعية على استخدامها وتنظيم أنشطة مقدمي خدمات الأصول الافتراضية قانونيًا. ويُعد هذا النموذج الأكثر شيوعًا في جميع أنحاء العالم.

وقد أقرّت غالبية الدول قوانين تنظم وضع الأصول الافتراضية ضمن نطاق اختصاصها القانوني، وتتناول هذه القوانين جوانب مختلفة مثل: الحظر/ السماح باستخدامها كوسيلة للدفع وإمكانية امتلاكها والاستثمار فيها وأمور أخرى ذات صلة. وعلى الرغم من أن تصنيف مزودي خدمات الأصول الافتراضية كخاضعين لقواعد مكافحة غسل الأموال وتمويل الإرهاب، يمثل أداة فعالة لمكافحة استخدام العملات المشفرة من قبل المجرمين، إلا أن تبني هذا التصنيف يتسم ببطء نسبي في العديد من البلدان.

[3] www.fatf-gafi.org
[4] وفي سياق هذه المقالة، تُعرّف العملة المشفرة على أنها عملة افتراضية لامركزية قابلة للتحويل. تُستخدم مصطلحات "العملات المشفرة" و"الأصول الافتراضية" و"الأصول المشفرة" في هذه المقالة كمصطلحات مترادفة.
[5] وثيقة مُلحقة بقرار جمعية البرلمانات لدول معاهدة الأمن الجماعي الصادر في 5 ديسمبر 2022 تحت رقم 15-6.5
[6] www.fatf-gafi.org

وتُستخدم جميع النماذج الثلاثة الموصوفة أعلاه في بلدان الاتحاد الاقتصادي الأوراسي. وبالفعل تم سن حظر على استخدام العملات الرقمية في البر الرئيسي للصين عام 2017، وكذلك في بيلاروسيا، والهند، وكازاخستان، وقيرغيزستان، وأوزبكستان، وتم تصنيف مقدمي خدمات الأصول الافتراضية كجهات تخضع لقواعد مكافحة غسل الأموال وتمويل الإرهاب، أما في روسيا الاتحادية، فقد تم سن تشريعات لتنظيم عمل مقدمي خدمات الأصول الرقمية[7]، بينما تعمل كل من طاجيكستان وتركمانستان على وضع قواعد مماثلة.

جمهورية بيلاروسيا

تم سنّ أحكام قانونية تنظم تداول الأصول الافتراضية في بيلاروسيا لأول مرة في عام 2017 من خلال مرسوم رئيس جمهورية بيلاروسيا بتاريخ 21.12.2017 رقم 8 "بشأن تطوير الاقتصاد الرقمي" [8](المشار إليه فيما بعد باسم المرسوم). إذ تهدف هذه الوثيقة إلى تهيئة البيئة المناسبة لتطبيق تقنية سلاسل الكتل "بلوكشين" وغيرها من التقنيات الحديثة التي تعتمد على مبادئ التوزيع واللامركزية والأمان في مختلف المعاملات الاقتصادية داخل الجمهورية.

عملاً بالملحق 1 للمرسوم، يُقصد بمصطلح العملة المشفرة البيتكوين، أو أي رمز رقمي آخر (رمز مميز) يُستعمل في المعاملات الدولية كوسيلة تبادل عالمية.

وفقًا للتشريعات السارية في بيلاروسيا، يُسمح لمواطني الجمهورية بشراء وبيع العملات المشفرة على أي منصات تداول للعملات المشفرة، بما في ذلك المنصات الدولية. وبالمقابل، لا يُسمح للشركات بالتعامل إلا مع الشركات المقيمة في مجمع التكنولوجيا الفائقة.[9] ويُسمح لأصحاب المشاريع الفردية بالقيام بعمليات شراء وبيع العملات المشفرة، وذلك بصفتهم مقيمين في "مجمع التكنولوجيا الفائقة" (بموجب الفقرة الفرعية 2.2 من المرسوم).

ويُحظر على الأفراد والشركات من غير المقيمين في "مجمع التكنولوجيا الفائقة" ممارسة الأنشطة التجارية التالية: تقديم المساعدة على أراضي جمهورية بيلاروسيا أو استخدام الإنترنت لأشخاص آخرين في إبرام أو تنفيذ المعاملات (العمليات) المتعلقة بالرموز المميزة (بما في ذلك العمل كطرف في هذه المعاملات (العمليات) باستخدام نظام معلومات يعمل على الإنترنت أو من خلال منح الحق (الإذن) لأشخاص آخرين لاستخدامه، وكذلك شراء أو التنازل عن الرموز المميزة، بما في ذلك تبادلها (البند الفرعي 2.6 من البند 2 من المرسوم).

تخضع أنشطة مقدمي خدمات الأصول الافتراضية داخل الدولة للتنظيم من قبل إدارة "مجمع التكنولوجيا الفائقة" والبنك الوطني لجمهورية بيلاروسيا ولجنة الرقابة الحكومية. ولا يجوز إجراء عمليات التفتيش على المقيمين في "مجمع التكنولوجيا الفائقة" دون الحصول على موافقة مسبقة من "إدارة مجمع التكنولوجيا الفائقة" (المادة 4.6 من المرسوم).

ووفقًا للتشريعات، يُسمح للمقيمين في "مجمع التكنولوجيا الفائقة" في بيلاروسيا بممارسة الأنشطة التجارية التالية، والتي تُصنف كخدمات للأصول الافتراضية وفقًا لمعايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF): بورصة العملات المشفرة، منصة تبادل العملات المشفرة، منظم العروض الأولية للعملات المشفرة (ICO)، مجموعة تعدين العملات المشفرة.

ويُصنف جميع مقدمي خدمات الأصول الافتراضية الذين يمارسون أنشطتهم على منصة "مجمع التكنولوجيا الفائقة" - ككيانات خاضعة لقواعد مكافحة غسل الأموال وتمويل الإرهاب، ويلتزمون بتنفيذ إجراءات تهدف إلى الامتثال لمتطلبات مكافحة غسل الأموال.

جمهورية كازاخستان

سنّت قواعد تنظيمية لتداول الأصول الافتراضية في جمهورية كازاخستان بموجب القانون رقم VI-347 الصادر في 25/06/2020 بشأن "التعديلات والإضافات على بعض التشريعات في جمهورية كازاخستان في المسائل المتعلقة بتنظيم التقنيات الرقمية"، وبموجب هذا القانون، تمّ الاعتراف بالأصول الرقمية كممتلكات، ولكن يُحظر استخدامها كوسيلة دفع داخل أراضي كازاخستان.

وتنقسم الأصول الرقمية في قانون العملات المشفرة إلى نوعين: الأصول المضمونة

[7] مُقدم خدمات الأصول الرقمية
[8] https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716
[9] يشار إليه فيما يلي باسم - مجمع التكنولوجيا الفائقة، المجمع

والأصول غير المضمونة. تُعتبر العملات المشفرة أصولًا غير مضمونة، ويُحظر إصدارها وتداولها داخل كازاخستان، باستثناء منطقة المركز المالي الدولي "أستانا" والتي تأسست في العام 2018.

في 18 نوفمبر 2021، تم إقرار قانون جمهورية كازاخستان رقم VII-73 بشأن "تعديل وإكمال بعض التشريعات في جمهورية كازاخستان المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب"، ووفقًا للقانون، تم تصنيف الأشخاص الذين يمارسون أنشطة إصدار الأصول الرقمية وتنظيم تداولها، بالإضافة إلى تقديم خدمات تبادل الأصول الرقمية مقابل المال والأشياء الثمينة والممتلكات الأخرى، بالإضافة إلى تحديد الكيانات الخاضعة لمراقبة المعاملات المالية. وأصبحت هذه الكيانات ملزمةً بإبلاغ الجهة المختصة في مجال المعلوماتية ببدء مزاولتها لنشاطها أو وقفه، ويتم تدوين ذلك في السجل الحكومي المخصص لهذا الغرض.

وقد حدد قانون جمهورية كازاخستان رقم VII-53 الصادر في 24 يونيو 2021 بشأن "تعديل وإكمال قانون جمهورية كازاخستان "بشأن الضرائب والمدفوعات الإلزامية الأخرى للميزانية" (قانون الضرائب) وقانون جمهورية كازاخستان بشأن "دخول قانون جمهورية كازاخستان "الضرائب والمدفوعات الإلزامية الأخرى للميزانية" (قانون الضرائب) حيز التنفيذ" - القواعد المتعلقة بفرض الضرائب على استخراج العملات الرقمية (التعدين الرقمي)

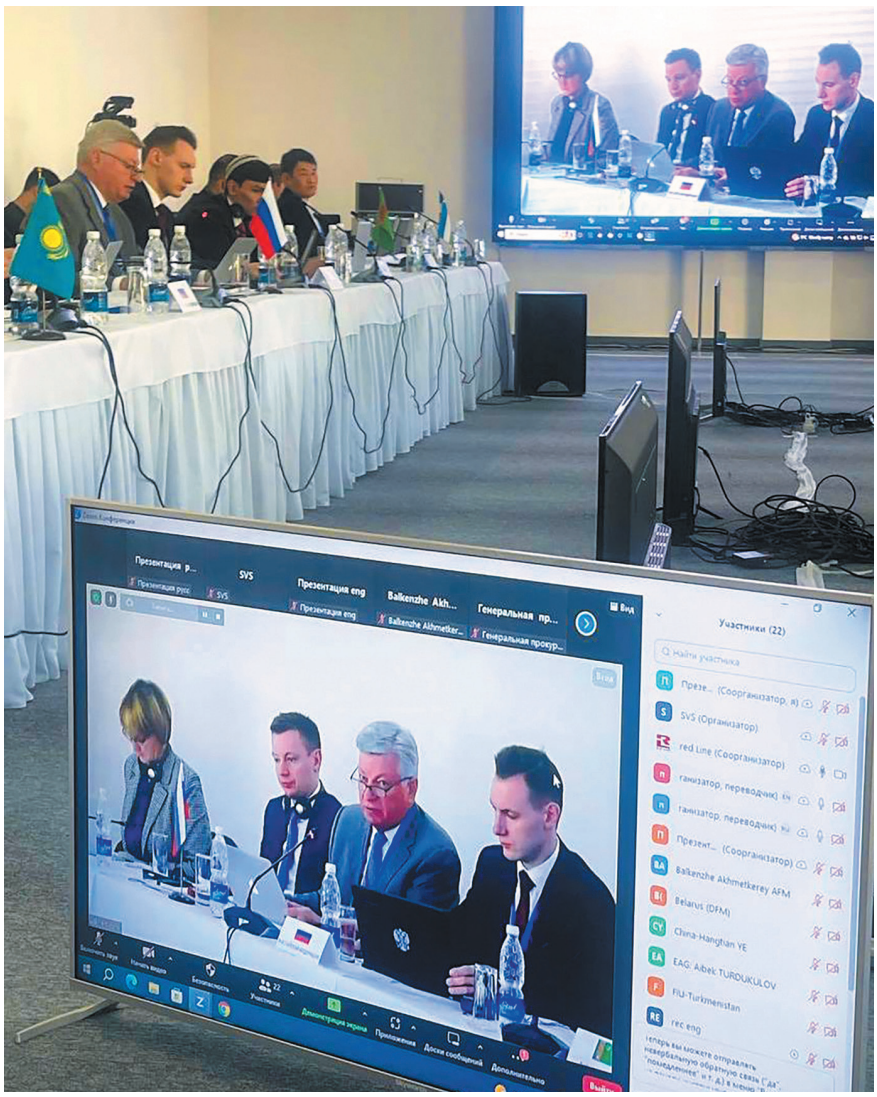
وسعيًا لتنمية قطاع الأصول الرقمية، وقّع رئيس جمهورية كازاخستان في 6 فبراير 2023 قانون جمهورية كازاخستان "الأصول الرقمية في جمهورية كازاخستان" (يُشار إليه فيما بعد باسم - "القانون")، والذي ينظم آليات الرقابة والإدارة والترخيص والضرائب على الأصول الرقمية.

وقد أوكلت مهمة تحديد الوضع القانوني لتداول الأصول الرقمية إلى وزارةِ التنمية الرقمية والابتكار وصناعة الطيران في جمهورية كازاخستان. يُحظر، بموجب قانون الأصول الرقمية، إصدار وتداول الأصول الرقمية غير المضمونة بأصول حقيقية، وكذلك عمل بورصات الأصول الرقمية الخاصة بهذه الأصول، داخل الأراضي الكازاخستانية، باستثناء منطقة المركز المالي الدولي "أستانا". كما يخضع مقدمو خدمات الأصول الرقمية، إلى جانب تداول الأصول الرقمية، لتنظيمٍ يتم تطبيقه من خلال بيئة اختبار تنظيمية في المركز المالي الدولي "أستانا".

بالإضافة إلى تداول الأصول الرقمية، تنظم قوانين المركز المالي الدولي "أستانا" مجموعة واسعة من مقدمي خدمات الأصول الرقمية، بما في ذلك بورصات العملات المشفرة، والوسطاء، والتجار، وأمناء حفظ السجلات، ومديري الصناديق، والشركات الاستشارية.

ولمنع استغلال مزودي خدمات الأصول الرقمية في غسل الأموال وتمويل الإرهاب، يتوجب على مزودي هذه الخدمات تطبيق أنظمة الرقابة الأساسية التالية: اعرف عميلك (أو كما هو شائع "know your customer") واعرف معاملتك (أو كما هو معروف "know your transaction"). ويتولى مقدمو خدمات الأصول الرقمية مهمة التحقق من هوية عملائهم والتأكد من امتثالهم للقوانين المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب، ويتم ذلك من خلال التحقق من هوية كل عميل، بالإضافة إلى التحقق من محفظته الرقمية الشخصية وسجل معاملاته.

تُصنف المادة 3 من قانون جمهورية كازاخستان بشأن "مكافحة غسل الأموال وتمويل الإرهاب" الأشخاص الذين يمارسون أنشطة إصدار الأصول الرقمية



وتنظيم تداولها وتقديم خدمات تبادل الأصول الرقمية مقابل النقود والأوراق المالية والممتلكات الأخرى بصفتهم كيانات خاضعة للرقابة المالية. وقد أصدر رئيس وكالة الرقابة المالية في جمهورية كازاخستان مرسومًا بعنوان "قواعد تقديم الكيانات الخاضعة للرقابة المالية للمعلومات والبيانات المتعلقة بالمعاملات الخاضعة للرقابة المالية وعلامات تحديد المعاملات المشبوهة"، حدد فيه علامات الكشف عن المعاملات المشبوهة في مجال الأصول الرقمية.

تُولي كازاخستان اهتمامًا خاصًا بالقواعد القانونية التي تحكم عمل مجموعات التعدين، والتي تم تصنيفها حسب معايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) بصفتها من مقدمي خدمات الأصول الافتراضية[10].

جمهورية قيرغيزستان

في 28 يوليو 2022، دخل قانون جمهورية قرغيزستان رقم 12 "الأصول الافتراضية" المؤرخ 21 يناير 2022 حيز التنفيذ. يُعرّف القانون المصطلحات الأساسية ذات الصلة بالمجال التنظيمي، ويحدد الوضع القانوني للأصول الافتراضية، وينص على متطلبات المشاركين في تداول العملات المشفرة.

ووفقًا للقانون المنظم لتداول العملات المشفرة في جمهورية قرغيزستان، يتم تحديد الجهات الفاعلة التالية كمشاركين في مجال تداول العملات المشفرة: مقدمو خدمات الأصول الافتراضية، مشغلو منصات تداول الأصول الافتراضية، بورصات العملات المشفرة، مجموعات تعدين العملات المشفرة[11].

وفقًا للبند 19 من الفقرة 1 من المادة 5 من قانون جمهورية قرغيزستان رقم 87 المؤرخ 6 أغسطس 2018 بشأن "مكافحة تمويل الإرهاب وغسل الأموال" [12](يشار

إليه فيما بعد باسم - "القانون رقم 87")، فإن مقدمي خدمات الأصول الافتراضية هم من بين المؤسسات المالية الملزمة بإجراء التحقق المناسب من هوية العملاء وإرسال تقارير عن المعاملات المشبوهة إلى وحدة الاستخبارات المالية الحكومية التابعة لوزارة المالية في جمهورية قرغيزستان، وكذلك أداء التزامات أخرى في إطار الرقابة الداخلية لمكافحة غسل الأموال وتمويل الإرهاب.

وعملًا بأحكام المواد 16 و18 و25 و28 من قانون جمهورية قرغيزستان بشأن "الأصول الافتراضية"، تم اعتماد قرار مجلس وزراء جمهورية قرغيزستان بشأن "قضايا تنظيم العلاقات الناشئة عن تداول الأصول الافتراضية" بتاريخ 16 سبتمبر 2022 برقم 514. وبموجب المادة 2 من القانون رقم 81 بشأن "تعديل بعض التشريعات في مجال الأصول الافتراضية" المؤرخ 5 أغسطس 2022، تم إدخال تعديلات على القانون رقم 87. ويُصنف مقدمو خدمات الأصول الافتراضية ضمن المؤسسات المالية، وتُطبّق عليهم جميع المتطلبات الواردة في القانون رقم 87 المتعلقة بتوصيات مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) رقم 21-10.

وتخضع أنشطة مقدمي خدمات الأصول الافتراضية في قرغيزستان للترخيص الإلزامي. حيث تصدر التراخيص عن هيئة تنظيمية وإشرافية على الأسواق المالية تابعة لوزارة الاقتصاد والتجارة في جمهورية قرغيزستان. ويقتصر تقديم خدمات الأصول الافتراضية على الأشخاص الاعتباريين المسجلين حصرًا داخل حدود الدولة.

ويخضع تواصل دائرة الاستخبارات المالية الحكومية في جمهورية قرغيزستان مع مشغلي أنظمة الدفع الإلكترونية للقانون رقم 87 ولوائح تقديم المعلومات والمستندات إلى هيئة الاستخبارات المالية في جمهورية قرغيزستان (المعتمدة بقرار حكومي لجمهورية قرغيزستان في 25 ديسمبر 2018 برقم 606). وتفرض هذه اللائحة على مقدمي خدمات الأصول الافتراضية ضرورة الالتزام بأحكامها عند تطبيق إجراءات "اعرف عميلك".

وبعد مرور 15 عامًا على ظهور العملات الرقمية، بات من الواضح أن الثغرات في الأنظمة القانونية المنظمة لتداولها تخلق مخاطر إضافية على الأمن الاقتصادي وتُضاعف احتمالية استخدامها لأغراض إجرامية.

تابعوا في العدد القادم من المجلة بقية المقال حول أنظمة تنظيم تداول العملات الرقمية في الدول الأخرى الأعضاء في بلدان رابطة الدول المستقلة ومجموعة بريكس.

[10] الفقرة 5 من المادة 11 من قانون جمهورية كازاخستان "الأصول المالية الرقمية" // https://online .zakon.kz/m/document/?doc_id=33689356
[11] http://cbd.minjust.gov.kg/act/view/ru
[12] http://cbd.minjust.gov.kg/act/view/ru-ru/111822?ysclid=loiruxojbb75473943

تحقيقات AML في قطاع Web-3

على مدار العقد الماضي، شهد عالم المال والأعمال تحولات جذرية بفعل ظهور العملات المشفرة. ويمثل ذلك، في الواقع، انبثاق نظام مالي موازٍ جديد. وبالرغم من أنّه لا يمكن الجزم بأنّ نسبة المعاملات غير القانونية في هذا النظام لا تصل إلى 100% (بل تبلغ في الواقع 0.5% فقط)، إلا أنّ عدد المخالفات لا يزال مرتفعًا بشكل كبير.

ديمتري سيرغيفيتش ماتشيخين،

- خبير دولي في أنظمة الدفع ومكافحة غسل الأموال وتمويل الإرهاب في مجال Web3
- عضو مجلس الخبراء المعني بتقنين العملات المشفرة في مجلس الدوما في روسيا الاتحادية

فنحن نتحدث هنا في المقام الأول عن غسل الأموال (Anti-Money Laundering - "AML") وتمويل الإرهاب وأشكال مختلفة من الاحتيال والقرصنة والسرقة. ولمواجهة هذه التحديات، أنشأت أدوات تقنية للرصد والتحقيق والمكافحة وجار تنفيذها بنجاح.

في هذه المقالة، سنناقش نقاط القوة والضعف للحلول القائمة لمكافحة غسل الأموال (AML) في سوق العملات المشفرة، ونحدد مختلف الأساليب المستخدمة لتحديد هوية مالكي عناوين العملات المشفرة، ونقيّم تكرار استخدام الأصول الافتراضية لأغراض إجرامية.

ما هي آثار مكافحة غسل الأموال (AML) المباشرة على العملات المشفرة؟ ومتى بدأت هذه التأثيرات؟

في بدايات عصر البيتكوين وبقية الأصول الرقمية الأولى الأخرى، لم يكن هناك أي قوانين أو إجراءات لمكافحة غسل الأموال (AML) سائدة في هذا المجال. يمكن إرجاع ظهور أسواق الإنترنت المظلمة المجهولة مثل طريق الحرير إلى هذه الفترة على وجه التحديد.

وقد اعتمدت المعايير التنظيمية على القوانين العامة (مثل القانون الإداري والقانون الجنائي والقانون الضريبي وغيرها) ولم يُبذل أي جهد لتتبع المعاملات عبر الإنترنت وتدقيقها. وبدورها، فرضت المنصات التجارية المرخصة بشكل مستقلّ إجراءات "اعرف عميلك" (KYC) (من العبارة الإنجليزية - Know Your Customer) على عملائها تماشيًا مع الأنظمة المالية.

لذلك، وإدراكًا منها لتفاقم مشكلة ازدياد شعبية العملات المشفرة، بالإضافة إلى القبض على مؤسسي موقع "طريق الحرير" (Silk Road) وكشف هوياتهم في يونيو 2014، أشارت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (المعروفة اختصارًا بالإنجليزية - FATF) لأول مرة إلى المخاطر المرتبطة بسوق العملات المشفرة.

في تلك الفترة، قامت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) بنشر تقرير بعنوان [1]"العملات الافتراضية: التعريفات الرئيسية والمخاطر المحتملة لغسل الأموال وتمويل الإرهاب" (Virtual Currencies: Key Definitions and Potential AML/CFT Risks)، حيث أوضحت فيه المخاطر المحتملة لغسل الأموال باستخدام العملات الافتراضية.

بعد مرور خمس سنوات فقط، في عام 2019، قدمت [2]مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) أولى إرشاداتها التي شملت ليس فقط المنصات التي تتعامل مع الأصول الافتراضية، ولكن أيضًا العملات المشفرة نفسها.

في المبادئ التوجيهية، حددت الهيئة التنظيمية المبادئ الأساسية لتنظيم مكافحة غسل الأموال (AML) لسوق العملات المشفرة وصلاحيات الوكالات الحكومية في هذا المجال.

الجرائم الإلكترونية المتعلقة بالعملات المشفرة: أنواعها، وتكرارها، ودورها

العملات الرقمية، التي لديها القدرة على إضفاء الطابع الديمقراطي على الأسواق المالية، تم استخدامها من قبل المجرمين.

[1] Virtual Currencies: Key Definitions and Potential AML/CFT Risks [المورد الالكتروني] // FATF. - وضع الوصول: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf (تاريخ تقديم الطلب: 20/02/2024)

[2] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [المورد الالكتروني] // FATF. - وضع الوصول: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html (تاريخ تقديم الطلب 20/02/2024)

وغالبًا ما تُستخدم الرموز المختلفة، بما في ذلك عملة البيتكوين نفسها، في مجموعة واسعة من الجرائم.

هكذا، تُستخدم العملة الرقمية لإضفاء الشرعية على عائدات الجريمة والاحتيال والابتزاز. يميل المجرمون في كثير من الأحيان إلى استخدام العملات المستقرة، وذلك لخلوها من مخاطر تقلبات الأسعار وثبات قيمتها مقابل الدولار الأمريكي، ومن أبرز الأمثلة على هذه العملات Teth-er (USDT) أو USD Coin (USDC).

على سبيل المثال، يلجأ المحتالون في كثير من الأحيان إلى انتحال شخصيات المشاهير للحصول على ثقة ضحاياهم. فقد أفاد محللو BitOK في أواخر عام 2023 [3]، بتعرض ضحايا لعمليات احتيال إلكتروني، حيث تمكن محتالون من سرقة ما يزيد عن 160 ألف دولار أمريكي عبر منصات بلوكشين متعددة. وقد تمكن المحتالون من تحقيق ذلك من خلال انتحال هوية رجل أعمال أمريكي عبر منصة يوتيوب، مستغلين منصة الفيديو الشهيرة لتنفيذ مخططهم الاحتيالي.

تُعزى جاذبية العملات المشفرة المتزايدة للتحويلات المالية العابرة للحدود بين المجرمين إلى ازدياد سرية الهوية لهذه العملات. وعلى الرغم من ذلك، تشهد الساحة العالمية توجهًا [4]متناميًا نحو تعزيز تنظيم هذه الأصول، مع ازدياد التركيز عليها.

تقسيم أحجام العملات المشفرة المرسلة إلى العناوين "المشبوهة" حسب الفئات. المصدر: Chainalysis

وعلى الرغم من ذلك، غالبًا ما يتم تضخيم استخدام العملات المشفرة في مجالات مثل تمويل الإرهاب. لذلك، تشير بيانات [5]منصة تحليل سلسلة الكتل الأمريكية Chainalysis إلى أنّه منذ عام 2017، كانت العملات المشفرة أكثر استخدامًا في مخططات الاحتيال مقارنة بتمويل الإرهاب.

تُستخدم العملات الرقمية أيضًا في تمويل الإرهاب. على الرغم من التدابير المكثفة للحد من هذا النشاط، كانت هناك بعض الحالات التي لم تكن الجهود المبذولة فيها كافية.

كيف يتم تتبع "العملات المشفرة المشبوهة" وماذا يحدث إذا تم الكشف عن عناوينها فقط؟

لكشف الأنشطة غير القانونية التي تُستخدم فيها العملات المشفرة، تطبق مجموعة متنوعة من تقنيات التعرّف والتحليل على المعاملات داخل سلسلة الكتل (بلوكشين). وفي الوقت نفسه، يرتبط نجاح التحقيقات بشكل وثيق ليس فقط بالطرق التي يستخدمها مزودو مكافحة غسل الأموال (AML)، بل أيضًا بتكتيكات مجرمي الإنترنت أنفسهم.

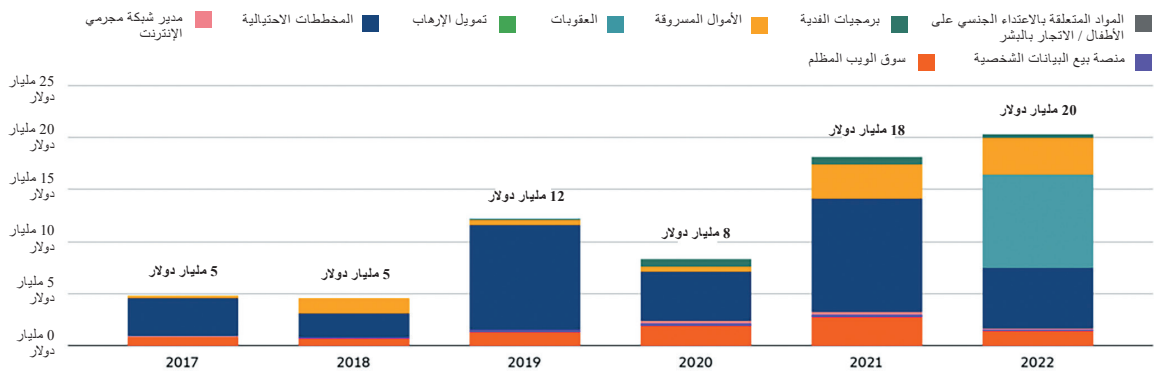
يلجأ موفرو خدمات مكافحة غسل الأموال (AML) إلى أساليب متعددة لكشف الأموال "المشبوهة". على سبيل المثال، من بين الأساليب الشائعة في مجال تتبع المعاملات المالية، "هجوم الغبار" [6](من العبارة الإنجليزية - Dust Attack) الذي يشمل توزيع كميات صغيرة من العملات المشفرة على عناوين محددة، بهدف الكشف عن هوية صاحب العنوان لاحقًا.

وقد نفى موظفو شركتي التحليلات Chainalysis وCipherTrace علنًا في وقت سابق [7]استخدام مثل هذه الأساليب في ممارساتهم. بيد أنهم اعترفوا بتبني بعض محللي سلسلة الكتل (بلوكشين) لمثل هذه الأساليب التحليلية.

ومع ذلك، لا ينحصر الأمر فقط في تحليل بيانات سلسلة الكتل (بلوكشين). عادةً ما يمتلك كبار مقدمي خدمات مكافحة غسل الأموال (AML) فرقًا كاملة من خبراء تحليلات سلسلة الكتل (بلوكشين) والتحقيقات الجنائية الذين يحددون عناوين

المصدر: Chainalysis

القيمة الكلية للعملات الرقمية التي تم تحويلها إلى عناوين (محافظ) المجرمين، 2017-2022



[3] لنساعد SpaceX: BitOK على كشف المحتالين الذين جمعوا 165 ألف دولار من خلال التبرعات [المورد الإلكتروني] // BitOK. - وضع الوصول: https://bitok.org/ru/blog/spacex_scam_giveaway_20_novl (تاريخ تقديم الطلب 25/02/2024)

[4] ستقوم Binance بحذف ANT وMULTI وVAI وXMR بتاريخ 2024/02/20 [المورد الإلكتروني] // Binance. - وضع الوصول: https://www.binance.com/en/support/announcement/binance-will-delist-ant-multi-vai-xmr-on-2024-02-20-f73b083ba6834771b07dbe5319917ae5 (تاريخ تقديم الطلب 20/02/2024)

[5] Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking 2023 [المورد الإلكتروني] // Chainalysis. - وضع الوصول: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction / (تاريخ تقديم الطلب 20/02/2024)

[6] ما هو Dusting Attack [المورد الإلكتروني] // هابر. - وضع الوصول: https://habr.com/ru/articles/450430/ (تاريخ تقديم الطلب 20/02/2024)

[7] Dust Attacks Make a Mess in Bitcoin Wallets, but There Could Be a Fix [المورد الإلكتروني] //CoinDesk. - وضع الوصول: https://www.coindesk.com/tech/2020/08/18/dust-attacks-make-a-mess-in-bitcoin-wallets-but-there-could-be-a-fix/ (تاريخ تقديم الطلب 20/02/2024)

العملات المشفرة بطريقة حتمية.

وعلى سبيل المثال، في مجال خدمات العملات المشفرة، يحدد المحللون عناوين إيداع وسحب العملات المشفرة. وباستخدام هذه الأدوات، تصبح عملية تتبع مسار الأصول الافتراضية ممكنة، بل قد تصل إلى حدّ كشف هوية صاحب العملات المشفرة في بعض الأحيان.

ربط محفظة العملة المشفرة بشبكة أجهزة الصراف الآلي للبيتكوين. المصدر: Chainalysis

يلجأ مقدمو خدمات مكافحة غسل الأموال (AML) أيضًا إلى تحليلات الاستخبارات مفتوحة المصدر (OSINT). وبشكل عام، يقتضي هذا الأمر من الخبراء دراسة البيانات[8] المتاحة للجميع على منصات مثل YouTube وTelegram وX (سابقًا Twitter) وReddit والمُنتديات والويب المظلم وغيرها من المنصات المشابهة.

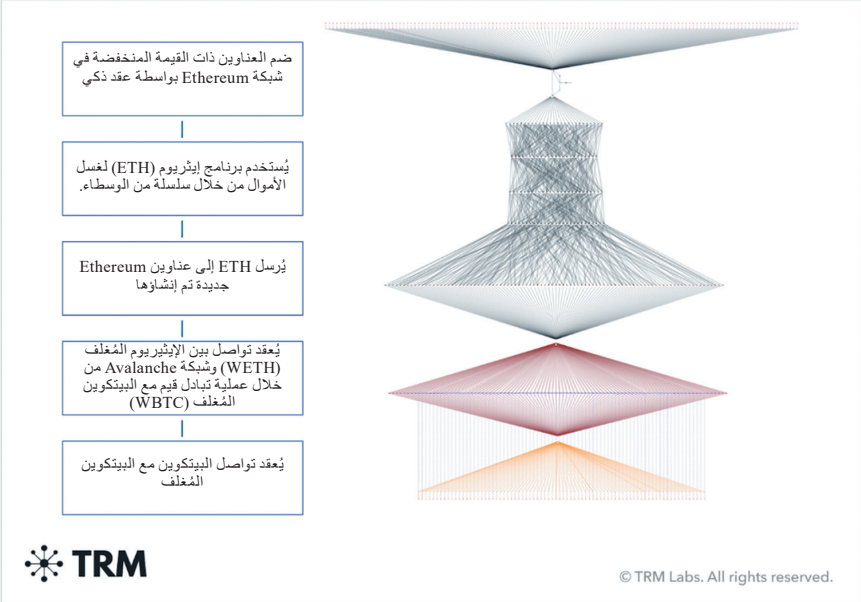
- على سبيل المثال، في روسيا، برزت حالة تمكن فيها محللو BitOK لمكافحة غسل الأموال (AML) من الكشف عن مخطط[9] فساد معقد داخل أجهزة إنفاذ القانون. وكشفت التحقيقات أن عملات البيتكوين التي صادرتها أجهزة إنفاذ القانون كانت في الواقع تحت سيطرة أفراد فاسدين.

عند توفر عناوين المحافظ فقط، يُمكن لمقدمي خدمات مكافحة غسل الأموال (AML) الاستفادة من سجلات المعاملات السابقة لتحديد أي اتصالات محتملة للمشتبه بهم بكيانات مركزية، والتي غالبًا ما تطبق إجراءات التحقق من هوية عملائها.

ويُعزز بعض مقدمي خدمات مكافحة غسل الأموال (AML) قدراتهم على مكافحة الجرائم المالية من خلال التعاون مع وكالات إنفاذ القانون وبورصات العملات المشفرة، مما يزيد من قدراتهم وسرعة تحديد الجهات الفاعلة الخبيثة.

مخطط غسل عملة الإيثيريوم (ETH) المسروقة وتحويلها إلى رموز أخرى بهدف استبدالها بعملة بيتكوين (BTC).

المصدر: TRM Labs



تلقى خلطات العملات المشفرة والجسور اللامركزية قبولًا واسعًا، مما يُصعّب عملية تتبع مصدر الأموال ووجهتها النهائية. واكتسب مزيج العملات المشفرة Torna-do Cash سمعة سيئة، حيث ابتعد عن هدفه الأصلي ليصبح أداة مفضلة للاعبين غير الشرعيين في سوق العملات المشفرة.

نقاط قوة وضعف مقدمي خدمات مكافحة غسل الأموال (AML) ومجالات التطوير المستقبلية

رغم التطورات المستمرة في خوارزميات مكافحة غسل الأموال، لا تزال هناك مجموعة من التحديات التي تواجه مقدمي هذه الخدمات. على سبيل المثال، يُعاني مقدمو الخدمات من عدم القدرة على تلقي معلومات الاستجابة من قبل بورصات تداول العملات المشفرة.

وتُشكل الاختلافات الجوهرية في متطلبات الامتثال التنظيمي بين مختلف الدول عقبة

على سبيل المثال، كشفت حادثة بارزة[10] اعتراف بورصة مركزية رائدة لتداول العملات المشفرة بأن أحد عملائها تورط بعمليات احتيال واسعة النطاق. وعلى الرغم من ذلك، لم تتخذ المنصة قرارًا بحظر عميلها، مبررةً ذلك بغياب طلب من جهات إنفاذ القانون.

Идентификация криптовалютного адреса к сети биткоин-автоматов
Источник: Chainalysis

[8] The Data Accuracy Flywheel: How Chainalysis Consistently Identifies and Verifies Blockchain Entities [المورد الإلكتروني] // Chainalysis. - وضع الوصول: https://www.chainalysis.com/blog/chainalysis-data-accuracy/ (تاريخ تقديم الطلب 20/02/2024)

[9] التحقيق: بينما انشغل الجميع بملف "التقاعد"، حدد فريق BitOK مخططًا لغسل أكثر من 5200 من عملة البيتكوين (BTC) (أكثر من 10 مليار روبل) [المورد الإلكتروني] // BitOK. - وضع الوصول: https://bitok.org/ru/blog/investigation_tambiev (تاريخ تقديم الطلب 20/02/2024)

[10] KuCoin confirms an exchange user is behind alleged daily rug pulls [المورد الإلكتروني] // Cointelegraph. - وضع الوصول: https://cointelegraph.com/news/kucoin-meme-coin-daily-rug-pull-confirmation (تاريخ تقديم الطلب 20/02/2024)

كبيرة أمام فعالية عمل مقدمي خدمات مكافحة غسل الأموال (AML) على الصعيد الدولي.

فضلًا عن ذلك، يعتمد كل مقدم رئيسي لخدمات مكافحة غسل الأموال (AML) على أساليب تحليل البيانات الداخلية وتقنيات تمييز العناوين، والتي لا يتم الكشف عنها للجمهور. وعلى الجانب الآخر، يُؤدّي ذلك إلى زيادة التنافسية في السوق وتيسير عملية الكشف عن الجرائم. من ناحية أخرى، يُؤدي عدم وجود معايير مُحددة إلى تفاوتٍ كبير في جودة الأعمال المُنجزة، ممّا يُتيح مجالًا للتلاعب بالبيانات والترميز.

وهكذا فقد عمدت مجموعة العمل المالي الدولي المعنية بمكافحة غسل الأموال (FATF) في عام 2021 إلى التواصل مع مجموعة[11] من مقدمي خدمات مكافحة غسل الأموال (AML) تشمل Coinfirm و-El liptic وMerkle Science و-Score chain، وذلك بهدف تقييم مدى تفاعل العناوين مباشرة مع البورصات، سواء داخلها أو خارجها. كان الفارق في البيانات النهائية هائلاً جدًا لدرجة أن فريق العمل المعني بمكافحة غسل الأموال (FATF) اضطر إلى الاعتراف بعدم إمكانية استخلاص استنتاجات قاطعة بناءً على النتائج التي تم الحصول عليها.

ومع تقدم تطور قاعدة بيانات موحدة للمتطلبات وإصدار شهادات جودة للخدمات المقدمة، سيتمكن مقدمو خدمات مكافحة غسل الأموال (AML) من تعزيز كفاءة عملهم بشكل كبير وضمان الأمن العام لبيئة العملات المشفرة.

إلى جانب ذلك، يُشكل ضعف التنظيم عقبة رئيسية أخرى في هذا المجال. كما تتبع العديد من الدول سياسات متباينة لتنظيم العملات المشفرة، مما يخلق مشاكل لمقدمي خدمات مكافحة غسل الأموال (AML) الذين يمارسون عملهم عبر نطاقات جغرافية متعددة. ويُشكل ذلك أيضًا عائقًا أمام التعاون الدولي في مكافحة الجرائم المالية.

وتُعدّ صياغة معايير دولية متسقة لمكافحة غسل الأموال (AML) لتنظيم سوق العملات المشفرة خطوة حاسمة لمكافحة الجرائم المالية في هذا المجال بشكل فعّال. على سبيل المثال، يبذل مسؤولو مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) جهودًا حثيثة منذ فترة طويلة لوضع معايير موحدة للتنظيم الدولي للأنظمة المالية. بيد أنه، لم يُكتب لهذا الأمر النجاح حتى هذه اللحظة.

ومن الأهمية بمكان أن تُعزّز الجهات الحكومية تعاونها مع مقدمي خدمات مكافحة غسل الأموال (AML) وذلك لتحقيق جملة من المزايا، أهمها تقصير مدة تدريب الموظفين الجدد ورفع مستوى جودة الإجراءات المُنفذة.

ومن الأهمية بمكان أيضًا تدريب خبراء مكافحة غسل الأموال (AML) حتى يتمكنوا من مواجهة الجرائم المالية بشكل فعال في مجال العملات المشفرة. وتساهم برامج التطوير المهني ودورات الاعتماد في مساعدة المتخصصين على اكتساب المهارات والكفاءات التي تتطلبها وظائفهم.

وهنا نودّ الإشارة بشكل خاص إلى التناقضات في بيانات مقدمي خدمات مكافحة غسل الأموال (AML) مع بعضهم البعض، والتي غالبًا ما تكون ناجمة عن دوافع سياسية أو عقوبات. على سبيل المثال، قد يصنف أحد مقدمي خدمات مكافحة غسل الأموال في الولايات المتحدة محفظة معينة على أنها خاضعة للعقوبات، بينما قد يمتلك مقدم خدمات مكافحة غسل الأموال في روسيا معلومات مغايرة. وفي حالة وصول الأصول من مثل هذا العنوان، على سبيل المثال، إلى بورصة مركزية قانونية، قد تنشأ اختلافات في التفسير، بما في ذلك تجميد الأموال.

الخلاصة

وفقًا لإحصائيات عام 2023، انخفضت قيمة العملات الرقمية "المشبوهة" المكتسبة من خلال الأنشطة غير القانونية إلى 24.2 مليار دولار أمريكي، مقارنة بمبلغ 39.6 مليار دولار أمريكي في عام 2022.

وعلى الرغم من أن هذا الرقم لا يزال مرتفعًا، إلا أنه يُعتبر ضئيلًا مقارنةً[12] بالمخالفات المالية في الأسواق المالية التقليدية. ومع ذلك، فإن التصدي للجرائم في قطاع Web3 يتطلب بلا شك نهجًا شاملًا.

ومن هذا المنطلق، تجدر الإشارة إلى أن هذا ينطبق فقط على "العناوين المشبوهة" المحددة بوضوح، بينما يصعب تقييم العدد الفعلي للمعاملات المشفرة الموجودة في "المنطقة الرمادية"، وكمية الأموال التي تنتهك سياسات مكافحة غسل الأموال في البنوك، وعدد الأصول المخفية عن الضرائب وكشف الهوية، وقد تكون الأرقام الحقيقية أعلى بكثير من الأرقام المقدرة، وربما بمئات المرات.

ومن الواضح أن مجرد تصميم آليات لمكافحة غسل الأموال (AML) فعّالة لن يعالج المشكلة بشكل جذري. فهناك حاجة إلى تعاون دولي، وعلى نفس القدر من الأهمية، زيادة الكفاءة في مجال مكافحة غسل الأموال للاعبين في قطاع العملات المشفرة.

ومع ذلك، لا يمكن إنكار أهمية دور مقدمي خدمات مكافحة غسل الأموال (AML) في الحد من انتشار الجرائم المتعلقة بالعملات المشفرة. فبفضل جهودهم، لم تنزلق صناعة العملات المشفرة في مستنقع من القيود التنظيمية.

وهنا يبرز دور التوازن بين الأمن والخصوصية كحجر زاوية في التنظيم الفعال. ويجب ألا تنتهك التدابير التنظيمية لمكافحة غسل الأموال (AML) حقوق المستخدمين، مع مراعاة مبادئ خصوصية البيانات وأمنها.

على الرغم من التحديات الكبيرة، يظل تحقيق مستقبل آمن للعملات المشفرة أمرًا ممكنًا. إن تحسين التكنولوجيا وزيادة التعاون الدولي وتضافر الجهود من قبل الحكومات والجهات الرقابية ومقدمي خدمات مكافحة غسل الأموال وشركات العملات المشفرة يمكن أن يمهد الطريق لإنشاء نظام آمن وشفاف لنمو صناعة العملات المشفرة.

[11] Second 12-Month Review Revised FATF Standards Virtual Assets VASPS [المورد الإلكتروني] // FATF. - وضع الوصول: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (تاريخ تقديم الطلب 20.02.2024)

[12] Fraud and Financial Crime Report 2023 [المورد الإلكتروني] // Kroll. - وضع الوصول: https://www.kroll.com/en/insights/publications/fraud-and-financial-crime-report (تاريخ تقديم الطلب 20/02/2024)

إدارة الأصول الرقمية: العملات المشفرة، والرموز غير القابلة للاستبدال (NFT)، وتعزيز الأمن المالي

لقد مثلت الثورة الرقمية، التي تميزت بظهور تقنية سلاسل الكتل (البلوكشين) والعملات المشفرة، نقطة تحول في القطاع المالي، إيذانًا ببداية حقبة جديدة. فقد فتحت هذه التقنيات آفاقًا جديدة وأدت إلى تغييرات جوهرية في كيفية عمل المؤسسات المالية.

شون منير
، الرئيس التنفيذي والمؤسس المشارك
لموقع Coinweb.com

من الأهمية بمكان إدراك الطبيعة المزدوجة للأصول الرقمية، فعلى الرغم من إمكانياتها في إحداث ثورة إبداعية وفتح آفاق جديدة، إلا أنها تُشكل في الوقت نفسه خطرًا حقيقيًا إذا تم استغلالها من قبل العناصر الإجرامية لممارسة الأنشطة غير القانونية، وعلى رأسها تمويل الإرهاب.

ومن هذا المنطلق سنوفر لك فهمًا عميقًا للأصول الافتراضية، مع استعراض أمثلة واقعية تُظهر تأثيرها على مختلف المجالات. وقد تُشكل بعض الأفكار التي ستُطرح مفتاحًا لفهمٍ أعمق لهذا المجال وتأثيره على عملك أو مؤسستك.

الحالة الراهنة للأصول الرقمية

نحن الآن في خضم الدورة الرابعة لتطور تقنيات سلاسل الكتل (البلوكشين) والعملات المشفرة. وقد تبدو هذه العملية فوضوية للوهلة الأولى، لكنها في الواقع عملية منظمة تعتمد على رأس المال السوقي والتفاعل مع المطورين والشركات الناشئة ووسائل التواصل الاجتماعي.

في عام 2024، تم اعتماد صندوق المؤشرات المتداولة (ETF) لعملة البيتكوين، ومن المتوقع أن يتم اعتماد صندوق مماثل (Ethereum-ETF) لعملة Ethereum أيضًا. في الوقت نفسه، من المنتظر أن تشهد عملة بيتكوين عملية "التقسيم إلى النصف" في شهر مايو 2024، والذي سيمثل لاحقًا بداية زيادة حادة في أسعار العملات المشفرة (فترة الصعود).

وعلى الرغم من حداثة مجال التمويل اللامركزي (DeFi)، إلا أنه حقق قفزة نوعية في تقييمه، إذ انتقل من العدم تقريبًا لتصل قيمته السوقية اليوم إلى 100 مليار دولار وقد تحقق هذا الإنجاز خلال فترة قصيرة نسبيًا امتدت من عام 2020 إلى عام 2022.

شهدت العملات المشفرة المستقرة، التي صممت للحفاظ على استقرار القيمة على غرار الدولار الأمريكي أو الذهب، انتشارًا واسعًا في المناطق التي تواجه مستويات عالية من التضخم وتقلبات العملات، ولا سيما في إفريقيا والشرق الأوسط وجنوب شرق آسيا.

في الوقت ذاته، يشهد سوق الرموز غير القابلة للاستبدال (NFT) قفزة هائلة في النمو، حيث ارتفع حجم التداول في عام 2021 إلى 44.2 مليار دولار، مقارنة بمبلغ 106 ملايين دولار فقط في العام السابق. غير أن هذا السوق لا يخلو من التحديات والمشاكل، مثل التداول الوهمي وغسل الأموال

مكافحة غسل الأموال وتمويل الأنشطة الإرهابية

في مفارقة غريبة، أصبحت العملات المشفرة، التي لطالما واجهت شكوكًا

واسعة، أول قطاع يقدم حلاً فعّالًا لمشكلة غسل الأموال.

ويعود الفضل في التقدم المحرز إلى حد كبير إلى السرعة في إصدار التشريعات بقيادة مجموعة العمل المالي (FATF)، وهي المنظمة الدولية الرائدة في مكافحة غسل الأموال وتمويل الإرهاب.

ومن هنا يتوجّب على جميع الأطراف المعنية اتّخاذ خطوات عاجلة في مسار مكافحة غسل الأموال وتمويل الإرهاب لتحقيق أهدافها. إذ لا يُعيق غياب الأطر التنظيمية المجرمين والإرهابيين عن ممارسة جرائمهم وأعمالهم الإرهابية.

القطاع الخاص بحاجة إلى قوانين تنظيمية

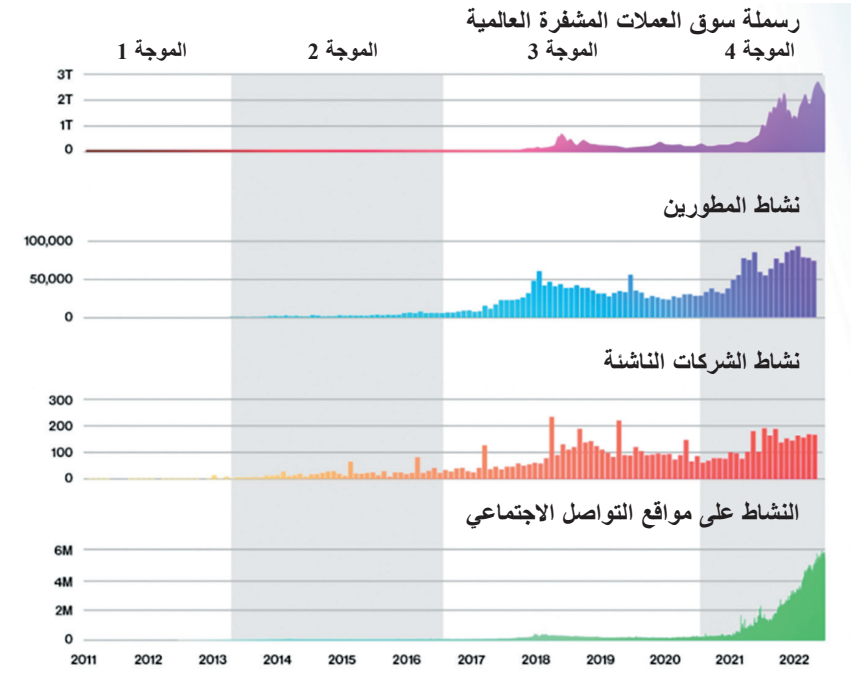
يُظهر قطاع العملات المشفرة رغبة مُلحّة في الخضوع لضوابط تنظيمية. ويأتي ذلك نتيجة تأثير الشبكة في الأسواق المالية، حيث تُفضل المؤسسات التعامل مع الشركاء المُنظمين للحد من المخاطر المحتملة.

لقد حفز الطلب على التنظيم في مجال العملات المشفرة تطوير حلول تنظيمية تنافسية، تهدف إلى تسهيل التعاون بين الشركات الناشئة في مجال العملات المشفرة والجهات الفاعلة التقليدية في السوق المالية للحصول على السيولة، مما يُعزز من استقرار السوق ويزيد من فرص النمو للجميع.

ومع أن سوق العملات المشفرة حقق نجاحات باهرة، إلا أن رسملته السوقية لا تزال متواضعة للغاية، حيث تبلغ 2 تريليون دولار مقارنة بحجم التداولات اليومية بالدولار الأمريكي البالغ 2.6 تريليون دولار.

الشراكة بين القطاع الخاص والجهات التنظيمية

للتصدي للجرائم المالية، لا بد من تكثيف الجهود وتوحيدها لتتبع مسار الأموال ومصادرها. وتقع على عاتق المؤسسات المالية مسؤولية جوهرية في منظومة مكافحة هذه الجرائم. حيث تُكلف بمهمة تحليل



سلوكيات العملاء، ورصد أي ممارسات مريبة، ومراقبة المعاملات المالية بدقة.

ويُعدّ إبلاغ وحدة الاستخبارات المالية بالأنشطة المالية المشبوهة عنصرًا أساسيًا في الجهود المُشتركة بين القطاع الخاص والهيئات التنظيمية للكشف عن الجرائم المالية والقضاء عليها.

الرموز غير القابلة للاستبدال (NFT) - أسلوب ثوري لتمثيل ملكية الأصول الرقمية

لقد أدت الرموز غير القابلة للاستبدال (NFT) إلى تغيير جذري في فهمنا للملكية الرقمية، وذلك من خلال تحويل البيانات الرقمية إلى أصول فريدة قابلة للتداول على تقنية سلاسل الكتل (البلوكشين).

وظهرت بوادر هذا الاتجاه عام 2017 من خلال مجموعة CryptoPunks التي تتألف من 10 آلاف صورة نقطية فريدة من نوعها. وقد لعبت هذه المجموعة دورًا محوريًا في إرساء معيار ERC-721، الذي يمثل الأساس للرموز غير القابلة للاستبدال (NFT) وفنّاني العملات المشفرة في الوقت الحالي.

الرموز غير القابلة للاستبدال (NFT) والجرائم

تُواكب التقنيات الحديثة مخاطر جديدة، ولا تُشكل الرموز غير القابلة للاستبدال (NFT) استثناءً من هذه القاعدة. فمع ازدياد شعبية الرموز غير القابلة للاستبدال (NFT) بشكل ملحوظ، خاصةً في ظل جائحة كوفيد19-، برزت الحاجة الملحة لإنشاء منصات آمنة وتطبيق الرقابة من قبل الجهات التنظيمية.

ومن المرجح أن تكون جائحة كورونا، إلى جانب الانخفاض في مبيعات الأعمال الفنية التقليدية قد أعادت توجيه مسار الاستثمارات إلى الرموز غير القابلة للاستبدال (NFT) حيث ارتفع حجم التداول من 106 مليون دولار في عام 2020 إلى أكثر من 17 مليار دولار في عام 2021.

تمويل الإرهاب والأصول الافتراضية

تستخدم المنظمات الإرهابية العملات المشفرة في تمويل أنشطتها.

في عام 2020، تمكنت وكالات إنفاذ القانون من إحباط مخطط لجمع التمويل من قبل تنظيم القاعدة عبر وسائل التواصل الاجتماعي. وبفضل التعاون الدولي والتنسيق

بين مختلف الجهات، تم ضبط أكثر من مليون دولار من الأموال المخصصة لتمويل الأنشطة الإرهابية.

في مطلع عام 2021، حصل الجناح العسكري لحركة حماس على ما يزيد عن 100 ألف دولار أمريكي من العملات المشفرة، تمّت مصادرة نسبة كبيرة منها من قبل السلطات الإسرائيلية.

أدت الجهود المبذولة في تعقب وتحديد مثل هذه المعاملات إلى نتائج إيجابية في الغالب، مما ساعد على الحد من غسل الأموال من خلال البورصات.

الرموز غير القابلة للاستبدال (NFT) الدعوات المنتشرة للإرهاب

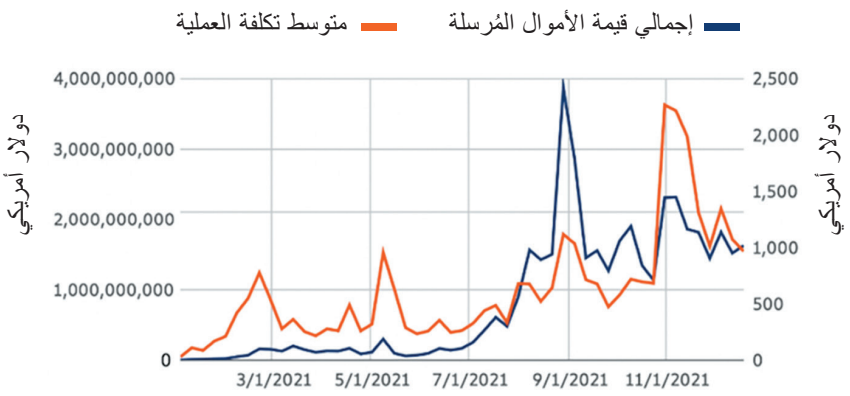
على سبيل المثال، في السادس من سبتمبر عام 2022، قام تنظيم الدولة الإسلامية* بنشر رسالة تمجّد الهجوم الإرهابي الذي وقع في أفغانستان، وذلك عبر استخدام تقنية الرموز غير القابلة للاستبدال (NFT). وقد جاءت الرسالة من تنظيم الدولة الإسلامية في خراسان، وهو الفرع التابع للتنظيم في أفغانستان.

ويُعدّ هذا الحادث أول استخدام مُسجل لاستخدام الرموز غير القابلة للاستبدال (NFT) لأغراض إرهابية. حيث قامت الجهات الفاعلة ذاتها بإنشاء سلسلة من الرموز غير القابلة للاستبدال (NFT) بهدف اختبار إمكانية الالتفاف على إجراءات إنفاذ القانون وقواعد مراجعة المحتوى على منصات الرموز غير القابلة للاستبدال (NFT) المتنوعة.

الرموز غير القابلة للاستبدال (NFT) وتمويل جماعات اليمين المتطرف

تجاوز استخدام الرمز غير القابل للاستبدال (NFT) المتمثل في "الضفدع بيبي" (أو بيبي النادر- العملة الرقمية المستوحاة من الضفدع بيبي)

"الضفدع بيبي" (أو بيبي النادر- العملة الرقمية المستوحاة من الضفدع بيبي) حدود كونه ميمي على الإنترنت، ليصبح أداة



توظفها جماعات اليمين المتطرف لتحقيق مآربها. وشهد شهر ديسمبر من عام 2020، تسجيل عملية تبرع ضخمة تمثلت في أكثر من 500 ألف دولار من عملة البيتكوين لشخصية من أتباع اليمين المتطرف.

وعند تفتيش محفظته، تم الكشف عن معاملة تحويل تهدف إلى التبرع بملكية عملة "الضفدع بيبي" (أو بيبي النادر- العملة الرقمية المستوحاة من الضفدع بيبي) الرقمية النادرة القائمة على بيتكوين لصالح مالك مجهول.

إن استخدام رمز "الضفدع بيبي" (أو بيبي النادر- العملة الرقمية المستوحاة من الضفدع بيبي) غير القابل للاستبدال (NFT) يسلط الضوء على دور رموز NFT في تمويل الأنشطة المتطرفة.

الاستنتاجات:

تُلقي الحقائق المذكورة أعلاه الضوء على مخاطر استغلال تقنية الرموز غير القابلة للاستبدال (NFT) كأداة لتمويل الأنشطة الإرهابية. تُشير هذه النتائج إلى أن جماعات متطرفة مثل اليمين المتطرف أو تنظيم الدولة الإسلامية قد تكون بصدد استكشاف طرق جديدة لجمع الأموال ونشر رسائلها باستخدام تقنيات جديدة، بما في ذلك تقنية الرموز غير القابلة للاستبدال (NFT).

لا يعد لجوء الجماعات الإرهابية إلى استخدام الرموز غير القابلة للاستبدال (NFT) لإنشاء سلسلة قيمة وتمويل أنشطتها أمرًا مستجدًا. وأصبح من الواضح أن نقل الرمز غير القابل للاستبدال (NFT) "الضفدع بيبي" (أو بيبي النادر- العملة الرقمية المستوحاة من الضفدع بيبي) وتطوير IS-NEWS #01 أمرًا لا مفر منه.

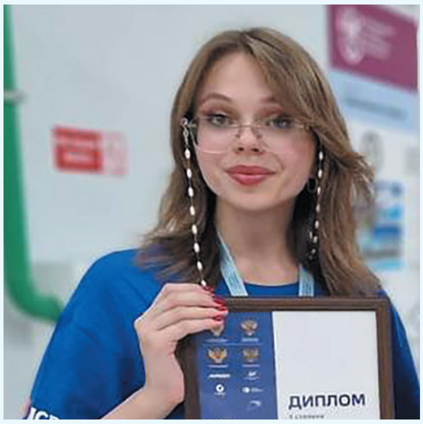
وعلى الرغم من عدم طرح هذه الرموز غير القابلة للاستبدال (NFT) للبيع، إلا أنها تبقى مسجلة على سلاسل الكتل وتنتشر عبر منصات الإنترنت المختلفة. وبالتالي فإن إجراءات وزارة العدل أو غيرها من جهات إنفاذ القانون لا تكاد تؤثر عليها.

ولا شك أنها تتمتع بمناعة عالية ضد الرقابة، الأمر الذي يُعقد بشكل كبير عملية مكافحة المحتوى المتطرف.

* منظمة إرهابية محظورة في روسيا الاتحادية

الحتمية القانونية لتنظيم عمل مقدمي خدمات الأصول الافتراضية في مجال مكافحة غسل الأموال وتمويل الإرهاب على الصعيد الدولي

وسّعت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) نطاق تطبيق معاييرها في أكتوبر 2018 لتشمل الأنشطة المالية المرتبطة بالأصول الافتراضية. كما تُصدر مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) تحديثات سنوية لتوصياتها منذ عام 2021. فقد نشرت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) في عام 2020 تقريرًا يحدد المؤشرات الحمراء لعمليات غسل الأموال وتمويل الإرهاب المرتبطة بتداول الأصول الافتراضية، كما أصدرت المجموعة نفسها تقريرًا منفصلاً موجهًا إلى وزراء المالية والبنوك المركزية للدول الأعضاء في مجموعة العشرين حول العملات المستقرة.



صوفيا رودكوفيتش -
طالبة في السنة الأولى بجامعة موسكو الحكومية التي تحمل اسم م. ف. لومونوسوف، الفائزة مرتين في الأولمبياد الدولي للأمن المالي (الأعوام 2021 و2022)
المشرف العلمي - رئيس الإدارة القانونية لهيئة المراقبة المالية الاتحادية (روسفينمونتورينغ)، حائز على دكتوراه في القانون. أو. ن. تيسن

ومع ذلك، لا تزال أنشطة مقدمي خدمات الأصول الافتراضية غير منظمة في العديد من بلدان العالم. إذ تُشكل هذه الفجوة ثغرةً أمنيةً في استخدام الأصول الافتراضية[1] ومقدمي خدماتها، مما يجعلها عرضةً للاستغلال وإساءة الاستخدام. ويُترتب على ذلك عوائقٍ أمام التحقيقات الأولية للجرائم المرتكبة باستخدام الأصول الافتراضية (مثل تمويل الإرهاب وغسل الأموال) وصعوباتٍ في حجز الأصول الافتراضية المُتحصلة بطرق غير مشروعة أو المخصصة لتمويل الإرهاب أو تجميدها أو مصادرتها.

يُعرّف مصطلح "مقدمي خدمات الأصول الافتراضية" في دليل تطبيق النهج القائم على المخاطر على الأصول الافتراضية ومقدمي خدمات الأصول الافتراضية. ويشير هذا المصطلح إلى أيّ فرد أو شركة تمارس نوعًا واحدًا أو أكثر من الأنشطة أو المهام على أساس تجاري نيابةً عن أو لصالح شخص أو شركة أخرى:

1) تبادل الأصول الافتراضية بالعملة الورقية والعكس صحيح.
2) تبادل شكل أو أكثر من أشكال الأصول الرقمية بأصول رقمية أخرى.
3) تحويل الأصول الافتراضية.
4) توفير خدمات الحفظ والإدارة الآمنة للأصول الافتراضية، بما في ذلك الأدوات التي تُمكّن أصحابها من التحكم الكامل فيها.
5) المساهمة في تسهيل وتقديم الخدمات المتعلقة بعرض أو بيع الأصول الافتراضية للشركة المصدرة[2].

بموجب الفقرة 7 من قرار مجلس الأمن التابع للأمم المتحدة رقم 1617 الصادر في 29 يوليو 2005، تُعتبر توصيات مجموعة

[1] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf, p. 3.

[2] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf, p. 109.

العمل المالي المعنية بمكافحة غسل الأموال (FATF) واجبة التنفيذ[3]. مع ذلك، خلصت مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) في عام 2022 إلى أنَّ عددًا قليلًا فقط من الدول الأعضاء قام بتنفيذ التوصيات الجديدة المتعلقة بمقدمي خدمات الأصول الافتراضية[4].

أما فيما يتعلق بالأصول الافتراضية ومقدمي خدمات الأصول الافتراضية، تُطبّق بشكل أساسي معايير مجموعة

العمل المالي المعنية بمكافحة غسل الأموال (FATF) فيما يخص:

- استخدام نهج قائم على تقييم المخاطر للأنشطة والعمليات المتعلقة بالأصول الافتراضية ومقدمي خدمات الأصول الافتراضية.
- المراقبة والإشراف على مقدمي خدمات الأصول الافتراضية لأغراض مكافحة غسل الأموال وتمويل الإرهاب.
- إجراءات الترخيص أو التسجيل.
- الإجراءات الوقائية، والتي تشمل على وجه الخصوص: التحقق الدقيق من هوية العملاء، وحفظ السجلات والمستندات، إضافة إلى الإبلاغ عن المعاملات المشبوهة.
- تطبيق العقوبات وغيرها من تدابير إنفاذ القانون.
- التعاون الدولي.

على الرغم من عدم تنظيم عمل مقدمي خدمات الأصول الافتراضية، إلا أن ذلك لا يعيق عملهم بل يُساهم في ازدياد حصة القطاع الموازي في الاقتصاد. يُمارس عدد كبير من بورصات وتجار العملات المشفرة أنشطتهم خارج إطار القانون، دون ترخيص أو رقابة من أي جهة رسمية، ودون التحقق من هوية مستخدمي العملات المشفرة، ولا تتبع معايير الامتثال، ولا الالتزام بأي متطلبات قانونية. ويخلق هذا الأمر ثغرة تسمح باستخدام العملات المشفرة في تنفيذ الأنشطة الإجرامية، مثل غسل الأموال المُتحصلة من مصادر غير قانونية وتمويل الإرهاب، والإفلات من التعرض للمساءلة القانونية[5].

ويُعدّ غياب تنظيم الوضع القانوني لمقدمي خدمات الأصول الافتراضية مشكلةً تتفاقم بشكلٍ كبير في مجال الإجراءات الجنائية. وتُسترد الأموال المكتسبة من خلال الجرائم الإلكترونية في شكل عملات رقمية بطريقتين:

1) من خلال إجراءات التحقيق أو الأنشطة الاستقصائية التشغيلية، وذلك عن طريق مصادرة محافظ العملات المشفرة "الباردة" (الأجهزة) أو الحصول على المفتاح الخاص لمالك المحفظة الرقمية، مما يمنح ضباط إنفاذ القانون إمكانية الوصول إلى العائدات الإجرامية.
2) عبر التعاون مع مقدمي خدمات الأصول الافتراضية.

في حال تعذر مصادرة المحفظة الرقمية أو المفتاح الخاص خلال التحقيقات أو الإجراءات الاستقصائية، فإن الطريقة الوحيدة لتجميد أو حظر العملات المشفرة تتمثل في إرسال وكالات إنفاذ القانون طلبًا إلى مزود خدمات الأصول الافتراضية المُستخدم من قبل المشتبه به/المتهم، يتضمن الطلب البيانات التالية: الاسم الكامل، بيانات وثيقة الهوية، الجنسية، العنوان، صورة المستخدم، بيانات الاتصال، عنوان IP، معلومات استخدام VPN، عنوان IP الفعلي عند استخدام برامج إخفاء هوية العنوان، الموقع الجغرافي، معلومات عن جهاز العميل، الإحصائيات، التفضيلات، النشاط، رقم حساب المستلم، تاريخ ووقت إنشائه، حالة عملية التبادل، مبلغ الإيداع والسحب[6]. لا يُنصح باستخدام هذه الطريقة إلا في حال كان مُقدمو خدمات الأصول الافتراضية يمارسون أنشطتهم بشكل قانوني ويقومون بالتحقق من هوية مستخدميهم وفقًا لمبادئ "اعرف عميلك" (KYC – Know Your Client)، على سبيل المثال لا الحصر، مطالبة المستخدمين الإلزامية بتقديم نسخة من جواز السفر وصورة شخصية مع جواز السفر عند التسجيل[7].

تُقدم هذه البيانات، في كثير من الأحيان، من قبل مقدّمي خدمات الأصول الافتراضية، استنادًا إلى التشريعات الوطنية المعمول بها. وفي الواقع، تظلّ هذه القاعدة المتعلقة بمزودي خدمات الأصول الافتراضية غير فعّالة إلى حدّ كبير، حيث يمتنع مزوّدو هذه الخدمات الخاضعون لسلطة قضائية أجنبية عن تقديم معلومات حول عملائهم ويتجنّبون ذلك. ونظرًا لأن بعض الدول لا تزال في طور سنّ قوانين تنظم عمل مزودي خدمات الأصول الافتراضية، تُمارس بعض الدول الأخرى سياسة الكشف عن معلومات مزودي خدمات الأصول الافتراضية المسجلين في نطاقها[8].

وبسبب المخاطر الكبيرة الناجمة عن غياب تنظيم الوضع القانوني لمقدمي خدمات الأصول الافتراضية، فإنني أرى أنه من الضروري:

1) اعتماد نهج شامل لتنظيم مقدمي خدمات الأصول الافتراضية على مستوى عالمي، يشتمل على تصنيفهم كمؤسسات تخضع لقواعد مكافحة غسل الأموال وتمويل الإرهاب، مع فرض متطلبات التسجيل والترخيص الصارمة.

---

[3] قرار مجلس الأمن التابع للأمم المتحدة رقم 1617 الصادر بتاريخ 29 يوليو 2005 (اعتمد في مدينة نيويورك في 29 يوليو 2005 في الاجتماع 5244 لمجلس الأمن التابع للأمم المتحدة) // منصة المعلومات القانونية "كونسلتانت بلوس".

[4] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, p. 7

[5] أو. ن. تيسين؛ تحديد هوية ملاك محافظات العملات المشفرة والكشف عن مفاتيحها الخاصة ومصادرتها في إطار التحقيقات الجنائية // الإجراءات الجنائية. 2024 رقم 1. ص. 83-78.

[6] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, p. 80.

[7] أو. ن. تيسين؛ الأساليب والتقنيات لكشف الجرائم والتحقيق فيها والمرتكبة باستخدام العملات المشفرة. موسكو، 2023. ص. 53

[8] أو. ن. تيسين، دور تتبع معاملات العملات المشفرة في التحقيقات الجنائية // الإجراءات الجنائية. 2024. الرقم 2. ص. 59-54، ص 59.

2) تحديد حد أدنى لمبلغ المعاملات الفردية، يلزم تجاوزه مقدمي خدمات الأصول الافتراضية بإجراء عمليات التحقق من هوية العملاء (KYC) بشكل صارم. على سبيل المثال، توصي مجموعة العمل المالي الدولية المعنية بمكافحة غسل الأموال (FATF) بحد أدنى يبلغ 1000 دولار أمريكي أو يورو.

ويُؤكد دليل مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) لعام 2021 على ضرورة التعاون الدولي بين الهيئات التنظيمية، آخذين بعين الاعتبار الطبيعة العابرة للحدود لأنشطة وخدمات مقدمي خدمات الأصول الافتراضية. ولا شك في أن ازدياد مخاطر استخدام الأصول الافتراضية في النشاطات الإجرامية خلال هذه الفترة يتطلب تعاونًا دوليًا وثيقًا لمواجهة هذه المخاطر المتنامية، مع الحرص على تجنب أي تسييسٍ لجهود مكافحة الجريمة.

لقد أسعدني أن أكون الفائزة الأولى في كل من الدورتين الأولى والثانية من الأولمبياد الدولي للأمن المالي. لقد سمعتُ عن الأولمبياد لأول مرة في الصف التاسع من خلال متابعتي لوسائل التواصل الاجتماعي، وشعرتُ بالحماس فورًا للمشاركة فيه. فمنذ الصف الثامن، كنت أُكنّ اهتمامًا كبيرًا بدراسة القانون، وانضممت إلى فريق موسكو للقانون. واستعدادًا للمشاركة في الأولمبياد، قمت بدراسة معايير مجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF) والتشريعات الروسية ذات الصلة بمكافحة غسل الأموال وتمويل الإرهاب، كما تابعتُ دروسًا مرئية حول الأمان المالي. وقد أثمرت تحضيراتي المتميزة عن وصولي إلى الدور النهائي ونيل شرف الفوز.

تختلف آليات تنظيم نهائيات مسابقة الأمان المالي الدولية بشكل جوهري عن آليات الجولات النهائية للمسابقات الأخرى المدرجة في القائمة، بما في ذلك مسابقة عموم روسيا المدرسية، التي شهدت تتويجي بالفوز مرارًا وتكرارًا خلال الفترة 2020-2022.

لقد ترك برنامج نهائي الأولمبياد الدولي للأمن المالي انطباعًا عميقًا في نفسي، وشجّعني على السعي وراء المزيد من التميز، وساعدني على تحديد طموحاتي المهنية. وكان أكثر ما أثار إعجابي في هذا الأولمبياد هو برنامج حفل ختامه. تستغرق المرحلة الختامية أسبوعًا واحدًا تقريبًا، بينما يُخصص لإنجاز المهامّ نفسها ساعتين فقط. وتُكرَّس باقي الفترة للرحلات الاستكشافية والفعاليات الترفيهية والتدريبية، والتي أتاحت لنا فرصة التعرّف على النظرية والتطبيق العملي لمكافحة غسل الأموال وتمويل الإرهاب.

تميزت فعاليات التدريب لبرنامج نهائيات الأولمبياد بأساليب تعليمية مبتكرة وفريدة من نوعها. فقد وفّرت محاكاة قضائية تفاعلية مستوحاة من فيلم "اليد الماسية" السوفيتي، إلى جانب لعبة "شرعنة الدخل المكتسب من غسل الأموال" المستمدة من أفلام الكرتون والأفلام السينمائية، تجربة ثرية وممتعة بالنسبة لي ولأصدقائي، فقد ساعدتنا هذه الأنشطة ليس فقط على تعزيز معرفتنا القانونية بل وإتاحة الفرصة لنا لإظهار مهاراتنا الإبداعية ومواهبنا التمثيلية ومهارات التواصل الفعّال.

لقد ترك لقاء السيد يوري أناتوليفيتش تشيخانشين، مدير هيئة الرقابة المالية الروسية (روسفينمونيتورينغ)، بصمة لا تُمحى في ذاكرتي. فهو رجلٌ استثنائيٌّ وإنسانٌ محترفٌ بكل معنى الكلمة.

تُلهمنا وتُثير فخرنا قصة نضال دولتنا ضد الجرائم المالية. ففي عام 2001، واجهت دولتنا اختبارًا صعبًا تمثل في إدراجها على "القائمة السوداء" لمجموعة العمل المالي المعنية بمكافحة غسل الأموال (FATF). وبفضل الجهود الجماعية، تمكنت روسيا الاتحادية، بعد مرور عقدين من الزمن، من أن تصبح دولة تتمتع بإحدى أكثر أنظمة مكافحة الجرائم المالية فعاليةً، والتي تُشكل خطرًا على الأمن المالي.

تُشكل مسيرةُ العمل في مجال الأمن المالي طموحي المستقبلي، حيث أرغب في أن أُسهم في هذا المجال كباحثة وعاملة ميدانية.

أخبار نظام مكافحة غسل الأموال

84 "ألعاب المستقبل". الفائزون في بطولة "كأس القارات الأربع" يتوافدون على قازان

85 الاجتماع الأول لمجلس بريكس لمكافحة غسل الأموال وتمويل الإرهاب ينعقد بمشاركة واسعة

85 قضايا الأمن المالي أصبحت محورًا للنقاش في مهرجان الشباب العالمي

"ألعاب المستقبل". الفائزون في بطولة "كأس القارات الأربع" يتوافدون على قازان

ضمن فعاليات دورة "ألعاب المستقبل"، استضافت مدينة قازان - عاصمة جمهورية تتارستان - نخبة من طلاب المدارس والجامعات الفائزين بالدورة الثالثة للأولمبياد الدولي للأمن المالي، من مختلف الدول المشاركة، بما في ذلك روسيا والجزائر وإيران وكوبا وقيرغيزستان وطاجيكستان وأوزبكستان.

وخلال فعاليات ختام الأولمبياد الدولي التي جرت في مدينة قازان، أبهر الشباب الحاضرون بأدائهم المتميز في بطولة كرة القدم الرقمية، واغتنموا فرصة المشاركة للتعرّف على رياضات إلكترونية أخرى.

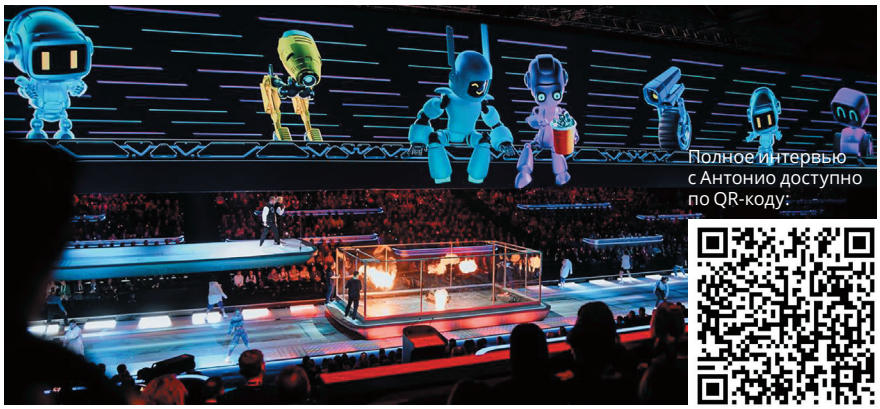
وبمبادرة من نائب رئيس حكومة روسيا الاتحادية، دميتري تشيرنيشنكو، تم توجيه دعوة للطلاب للمشاركة في فعاليات دورة "ألعاب المستقبل" للمسابقات الرياضية الدولية المتعددة.

وخلال فعاليات الأولمبياد، تألق الكوبي جوردان أنطونيو رودريغيز كضيفٍ وبطلٍ في آنٍ واحد، حاملاً معه حكاية تربطه بروسيا منذ الصغر، فجدته التي هاجرت إلى كوبا في شبابها، حافظت على ارتباطها الوثيق بوطنها الأم. لقد ترعرع الشاب على سماع قصص عن بلادنا، وحقق حلمه في عام 2023 بالمشاركة في الأولمبياد الدولي للأمن المالي في "سيريوس". طلبنا من أنطونيو أن يُشاركنا أفكاره حول مستقبل الأمن المالي الدولي فتحدث قائلًا: "في ظل العولمة المتزايدة والتطور التكنولوجي المتسارع، بات من الأهمية بمكان أن يدرك الأفراد والحكومات على حدّ سواء ضرورة حماية ممتلكاتهم الشخصية وأمن بلدهم ككل. أتطلع إلى رؤية تعاون دولي واسع النطاق في مجال الأمن المالي، تتخطى فيها الدول الخلافات السياسية والاقتصادية، وتنطلق لتتعاون من أجل القضاء على الإرهاب ومكافحة جرائم غسل الأموال. إلا أنّ هذا الهدف النبيل لا يزال حلمًا بعيد المنال في الوقت الحالي".

وقام اثنان من المشاركين، وهما فاتح بوسري من الجزائر وبحر الدين روستاموف من طاجيكستان، بتوسيع نطاق رحلتهما عبر ربوع روسيا لتشمل حضور مهرجان الشباب العالمي في المنطقة الاتحادية "سيريوس". وخلال مشاركتهم في البرنامج الحافل للمهرجان، وجد الشباب وقتًا لمشاركة أفكارهم وانطباعاتهم حول دورة "ألعاب المستقبل" والأولمبياد الدولي للأمن المالي.

وعبر بحر الدين عن آراءه قائلًا: "لقد توليت قيادة الفريق الدولي "الذئاب" لتحقيق النصر في بطولة كرة القدم الرقمية خلال الأولمبياد الدولي للأمن المالي في العام الماضي. وبفضل هذا الإنجاز، تلقينا دعوة للمشاركة في دورة "ألعاب المستقبل" في قازان، وأنا أشارك حاليًا في فعاليات مهرجان الشباب العالمي. ووجودي هنا ليس فقط من أجل تطوير معرفتي في مجال الأمن المالي، بل أيضًا لمشاركتها مع الآخرين. وأعمل بجد في هذه الآونة للتحضير للأولمبياد القادم، وأسعى بكل ما أوتيت من قوة للوصول إلى المرحلة النهائية. بالإضافة إلى ذلك، أشارك أيضًا في الأنشطة التوعوية الخاصة بالحركة، وأبذل قصارى جهدي لنشر معلومات عن المشروع في بلدي".

أما فاتح فقد أشار إلى أن لقاءاته مع شخصيات سياسية ورياضية بارزة من جميع أنحاء العالم كانت من بين أكثر تجاربه التي لا تُنسى. ويضيف" "من بين الذكريات التي حفرت في ذاكرتي وأحتفظ بها من مشاركتي في دورة "ألعاب المستقبل"، كان لقاءً مميزًا مع فخامة الرئيس الروسي فلاديمير بوتين خلال حفل الافتتاح، وشرف الحضور من مقصورة كبار الضيوف مع رؤساء الدول. لقد كان هذا شرف عظيم لي بأن أُشارككم هذا الحدث، وسيظل هذا التواجد ذكرى جميلة راسخة في ذهني. أودّ أن أعرب عن خالص شكري وتقديري لكم جميعًا على حسن استقبالكم وكرم ضيافتكم، وأتطلع بفارغ الصبر إلى فرصة العودة لزيارة روسيا مرة أخرى".



الاجتماع الأول لمجلس بريكس لمكافحة غسل الأموال وتمويل الإرهاب ينعقد بمشاركة واسعة

عقد مجلس بريكس المعني بمكافحة غسل الأموال وتمويل الإرهاب أولى اجتماعاته لعام 2024 عن بعد، مستخدمًا تقنية مؤتمر الفيديو، في مقر هيئة الرقابة المالية الروسية.

وقد تبادل المشاركون في الاجتماع وجهات النظر حول سبل تطوير أنظمة مكافحة غسل الأموال الوطنية وبلورة خطوات مشتركة لتعزيز الأمن المالي.

وفي إطار رئاسة روسيا لمجموعة بريكس، تم طرح العديد من المبادرات الرامية إلى تعزيز الشفافية في الأنظمة المالية والحد من المخاطر والتهديدات، وتوطيد التعاون بين القطاعين العام والخاص، فضلاً عن دمج الشباب في مجال الأمن المالي. وعلى وجه الخصوص، أثارت مشاريع محددة اهتمامًا كبيرًا، ونذكر منها على سبيل

المثال لا الحصر: المركز الدولي لتقييم المخاطر وخدمة "البلوكتشين الشفاف" وأولمبياد الأمن المالي الدولي والمجلس الدولي للامتثال.

كما أعربت الأطراف عن قناعتها الراسخة بأنّ مجلس بريكس لمكافحة غسل الأموال وتمويل الإرهاب يملك الإمكانيات اللازمة لتقديم مساهمة جوهرية في منظومة مكافحة غسل الأموال وتمويل الإرهاب على الصعيد العالمي، فضلًا عن دوره المحوري في تحقيق أهداف استراتيجية الشراكة الاقتصادية لمجموعة بريكس للفترة الممتدة حتى عام 2025.

قضايا الأمن المالي أصبحت محورًا للنقاش في مهرجان الشباب العالمي

في شهر مارس، انعقد حدث ضخم في مركز "سيريوس"، ضم نخبة من الشباب من مختلف أنحاء العالم.

فقد استقطب مهرجان الشباب العالمي 20 ألفًا من القادة الروس والأجانب من مختلف المجالات التي تشمل الأعمال والإعلام والتعاون الدولي والثقافة والعلوم والتعليم والعمل التطوعي والخيري والرياضة ومختلف مجالات الحياة العامة، بالإضافة إلى مشاركة مجموعات من المراهقين الذين يمثلون منظمات وجمعيات أطفال مختلفة.

ولعبت مواضيع الأمن المالي دورًا محوريًا في جدول أعمال المهرجان. وقد تميز المهرجان بمشاركة خبراء من هيئة الرقابة المالية الروسية والمركز الدولي للتدريب والمنهجيات في مجال الرقابة المالية وبنك بروسفيازبنك الذين قدموا جناح "سودروجستفو" ونظموا سلسلة من الفعاليات للمشاركين. من بينهم أكثر من 50 من المتأهلين للتصفيات النهائية في الأولمبياد الدولي للأمن المالي، بالإضافة إلى موظفين شباب من أجهزة الاستخبارات المالية من مختلف الدول.

وتعرّف الشباب على ماهية الحركة الأولمبية الدولية للأمن المالي وكيفية المشاركة في فعالياتها، بما في ذلك شروط المشاركة في أولمبياد العام

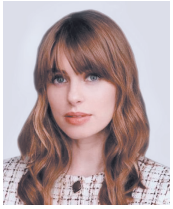
2024. وشهدت جلسات النقاش والأنشطة التفاعلية حوارات مُعمّقة، تمّ تسليط الضوء فيها على القضايا ذات الصلة بمكافحة الجرائم المالية، مع مشاركة الدول لتجاربها في هذا المجال.

هيئة التحرير

رئيس هيئة التحرير
يوري تشيخانتشين

نائب رئيس هيئة التحرير
فلاديمير أوفتشينيكوف

نائب رئيس هيئة التحرير
هيرمان نيغلياد



رئيس التحرير
إيرينا ريازانوفا

أعضاء هيئة التحرير

غالينا بوبريشيفا

إيفان كورنيف

أوليغ كريلوف

أنطون ليسيتسين

سيرغي تيتيروكوف

أليكسي بيترينكو

مارغريتا أندرونوفا

يفغيني غيليتا

مارينا شيمياكينا

هيئة الرقابة المالية الروسية والمركز الدولي التربوي والمنهجي للرصد المالي في Telegram و VKontakte

دار النشر
المؤسسة المستقلة غير الربحية
المركز الدولي التربوي والمنهجي للرصد المالي 119017، موسكو، ستارومونيتني بيريولوك، بناء 31، وحدة 1.
البريد الإلكتروني: info@mumcfm.ru
عدد النسخ: 600 نسخة
قد لا تعكس آراء هيئة التحرير بالضرورة آراء الكُتّاب.

المركز الدولي التربوي والمنهجي للرصد المالي
2024