SEGURIDAD FINANCIERA

#43
SEPTIEMBRE / 2024

PRESIDENTE - JEFE D
E LA JUNTA DIRECTIVA DEL VTB

ANDREI KOSTIN:

«La eficiencia del sistema nacional de prevención de la actividad financiera ilícita responde a los objetivos estratégicos de todos los participantes legales del mercado»

YURI CHIJANCHIN,
Director de Rosfinmonitoring,
Presidente del Comité editorial

¡ESTIMADOS LECTORES!

Bienvenidos a este número 43 de la revista, dedicado al papel de los bancos en la lucha por la seguridad financiera y a aspectos de la cooperación público-privada.

Del trabajo de las unidades de compliance de los bancos depende la seguridad de los ciudadanos y de todo el Estado en general. Para minimizar los riesgos en el ámbito de la prevención del lavado de activos ilícitos y el financiamiento del terrorismo se necesita seguir perfeccionando el funcionamiento de la inteligencia financiera y de los representantes del sector privado, la comunicación de todos los participantes del sistema nacional de antilavado.

Con estos fines siguen funcionando el Consejo de Compliance y el Consejo Internacional de Compliance que une en su plataforma las estructuras especializadas de los Estados miembros del Grupo Euroasiático de lucha contra el lavado de activos y el financiamiento del terrorismo (EAG).

Quisiera destacar el papel especial de los reguladores nacionales y los bancos, tanto en la solución de las tareas relacionadas con la seguridad financiera como en la mejora del nivel de conocimientos financieros de la población y la prevención del involucramiento de los ciudadanos en la economía sumergida. Hoy día aparecen nuevos esquemas delictivos relacionados, entre otros, con las criptomonedas, el uso de personas físicas («mulas») por defraudadores para realizar transferencias y retirar dinero efectivo.

En la situación actual, son las instituciones financieras precisamente, quienes tienen la posibilidad de detectar actividades sospechosas en la etapa primaria e informar sobre posibles amenazas. Así, según los datos del año 2023 la operatividad de presentación de reportes de operaciones sospechosas (ROS) seincrementó en el 18%, mientras que el número de ROS, enfocados en zonas de riesgo se triplicó. Asímismo, Rosfinmonitoring recibió más de 200.000 reportes de operaciones sospechosas relacionadas con la circulación de divisa digital por un importe superior a 26.000.000.000 de rublos.

¡Queridos amigos! Espero que la revista «Seguridad financiera» revelará mucha información nueva y útil para ustedes. En sus páginas podrán encontrar datos sobre las prácticas actuales de los bancos en relación con la detección de riesgos de blanqueo de activos y financiamiento del terrorismo, el fomento de la cooperación de las unidades de inteligencia financiera con el sector privado y de la cooperación internacional en esté ámbito.

ÍNDICE

6 ANDREI KOSTIN
«En Rusia se logró crear un esquema verdaderamente eficiente para la lucha contra los flujos financieros criminales»

24 MOSCÚ FUE SEDE DEL PROGRAMA «NUEVA GENERACIÓN 2024» CON LA PARTICIPACIÓN DE EMPLEADOS DE LOS SERVICIOS DE INTELIGENCIA FINANCIERA DE OCHO PAÍSES

15

MAXAT SHAGDAROV
República de Kazajistán: papel de los bancos en el ámbito de la PLA/FT

ANDREI KOSTIN:

«EN RUSIA SE LOGRÓ CREAR UN ESQUEMA VERDADERAMENTE EFICIENTE PARA LA LUCHA CONTRA LOS FLUJOS FINANCIEROS CRIMINALES»

Cada año crece la responsabilidad de los bancos como «guardianes de los flujos financieros». Solamente el año pasado el volumen de operaciones de los clientes del banco VTB, clasificados como categoría de sospechosos alcanzó 155 000 millones de rublos, informa el presidente del consejo de directores del Banco VTB, Andrei Kostin. En entrevista exclusiva a la revista «Seguridad financiera» él contó sobre la interacción con los órganos de regulación y control, el trabajo para fortalecer los mecanismos nacionales de control financiero y las medidas de detección de transacciones sospechosas

— Andrei Leonídovich, el VTB es una de las instituciones financieras clave en la economía rusa. Tan solo por esta razón el banco tiene un papel importante en el fomento de la seguridad financiera y posee un importante peritaje en este ámbito. ¿Cuáles son los resultados alcanzados desde el momento de la creación del sistema nacional antilavado?

— Estoy muy contento de poder saludar a los lectores de la revista «Seguridad financiera» y compartir en sus páginas la experiencia y el peritaje del Banco VTB.

Durante más de diez años su publicación actúa como una plataforma demandada para el intercambio de opiniones e información sobre las mejores prácticas en el ámbito de la seguridad financiera,

ofrece el análisis de las tendencias clave y los desafíos actuales en esta dirección.

Valoro mucho esta oportunidad de dirigirme a los lectores de la revista representados por profesionales que trabajan en el ámbito de la gestión pública, la ciencia, la educación y el mundo de los negocios.

La seguridad financiera es un factor muy importante para la estabilidad de la economía en general. La estabilidad y la eficiencia de las estructuras nacionales para la prevención de la actividad financiera ilícita cumple con los objetivos estratégicos de todos los participantes de buena fe del mercado, ya que aumenta su transparencia y sirve como uno de los indicadores principales de la salud financiera del sector.

Gracias a los esfuerzos sistematizados del poder ejecutivo, del regulador y de la sociedad bancaria con el papel coordinador del Servicio Federal de monitoreo financiero en Rusia se logró crear un esquema verdaderamente eficiente para la lucha contra los flujos financieros criminales.

La calidad y la fiabilidad del sistema nacional de antilavado creado en nuestro país y este camino tan largo, que el sistema logró recorrer en estas dos décadas desde el momento de su creación están certificados por evaluaciones internacionales objetivas. Como bien saben, ya en el año 2019 la Federación Rusa estuvo entre los 5 mejores países del ránking de eficiencia del Grupo de Acción Financiera Internacional (GAFI).

Comparto la evaluación de la dirección de Rosfinmonitoring, que indica que el 90% de los bancos en Rusia en la actualidad funcionan de manera fiable. Y eso, a pesar de los desafíos relacionados con las sanciones que obligaron a una parte de los clientes a buscar soluciones fuera del círculo de los bancos más grandes. Este nivel tan alto de transparencia es el resultado de un continuo trabajo de muchos años enfocado al fortalecimiento de los mecanismos nacionales de control financiero.

— ¿Cómo se construye la interacción entre el VTB y los órganos de regulación y control en el ámbito de la seguridad financiera: Rosfinmonitoring y Banco de Rusia?

— Nuestra interacción está muy bien afinada y cuenta con una nutrida experiencia, además está en constante perfeccionamiento.

Cada año las tareas que tenemos delante se hacen más complejas, aumenta la responsabilidad de los bancos en su calidad de «guardianes de los flujos financieros», como nos llaman en las publicaciones internacionales dedicadas al monitoreo financiero. Este procedimiento, lamentablemente, en gran medida es objetivo, ya que la parte contraria tampoco se queda quieta, perfecciona y amplia sus herramientas ilícitas.

He aquí tan solo un ejemplo: si hace 10 años el número de tipos o códigos de operaciones de control obligatorio en el banco VTB era 29, ahora son 75. El volumen de operaciones de nuestros clientes que son clasificados como sospechosos, en el año 2018 era 8.000 millones de rublos, pero en el año 2023 hemos identificado este tipo de acciones por un importe que asciende a 155.000 millones de rublos.

El VTB en su calidad de institución financiera sistémica participa activamente en la promoción de la agenda nacional en el ámbito de la seguridad financiera. Adoptamos un enfoque proactivo: colaboramos estrechamente con las entidades relevantes más allá de los requisitos de supervisión estándar.

Participamos de manera sistemática en investigaciones y proyectos piloto de Rosfinmonitoring. Por ejemplo, durante la pandemia, monitoreamos el uso adecuado de los fondos gubernamentales y municipales, adaptando todas las capacidades del banco a las nuevas tareas.

Estamos activamente involucrados en el proyecto piloto de lucha contra el tráfico de drogas, proporcionando, además de los informes habituales sobre operaciones sospechosas, información sobre sitios web temáticos identificados, canales de Telegram y criptomonederos.

Trimestralmente, elaboramos y enviamos a Rosfinmonitoring las nuevas tipologías y esquemas de acciones sospechosas de clientes que actualmente son más comunes o tienen un carácter masivo.

Hemos llevado a cabo investigaciones que han recibido el reconocimiento internacional y han sido destacadas por la línea del Grupo Euroasiático de lucha contra el lavado de activos y el financiamiento del terrorismo como las mejores investigaciones financieras del año.

Permítanme compartir algunos indicadores adicionales que reflejan la magnitud y la intensidad de nuestra colaboración con los organismos reguladores y de control: en 2023, VTB envió más de 13 millones de reportes obligatorios, procesó casi 9 mil solicitudes de Rosfinmonitoring

«PARTICIPAMOS DE MANERA SISTEMÁTICA EN INVESTIGACIONES Y PROYECTOS PILOTO DE ROSFINMONITORING. POR EJEMPLO, DURANTE LA PANDEMIA, MONITOREAMOS EL USO ADECUADO DE LOS FONDOS GUBERNAMENTALES Y MUNICIPALES, ADAPTANDO TODAS LAS CAPACIDADES DEL BANCO A LAS NUEVAS TAREAS

y del Banco de Rusia (incluidas las urgentes, atendidas en modo 24/7/365), y realizó 120 revisiones de la base de clientes en el marco de actualizaciones de listas de personas vinculadas al terrorismo.

Uno de los resultados de este arduo trabajo ha sido una reducción considerablemente mayor, en comparación con el promedio del sistema, en aquellas operaciones de clientes que se clasifican como sospechosos: al cierre de 2023, esta cifra fue del 27% para VTB y del 12% para el sector en general.

— ¿Cuál es el significado de este trabajo del banco VTB en el ámbito de la seguridad financiera desde el punto de vista del desarrollo socioeconómico?

— Probablemente, lo mejor sea comenzar señalando que los objetivos clave en el ámbito de la seguridad financiera son la prevención de la expansión del sector informal y la práctica del uso ilegal de fondos públicos. Es evidente que el flujo financiero sumergido obstaculiza el funcionamiento eficiente de los mecanismos económicos.

La seriedad del problema puede ilustrarse con el hecho de que, solo el año pasado, VTB rechazó la realización de operaciones sospechosas desde las cuentas de sus clientes a favor de sus contrapartes por un monto total de aproximadamente 132 mil millones de rublos. Para dar una idea de la magnitud, esta cifra es el doble de la inversión en el proyecto de la primera fase de desarrollo del aeropuerto de Púlkovo, realizado con la participación del Grupo VTB.

La eficacia del sistema nacional de seguridad financiera es un factor significativo para la confianza de los ciudadanos y las empresas en el buen desempeño de las instituciones estatales. Y esto no se refiere únicamente a la confianza en los bancos y su capacidad para financiar el sector real de la economía. Se trata

también de la seguridad en el uso de canales digitales. En la actualidad, esta es una de las principales condiciones del crecimiento.

Hoy día la confianza digital es la condición clave para la creación de una economía de éxito. El Gobierno de Rusia, por encargo del Presidente, está trabajando en el proyecto nacional «Economía de los Datos», que reemplazará al proyecto «Economía Digital», el cual finaliza este año. Esto no implica simplemente un cambio de nombre, sino una transformación profunda de los enfoques, con un mayor énfasis en la gestión de los datos y su protección como una fuente importante de crecimiento futuro.

Los principales bancos rusos, entre ellos VTB, participan activamente en la creación de la economía de los datos en varias áreas, incluyendo, por supuesto, el ámbito de la seguridad financiera.

— ¿Cuáles son las herramientas y las mejores prácticas que permiten al VTB combatir con éxito los desafíos en el ámbito de la seguridad financiera?

— Hoy en día, la realización de operaciones ilegales se ha desplazado principalmente de las transferencias clásicas de dinero entre cuentas hacia nuevas formas de pagos y transferencias, como por ejemplo, mediante números de teléfono, de tarjeta a tarjeta, y a criptomonederos.

Por eso, para los bancos, actualmente el principal instrumento es el análisis automatizado de los clientes y sus operaciones para detectar posibles actividades ilegales.

Los especialistas de VTB, con fines de monitoreo financiero, analizan diariamente alrededor de 18 millones de transacciones entrantes y salientes. Sin duda, esto sería imposible sin una automatización avanzada y el uso de inteligencia artificial.

El banco realiza un monitoreo diario para identificar y bloquear rápidamente sitios de phishing.

VTB fue uno de los primeros en establecer formatos que anteriormente no se aplicaban, como el rastreo de flujos financieros de casinos en línea, casas de apuestas y puntos de intercambio de criptomonedas. En 2023, analizamos más de 6 mil lugares virtuales de operación de estas estructuras.

> **«LOS ESPECIALISTAS DE VTB, CON FINES DE MONITOREO FINANCIERO, ANALIZAN DIARIAMENTE ALREDEDOR DE 18 MILLONES DE TRANSACCIONES ENTRANTES Y SALIENTES. SIN DUDA, ESTO SERÍA IMPOSIBLE SIN UNA AUTOMATIZACIÓN AVANZADA Y EL USO DE INTELIGENCIA ARTIFICIAL**

Últimamente prestamos una especial atención a la detección de clientes no leales: titulares nominales de las cuentas controladas por los delincuentes los llamados «mulas». Durante todo el año 2023 y el primer

semestre del 2024 en el VTB se detectaron más de 93 mil clientes con estas características y en sus cuentas fueron congelados más de 1500 millones de rublos robados.

Teniendo en cuenta que durante los últimos año y medio en el sector fueron evitadas operaciones con personas con indicios de ser «mulas» por un importe total de 4 500 millones de rublos, la aportación de nuestro banco es más que considerable.

— Ud. se refirió a la inteligencia artificial como una herramienta importante para la detección de las transacciones sospechosas. ¿Cuál es la historia de éxito de VTB en esa dirección?

— Desde el año 2018 el banco VTB aplica las tecnologías de análisis de macrodatos e implementa modelos matemáticos en los procesos de monitoreo financiero.

Uno de los primeros resultados es la apertura automática de cuentas para los nuevos clientes corporativos prácticamente sin la participación de empleados del banco.

La decisión es tomada por la máquina, basándose en el modelo de puntuación que analiza más de 50 criterios del cliente de varias fuentes, detecta valores anómalos en su conducta financiera y determina riesgos potenciales.

Gracias a la implementación de la puntuación se logró alcanzar un porcentaje de toma de decisiones automáticas positivas durante el procedimiento de alta de las compañías a un nivel del 90%. La solución se toma en 3 segundos como máximo.

Además, en el banco se lleva a cabo un continuo trabajo para desarrollar y perfeccionar los procesos de detección de transacciones sospechosas basándose en las tecnologías de inteligencia artificial. Estos procesos pueden en tiempo real analizar el flujo de transacciones individualmente para cada cliente.

La implementación de la inteligencia artificial permite emplear todo el espectro de conocimientos accesibles para el banco sobre el cliente, para poder distinguir la conducta típica para el cliente de la conducta no característica para este, y de esta manera poder detectar las operaciones fraudulentas con mayor precisión.

Según los datos del Banco de Rusia durante los últimos 7 años el número de operaciones realizadas sin el consentimiento de los clientes aumentó de manera importante: desde casi 300 mil hasta 1.000 millones al año. En su equivalente monetario las pérdidas crecieron casi en 16 veces.

En el año 2023 gracias al sistema de prevención de operaciones fraudulentas creado en el banco, VTB preservó en las cuentas de clientes particulares casi 11.000 millones de rublos. Según los resultados del primer semestre del 2024 VTB detectó más de 6 millones de estas acciones, preservando más de 4.800 millones de rublos de los clientes.

Según nuestras estimaciones, un análisis más intensivo de los datos internos del banco permite identificar un 50% más de casos de fraude. En nuestros planes inmediatos está la implementación, ya en este año, del enfoque denominado AutoML (Automated Machine Learning). Este método permite que los modelos de inteligencia artificial se autoentrenen y actualicen continuamente, con el fin de detectar casos de fraude de manera más eficiente.

Un importante y novedoso proyecto del banco VTB es el desarrollo de la tecnología de unificación segura de datos. Este es el llamado criptoanclaje, que todavía no tiene análogos en nuestro país. La tecnología permite unificar datos de diversas fuentes sin perjuicio para su seguridad, incluyendo datos para la lucha contra la actividad ilícita dirigida contra los clientes de los bancos.

Por ejemplo, el uso de un criptoanclaje para la integración de datos entre el banco y el operador de telecomunicaciones permite identificar indicadores de comportamiento atípico, como largas conversaciones con abonados desconocidos, la recepción de múltiples llamadas o mensajes de texto. Esto, a su vez, facilita una detección más precisa de casos en los que el cliente podría estar siendo influenciado con fines de fraude.

— ¿Cuál es la dinámica observada por el banco en relación con el fraude y las herramientas que utilizan los delincuentes, tales, como por ejemplo, la ingeniería social? ¿Cómo deben ser las actuales medidas de protección?

— La particularidad de este año es el crecimiento múltiple del número de casos de fraude con obtención de efectivo en las oficinas. Si en el año pasado hasta el 75% de la retirada de fondos transcurría a través de canales online y el 25% a través de las oficinas, ahora la situación es completamente inversa.

¿Cómo puede ayudar el banco? En lo que nos concierne, monitoreamos el comportamiento financiero atípico del cliente en modo «360 grados», advirtiéndole preventivamente sobre el peligro potencial a través de todos los canales posibles.

«GRACIAS A LA IMPLEMENTACIÓN DE LA PUNTUACIÓN SE LOGRÓ ALCANZAR UN PORCENTAJE DE TOMA DE DECISIONES AUTOMÁTICAS POSITIVAS DURANTE EL PROCEDIMIENTO DE ALTA DE LAS COMPAÑÍAS A UN NIVEL DEL 90%. LA SOLUCIÓN SE TOMA EN 3 SEGUNDOS COMO MÁXIMO

Sin embargo, incluso esta tutela no garantiza la protección total. Actualmente los delincuentes utilizan activamente diversos esquemas híbridos: una combinación de fishing, robo de datos personales, deepfakes con manipulación directa de la conducta de la persona.

A menudo los clientes se convierten en víctimas de la ingeniería social, ya que no comprenden cómo en realidad funciona un producto bancario determinado. Por ejemplo, el código SMS de confirmación solo llega para las operaciones de gasto, mientras que no hay códigos para los ingresos. O que la cuenta más segura es la que usted ha abierto personalmente, y no la de terceros desconocidos, y así sucesivamente.

Informamos de la manera más amplia posible a nuestros clientes y socios, así como a los medios de comunicación, sobre los nuevos métodos y trucos de los estafadores que han sido detectados. En el último año y medio, el banco ha publicado más de 50 comunicados de prensa especiales solo sobre este tema.

La problemática de la seguridad financiera es un juego constante al gato y al ratón. Los estafadores idean

esquemas cada vez más sofisticados y no dudan en aprovechar la actualidad de las noticias para acceder a los fondos de los clientes.

Cada cliente del banco debe adoptar una postura proactiva en la gestión de sus finanzas. Cabe destacar, ante todo, la importancia de usar contraseñas complejas y la autenticación de dos factores, la gestión cautelosa de los consentimientos para el tratamiento y uso de datos personales, la verificación regular de recursos significativos y su historial crediticio, así como el seguimiento de la configuración de los teléfonos inteligentes y cuentas; insto a todos a instalar únicamente aquellas aplicaciones cuyos enlaces se encuentran en recursos oficiales, como el sitio web de VTB.

> ***«LA PROBLEMÁTICA DE LA SEGURIDAD FINANCIERA ES UN JUEGO CONSTANTE AL GATO Y AL RATÓN. LOS ESTAFADORES IDEAN ESQUEMAS CADA VEZ MÁS SOFISTICADOS Y NO DUDAN EN APROVECHAR LA ACTUALIDAD DE LAS NOTICIAS PARA ACCEDER A LOS FONDOS DE LOS CLIENTES***

El viejo y buen consejo «¡Manténganse alertas!» no ha perdido su relevancia.

— En el contexto de los nuevos desafíos y amenazas en el sistema financiero, incluyendo los relacionados con el desarrollo de las tecnologías, la importancia de la alfabetización financiera y la concienciación de los ciudadanos y las empresas sobre cuestiones de seguridad financiera ha aumentado críticamente. ¿Cuál es su opinión sobre este aspecto?

— Hoy día el tema de los conocimientos financieros es especialmente importante. No es casualidad que la Estrategia nacional especializada, adoptada en octubre de 2023, tenga como objetivo no solo aumentar la alfabetización financiera, como en ediciones anteriores, sino también formar una cultura financiera.

El Banco VTB ha llevado a cabo durante muchos años diversas campañas educativas, tanto para clientes como orientadas a un público más amplio, y en 2019 se convirtió en uno de los fundadores de la Asociación Profesional para el Desarrollo de la Alfabetización Financiera.

Entre las iniciativas apoyadas por VTB se encuentra la Olimpiada Internacional de seguridad financiera en el territorio federal de «Sirius» en Sochi, que este año se celebrará por cuarta vez y reunirá a 600 escolares y estudiantes de 36 países, así como «El abecedario financiero de VTB» para los más pequeños en el programa «¡Buenas noches, pequeños!», y el proyecto «Aumento de la alfabetización financiera para personas con discapacidades auditivas» en colaboración con la Asociación de Intérpretes de Lengua de Signos.

Para las instituciones educativas, el banco ofrece formación en 4 módulos de alfabetización financiera, uno de los cuales está completamente dedicado a la seguridad financiera en el entorno digital.

Además, desde 2021, el Banco VTB ofrece a ciertas categorías de sus clientes, como pensionistas y participantes de la operación militar especial (SVO), el servicio gratuito «Seguro contra fraudes», que protege contra un amplio rango de riesgos. El programa permite compensar las pérdidas de dinero hasta 100.000 rublos. Más de 2 millones de clientes de nuestro banco reciben anualmente esta protección aseguradora.

— Los bancos comenzaron a detectar transacciones con criptomoneda con mayor frecuencia y eficiencia. En su opinión ¿qué se necesita hacer para utilizar este tipo de transacciones de forma segura?

— Tanto en la jurisdicción rusa como en las extranjeras, la regulación del comercio de criptomonedas se encuentra en fase de desarrollo. Es evidente que para la seguridad de estas transacciones se necesita claridad jurídica respecto a las funciones de los participantes del mercado de criptomonedas (mineros, bolsas, clientes, supervisión), las restricciones, los riesgos para los clientes (las criptomonedas son mucho más volátiles que el dinero fiduciario tradicional), así como la armonización de los procedimientos de compliance de los bancos.

Los bancos rusos ya han aprendido a identificar las transacciones con criptomonedas y a evaluar su naturaleza, así como a definir los roles de los participantes de este mercado.

La ley federal adoptada en agosto de 2024 en el ámbito de la regulación del minado y el uso de criptomonedas dentro de regímenes legales experimentales, crea oportunidades para que los bancos concluyan la formación de sus sistemas.

También se han creado buenas oportunidades en el marco del servicio «Cadena de bloques transparente», lanzado por Rosfinmonitoring y el Banco de Rusia, con la participación de VTB. Este servicio permite realizar investigaciones financieras, identificar a las personas que realizan operaciones con el objetivo de convertir en efectivo las criptomonedas obtenidas de la venta de drogas, el lavado de dinero de origen delictivo y el financiamiento del terrorismo.

Para un uso seguro de las criptomonedas, es necesario contar con un sistema estatal de coompliance para criptomonedas. Considero que, en este proceso de creación, los reguladores,Rosfinmonitoring y el Banco Central ya desempeñan un papel importante.

— Ud. mencionó la ley sobre el minado de criptomonedas, ¿cuáles son las perspectivas en este ámbito? ¿Cuál es la influencia de las criptomonedas en el negocio principal de los bancos comerciales?

— El impacto de las operaciones con criptomonedas en los bancos hoy en día es menos significativo que el de las transacciones sin efectivo, debido a su número limitado y al régimen legal aún en desarrollo.

La ley de la que hablamos legalizó el minado como una actividad económica, estableció los requisitos clave para los participantes del mercado de criptomonedas y la formación de su infraestructura nacional, y amplió significativamente las posibilidades de uso de los activos financieros digitales (AFD), incluyendo los derechos digitales extranjeros y la criptomoneda estable.

En caso de aprobarse actos normativos que regulen no solo el minado, sino también su comercio posterior, las criptomonedas podrían utilizarse para pagos, incluyendo los internacionales. Como es sabido, desde el 1 de septiembre la legislación permite realizar pagos transfronterizos utilizando AFD en el marco de un régimen legal experimental.

VTB planifica participar en el experimento del Banco de Rusia sobre el uso de criptomonedas para pagos transfronterizos, que se está elaborando actualmente.

— En el verano de 2023, el banco VTB presentó una serie de iniciativas interesantes relacionadas con la creación de un sistema financiero del llamado «Sur Global». ¿De qué se trata?

— Efectivamente, en el verano de 2023, el banco VTB propuso la formación de mecanismos «paralelos» o «alternativos» para el sistema financiero internacional. La iniciativa fue aprobada por el Presidente y el Gobierno de la Federación Rusa.

Se prevén acciones en cuatro direcciones. La primera es el desarrollo e implementación de una alternativa al sistema occidental de transferencia de mensajes financieros (alternativa al SWIFT).

La segunda es la ampliación del sistema de relaciones de correspondencia directa entre bancos de países no occidentales. La tercera es la creación de un centro de depósito y liquidación internacional alternativo. La cuarta es el lanzamiento de nuevos instrumentos para el mercado internacional de capitales, que no dependan de la infraestructura occidental.

Consideramos que en el marco de la cooperación económica internacional actual se están gestando condiciones que pueden propiciar cambios significativos en la configuración del sistema financiero global. En gran medida es un proceso objetivo. El fortalecimiento de la competencia geoeconómica en el mundo en los últimos años ha acelerado considerablemente este proceso. Sin embargo, una transformación tan profunda es un proceso bastante largo.

Hoy día estamos en un punto de inflexión, cuando la idea comienza a ganar aceptación entre las masas: vemos la disposición fundamental de nuestros socios a discutir la creación de mecanismos alternativos.

Este diálogo se lleva a cabo principalmente en el marco de los BRICS. Su resultado sería el lanzamiento de la Plataforma BRICS Bridge, una plataforma multilateral para realizar pagos transfronterizos en monedas nacionales utilizando monedas digitales de bancos centrales o activos digitales estatales. Estoy seguro de que este tema se desarrollará en la próxima cumbre de los BRICS en Kazán, en octubre de este año. ¡Esperamos discusiones interesantes!

«PARA LAS INSTITUCIONES EDUCATIVAS, EL BANCO OFRECE FORMACIÓN EN 4 MÓDULOS DE ALFABETIZACIÓN FINANCIERA, UNO DE LOS CUALES ESTÁ COMPLETAMENTE DEDICADO A LA SEGURIDAD FINANCIERA EN EL ENTORNO DIGITAL

EL DIÁLOGO Y LA COOPERACIÓN COMO BASE PARA MEJORAR LAS COMPETENCIAS EN EL ÁMBITO DE LA SEGURIDAD FINANCIERA

En cuanto al sistema contra el lavado de dinero, la confianza entre los participantes es el elemento clave, diría yo, el factor que une a todos. Son importantes los esfuerzos conjuntos sobre una base de asociación, donde cada participante esté dispuesto a compartir problemas y riesgos, y lo más importante, los métodos para reducirlos

GALINA BOBRIISHEVA,
Directora adjunta del Servicio Federal de Monitoreo Financiero

El todo es más que la suma de sus partes.
Aristóteles

Hace tan solo algo más de 20 años se tomó la decisión sobre la creación del sistema ruso de antilavado. Hoy este sistema une más de 200.000 participantes. Y se puede decir con certeza que una condición clave para su desarrollo efectivo son las relaciones de confianza entre los socios, tanto dentro del sistema como con los corresponsales externos, para responder a los desafíos y amenazas actuales.

Es evidente que la disponibilidad de cualquier información y la colosal velocidad de su difusión, la digitalización de la identidad y de los servicios financieros, así como las posibilidades en línea, otorgan ventajas no solo a los mercados legales.

El mundo criminal y la delincuencia transnacional utilizan métodos cada vez más sofisticados. Las principales ventajas de la digitalización (accesibilidad y velocidad), multiplicadas por la inmadurez de los sistemas de cumplimiento de los nuevos jugadores del mercado financiero, son aprovechadas por la economía sumergida y crean condiciones para el enriquecimiento ilegal.

Surgen constantemente nuevas y nuevas técnicas que se integran en la interfaz habitual y en los métodos de comunicación más populares. Hace apenas 3-4 años, la principal categoría de víctimas de los estafadores financieros eran los representantes de la generación mayor, ya que no eran los usuarios más avanzados. Hoy en día, las principales víctimas son los jóvenes activos, que son consumidores masivos de las nuevas tecnologías.

¿Qué indica esta estadística? En primer lugar, habla de un notable incremento en la complejidad y sofisticación de las estafas, que explotan el hábito ya consolidado entre los jóvenes de confiar en los servicios en línea y las plataformas digitales. Vemos que esto puede representar un aspecto negativo para el consumidor desde el punto de vista de la seguridad financiera.

En cuanto al sistema contra el lavado de dinero, la confianza entre los participantes es el elemento clave, diría yo, el factor que une a todos.

Sin confianza, el sistema no va a funcionar de manera eficiente. Son importantes los esfuerzos conjuntos sobre una base de asociación, donde cada participante esté dispuesto a compartir problemas y riesgos, y lo más importante, los métodos para reducirlos.

Hoy en día, tanto nuestro Servicio como los bancos, que constituyen la primera línea de defensa del sistema antilavado, reconocen el problema

de la implicación de los jóvenes en el sector sumergido.

Las acciones emprendidas contra las llamadas empresas técnicas y las «empresas fantasmas», que tradicionalmente participan en la retirada de fondos de la economía formal hacia el sector informal, han dado buenos resultados. Su número ha disminuido considerablemente debido a la drástica reducción de las posibilidades de realizar operaciones sospechosas. Sólo en 2023, los bancos rechazaron la realización de dichas operaciones por un valor aproximado de 400 mil millones de rublos.

Gracias a los esfuerzos de Rosfinmonitoring, de la Fiscalía y de otros organismos de supervisión, se logró reducir de manera significativa las posibilidades de retiro injustificado de efectivo utilizando mecanismos de débitos forzosos desde cuentas bancarias.

Un gran mérito de esto recae en las organizaciones de crédito, que fueron capaces de identificar los riesgos en la primera etapa de dichas operaciones e informar a Rosfinmonitoring. Se implementó un conjunto de medidas legislativas y de supervisión que prácticamente bloquean esos canales de financiación del sector sumergido. Sin embargo, en respuesta, surgieron nuevas estrategias, cuyos organizadores explotan de manera cínica la mentalidad de ciertos grupos de jóvenes.

Se ha popularizado un término que describe a estas personas: «mulas». Se trata, generalmente, de jóvenes de entre 16 y 25 años que, en la práctica, «trabajan» para los estafadores y se convierten en cómplices de esquemas delictivos, vendiendo su identidad digital para el simple reintegro de efectivo.

¿Qué caracteriza a esta categoría? En primer lugar, un pensamiento estereotipado, donde se difunde el «ejemplo exitoso» de un ingreso fácil e ilegal. En segundo lugar, la incapacidad de evaluar críticamente la situación y calcular los riesgos, lo que lleva a una implicación prolongada en la «infantería» del sector informal, cerrándoles posteriormente todas las posibilidades de acceder a servicios financieros normales. También influyen negativamente el entorno de migrantes ilegales y de personas que padecen diversos tipos de adicciones, desde las drogas hasta la ludopatía.

La propagación de esquemas más sofisticados desde el punto de vista tecnológico, dirigidos a la captación ilegal de fondos, con riesgo de su posterior uso no solo para el enriquecimiento personal de los delincuentes, sino también para el financiamiento del terrorismo y el extremismo, se enfoca principalmente en el público joven, que es mucho más experto en el uso del espacio digital.

Los defraudadores utilizan activamente plataformas de inversión digital de manera ilegal, similares a las pirámides financieras, que ofrecen inversiones en criptoactivos, monetización de contenido de audio y video bajo la apariencia de apoyo financiero a sus altas calificaciones, recaudación de donaciones mediante «donaciones» en juegos en línea y otros métodos similares.

Se hace evidente que los esquemas clásicos de lavado de dinero, en los que el movimiento de fondos a través de las cuentas en organizaciones de crédito pasa por las principales etapas de legalización, se disfrazan de contenido popular entre la audiencia joven.

Surge una pregunta legítima: ¿cómo contrarrestar estos fenómenos? ¿Cómo desarrollar una cautela razonable, en qué patrones

deben fijarse tanto los consumidores de servicios financieros como los departamentos de compliance de los bancos, Rosfinmonitoring y las autoridades de orden público?

Un diálogo confidencial entre todos los participantes del sistema, retroalimentación de los organismos estatales con las instituciones financieras, y de estas con sus clientes, orientada a aumentar la concienciación, a la capacidad de reconocer a tiempo los planes delictivos y a evitar los métodos de ingeniería social, se convierte en un requisito esencial para la lucha contra estos problemas.

No se trata de una acción puntual ni de una campaña esporádica, sino de un trabajo sistemático y regular en todos los niveles del sistema de antilavado. Este trabajo debe estar orientado a cada clase de la sociedad y para cada categoría de ciudadanos deben existir sus propios métodos de trabajo proactivo.

El movimiento internacional por la seguridad financiera, las lecciones de educación financiera, los talleres y la publicidad social, el Instituto Internacional de Redes en el ámbito de la prevención del lavado de dinero, el análisis de modelos situacionales y de incidentes en forma de juegos con la participación de los consumidores de servicios financieros, las discusiones públicas en redes sociales y otros formatos de sensibilización ya se están llevando a cabo con la participación no solo de destacados expertos de Rosfinmonitoring, de los reguladores y de la comunidad bancaria, sino también de consumidores de servicios financieros que muestran un gran interés.

Nuestra revista «Seguridad Financiera», también realiza su aporte a la misión educativa.

Invitamos a especialistas prácticos, psicólogos y expertos a participar activamente en la investigación de los problemas de la digitalización de la economía sumergida y de mecanismos prometedores para la reducción de riesgos.

COOPERACIÓN PÚBLICO-PRIVADA COMO FUNDAMENTO DE LA SEGURIDAD FINANCIERA

MAXAT SHAGDAROV,
Director del Departamento de Compliance de «Altyn Bank» S.A. (FB China CITIC Bank Corporation Limited)

REPÚBLICA DE KAZAJISTÁN: PAPEL DE LOS BANCOS EN EL ÁMBITO DE LA PLA/FT

Durante los últimos años Kazajstán trabaja activamente para el fortalecimiento de su legislación en el ámbito de la PLA/FT y la modernización de los mecanismos de control. Los organismos reguladores de Kazajistán siguen perfeccionando los requerimientos para las instituciones financieras

Los aspectos de la PLA/FT adquieren una especial importancia para los países con sistemas financieros en desarrollo, tales como Kazajistán. Durante los últimos años, Kazajistán trabaja activamente para el fortalecimiento de su legislación en el ámbito de la PLA/FT y la modernización de los mecanismos de control. Los organismos reguladores de Kazajistán, incluyendo el Banco Nacional y la Agencia para la Regulación y el Desarrollo del Mercado Financiero, continúan perfeccionando los requisitos para las instituciones financieras, endureciendo el control sobre el cumplimiento de estos requisitos. Se observa un importante aumento de la presión regulatoria en el ámbito de la PLA/FT. Esto se debe al incremento de los flujos financieros internacionales, al desarrollo activo de las tecnologías digitales y a las nuevas amenazas relacionadas con la ciberdelincuencia. En los países extranjeros, así como también en la República de Kazajistán se implementan activamente nuevas normas y estándares que exigen de las organizaciones financieras el perfeccionamiento de sus sistemas de PLA/FT.

Dado que la mayor parte de los flujos financieros se concentran en los bancos, estos desempeñan un papel clave en el mantenimiento de la estabilidad del sistema financiero y en la prevención de su uso con fines delictivos. Una de las principales tareas de los bancos al implementar medidas para la PLA/FT, es no solo identificar las operaciones sospechosas, sino también realizar un trabajo preventivo con los clientes y mejorar su educación financiera. En el contexto de la globalización de los mercados financieros y la creciente complejidad de los esquemas de legalización de ingresos ilícitos, estas medidas se vuelven cada vez más relevantes.

Teniendo en cuenta la digitalización y la automatización de los procesos bancarios, un aspecto importante

para la creación de un sistema PLA/FT eficiente es la inteligencia artificial y el aprendizaje automático, que pueden ayudar a eliminar el trabajo manual y disminuir el número de falsas alarmas. Los algoritmos se entrenan con datos reales y pueden detectar anomalías que son difíciles de identificar mediante métodos tradicionales. Esto reduce la carga de trabajo del personal de compliance y permite concentrarse en casos más complejos. La inteligencia artificial no solo puede identificar riesgos existentes, sino también prever amenazas potenciales, analizando grandes volúmenes de datos provenientes de diversas fuentes. Esto permite a las instituciones bancarias y otras organizaciones, anticiparse a posibles esquemas de lavado de dinero o financiamiento del terrorismo. La inteligencia artificial se convierte en una herramienta indispensable en la lucha contra los delitos financieros, proporcionando verificaciones más precisas y rápidas. Sin embargo, para una integración exitosa de estas tecnologías en el proceso de la PLA/FT, es necesario contar con el apoyo cualificado de especialistas en compliance y una actualización regular de los datos para el aprendizaje automático.

La base del sistema de la PLA/FT es el conocimiento del cliente (Know Your Customer). Sin embargo, además de la recopilación obligatoria de datos y el análisis de transacciones, los bancos pueden utilizar medidas preventivas de manera activa para minimizar los riesgos de que los clientes se involucren en esquemas de lavado de activos o financiamiento del terrorismo. Dichas medidas incluyen:

1. Monitoreo continuo de transacciones. Las tecnologías modernas permiten a los bancos monitorear las operaciones sospechosas en modo de tiempo real, lo que ofrece la posibilidad de reaccionar más rápido ante amenazas potenciales. El uso de algoritmos avanzados e inteligencia artificial ayuda a los bancos a identificar patrones anómalos en la conducta que pueden indicar actividad ilícita.

2. Análisis integral de riesgos. Los bancos deben evaluar los riesgos no solo en la etapa de apertura de la cuenta, sino también a lo largo de todo el período de servicio al cliente. Esto incluye la actualización regular de la información sobre el cliente, la realización de revisiones periódicas, así como el análisis de la actividad del cliente teniendo en cuenta los cambios en su negocio o situación financiera.

3. Asesoramiento a clientes. Un aspecto importante del trabajo preventivo es la formación de los clientes y la entrega de recomendaciones para cumplir con los requisitos de la PLA/FT. Los bancos pueden organizar seminarios, webinarios y talleres para sus clientes, explicándoles cómo gestionar su negocio de acuerdo con los requisitos legales y cómo evitar involucrarse en esquemas ilícitos.

4. Cooperación con organismos públicos. Los bancos deben interactuar activamente con las autoridades reguladoras y de seguridad, intercambiando información sobre operaciones sospechosas y desarrollando conjuntamente estrategias para combatir el LA/FT. Esta cooperación aumenta la eficacia del sistema nacional de la PLA/FT y contribuye a la creación de un entorno financiero seguro.

La educación financiera es un elemento clave en la lucha contra el lavado de dinero y la financiación del terrorismo. Los clientes bien informados tienden a cumplir con las normas legales y a entender las consecuencias de participar en operaciones financieras ilícitas.

LOS BANCOS PUEDEN AYUDAR A LA EDUCACIÓN FINANCIERA DE SUS CLIENTES DE LA SIGUIENTE MANERA:

- Creación de programas educativos. Los bancos pueden desarrollar e implementar programas dirigidos a enseñar a los clientes las bases del conocimiento financiero, incluyendo los aspectos de la PLA/FT. Estos programas pueden ser impartidos en forma de cursos online, aplicaciones móviles o materiales impresos accesibles tanto para personas físicas como también para clientes corporativos;

- Soporte informativo. Los bancos pueden ofrecer a sus clientes información actualizada sobre nuevos riesgos y amenazas en el ámbito de la PLA/FT. Estos pueden ser suscripciones regulares, publicaciones en redes sociales o sitios web oficialesy también en forma de eventos temáticos;

- Estimulación de la conducta responsable. Los bancos pueden introducir programas de fidelización que premian a los clientes por su conducta responsable y el cumplimiento de la legislación. Este tipo de programas pueden incluir bonos o descuentos en los servicios bancarios a clientes que participaron en la formación o que cumplen con altos estándares de informes financieros.

«Altyn Bank» S.A. está implementando activamente tecnologías modernas para combatir el lavado de activos y el financiamiento del terrorismo. Los elementos más importantes de esta estrategia son: la identificación biométrica, el establecimiento de criterios y escenarios para la detección de operaciones sospechosas, y el monitoreo de transacciones en tiempo real.

El banco utiliza tecnologías biométricas para confirmar la identidad de los clientes. Esto incluye el reconocimiento facial y la comparación con bases de datos gubernamentales de personas físicas, lo que minimiza los riesgos de fraude y falsificación de documentos. La identificación biométrica garantiza un alto nivel de seguridad en la apertura de cuentas a distancia y en la realización de operaciones, asegurando el cumplimiento de los requisitos legales.

«Altyn Bank», S.A. ha desarrollado un sistema de criterios para clasificar las operaciones, lo que permite identificar de manera efectiva acciones sospechosas. Estos escenarios y reglas se actualizan de acuerdo con los estándares internacionales y los requisitos nacionales, asegurando la conformidad con las tendencias y desafíos actuales en el ámbito de la PLA/FT.

Un aspecto fundamental del sistema PLA/FT es el monitoreo continuo de las transacciones. «Altyn Bank», S.A. utiliza plataformas analíticas avanzadas e inteligencia artificial para analizar las operaciones en tiempo real. Estas tecnologías permiten detectar transacciones anómalas y sospechosas, lo que garantiza la capacidad de reaccionar rápidamente y prevenir operaciones ilegales.

«Altyn Bank», S.A. aplica activamente tecnologías innovadoras para garantizar un alto nivel de protección contra los riesgos asociados con el lavado de dinero y el financiamiento del terrorismo, manteniendo así su reputación como un socio financiero confiable. Esto resalta el compromiso del banco con los estándares internacionales y el uso de soluciones avanzadas para mejorar la efectividad de los sistemas PLA/FT.

En las condiciones actuales, los bancos desempeñan un papel críticamente importante en la prevención del lavado de dinero y el financiamiento del terrorismo. Un trabajo preventivo efectivo con los clientes y el aumento de su alfabetización financiera son componentes esenciales de esta actividad. Los bancos que implementan activamente medidas preventivas y programas educativos contribuyen a la creación de un sistema financiero seguro y transparente, lo que en última instancia asegura el desarrollo sostenible de la economía y la sociedad en su conjunto.

«LA INTELIGENCIA ARTIFICIAL NO SOLO PUEDE IDENTIFICAR RIESGOS EXISTENTES, SINO TAMBIÉN PREVER AMENAZAS POTENCIALES, ANALIZANDO GRANDES VOLÚMENES DE DATOS PROVENIENTES DE DIVERSAS FUENTES. ESTO PERMITE A LAS INSTITUCIONES BANCARIAS Y OTRAS ORGANIZACIONES, ANTICIPARSE A POSIBLES ESQUEMAS DE LAVADO DE DINERO O FINANCIAMIENTO DEL TERRORISMO

UNA NUEVA ETAPA EN EL DESARROLLO DEL MONITOREO FINANCIERO COMO UNO DE LOS ELEMENTOS CLAVE PARA LA SEGURIDAD FINANCIERA DEL PAÍS: PUNTO DE VISTA DEL VTB

Los esfuerzos nacionales para garantizar la seguridad financiera y medidas similares en el sector bancario han quedado determinados en gran medida por una serie de factores completamente nuevos. Estos incluyen la transición masiva de productos y transacciones bancarias al entorno digital

ERKIN NOROV,
miembro del consejo de dirección, banco VTB (PAO)

El desarrollo sostenible de la economía de Rusia está estrechamente vinculado al aumento de la capacidad del sector financiero y, en particular, del sector bancario, cuyas tareas más importantes son garantizar el funcionamiento ininterrumpido del sistema nacional de pagos en tiempo real, así como el financiamiento de las empresas y la población en la amplia geografía de nuestro país. Estas funciones deben combinarse con el monitoreo constante de las transacciones con el objetivo de prevenir la expansión del sector informal y el uso ilegal de los fondos presupuestarios.

En los últimos 10 años, el sistema nacional de monitoreo financiero bajo el auspicio del Servicio Federal ha evolucionado significativamente, tanto en términos de la lista de operaciones de control obligatorio (el número de códigos de operaciones ha aumentado de 29 a 75 en diez años), como en la tipología de identificación de transacciones sospechosas. Cabe señalar que el regulador ha llevado a cabo depuraciones de indicios de operaciones sospechosas, excluyendo tipos que ya no son relevantes en las condiciones actuales, como las transferencias a cuentas anónimas, la circulación de cheques bancarios, etc. Esto ha tenido un impacto positivo en la carga de trabajo de los servicios de compliance de los bancos. A pesar de esto, la complejidad y el volumen de trabajo eran tales que llevaron a una necesidad objetiva de transformación tecnológica en este segmento regulatorio, que ya no podía funcionar en el antiguo modo manual o semiautomático con baja productividad del trabajo. Esta transformación no solo va acompañada de innovaciones tecnológicas y de gestión sistémicas, sino que también conduce a una interacción más estrecha entre los principales bancos y los principales órganos reguladores y de control, como Rosfinmonitoring y el Banco de Rusia. El banco VTB, como uno de los bancos más grandes del

país, está completamente involucrado en este trabajo de transformación y puede servir como un ejemplo para analizar lo que se ha hecho y evaluar lo que se debe hacer.

CAUSAS Y ELEMENTOS DE LA TRANSFORMACIÓN TECNOLÓGICA Y ADMINISTRATIVA

Hoy día los esfuerzos nacionales para garantizar la seguridad financiera y medidas similares en el sector bancario han comenzado a definirse en gran medida por una serie de factores completamente nuevos. Estos incluyen la transición masiva de productos y transacciones bancarias al entorno digital y al modo remoto, la formación de un amplio mercado de servicios de alto riesgo e ilegales en internet, el uso de criptomonedas. Es evidente que cada año la garantía de seguridad financiera se convierte en una tarea más compleja y de mayor envergadura, con un nuevo conjunto de requisitos para las tecnologías y las competencias profesionales.

Una condición ineludible para la actualización del modelo de monitoreo financiero es la transferencia de muchos productos y servicios al entorno digital y al formato de interacción remota con el cliente. Solo en los últimos tres años, VTB llevó a cabo la integración con el portal "Servicios públicos", proporcionando un servicio para personas físicas que permite la actualización remota de datos personales con solo presionar un botón, las personas pueden actualizar su información de identificación sin tener que acudir a la oficina del banco. Para los clientes de pequeñas y medianas empresas, el banco ha desarrollado un camino completamente remoto para la transición a los servicios de VTB, que elimina la necesidad de que las personas jurídicas y los emprendedores individuales acudan a las oficinas del banco para presentar información y documentos de identificación. Este método también se utilizó en el marco de la integración de los activos del banco «Otkritie» con VTB. Para las personas físicas, se ha hecho posible abrir una cuenta y acceder a los productos y servicios del banco sin visitar las sucursales, gracias al significativo desarrollo del servicio de mensajería del banco y al uso de la tecnología de firma digital de documentos del cliente a través de una aplicación móvil especial. Estas son solo algunas de las ilustraciones, que ya se han vuelto cotidianas, de un cambio a gran escala en el modelo de atención al cliente del banco, en el que se integran paralelamente mecanismos de control de compliance.

La respuesta adecuada al aumento de la magnitud del monitoreo financiero ha requerido la actualización regular de las tecnologías de recopilación, consolidación y análisis de la información, no solo de los sistemas de información del banco (que son más de 200), sino también de diversas fuentes externas. Se han implementado tanto soluciones de gestión, como la asignación de un equipo específico de especialistas en TI al departamento de compliance para apoyar y desarrollar a tiempo el proceso de negocio del monitoreo financiero, así como nuevas soluciones tecnológicas, como el uso de redes neuronales, elementos de inteligencia artificial y la robotización de funciones.

Como resultado, se ha construido y se está desarrollando continuamente un proceso de análisis efectivo, basado en nuevas soluciones de TI, con «asistentes» integrados en forma de elementos de inteligencia artificial y con una fuerte funcionalidad predictiva, que ha permitido cambiar cualitativamente, entre otras cosas, el enfoque para bloquear operaciones sospechosas, respondiendo de manera estricta a cualquier intento de involucrar al banco en su operación, y al mismo tiempo permitiendo que las operaciones legítimas pasen a través de los filtros, sin sobrecargar a los clientes con solicitudes excesivas. Estas medidas se conocen en el mercado, lo que reduce el interés por parte de los participantes en diversos esquemas de lavado de ingresos ilegales.

Una característica distintiva actual del control de compliance en VTB es su actividad proactiva, que va más allá de los requisitos formales de supervisión, y el desarrollo de contramedidas contra los esquemas fraudulentos en expansión en el espacio de internet. VTB fue uno de los primeros en establecer formatos que anteriormente no se aplicaban, como el rastreo de las actividades y flujos financieros de casinos en línea, casas de apuestas y puntos de intercambio de criptomonedas. Además, se implementó un monitoreo diario de la penetración de sitios de phishing en las transacciones comerciales, con su bloqueo operativo. Este proyecto permitió detener las operaciones de más de 4.000 organizadores de casas de cambio ilegales, casinos y más de un centenar de sitios de phishing; se identificaron y bloquearon alrededor de 1.000 clientes «mulas» el año pasado.

«SOLO EN LOS ÚLTIMOS TRES AÑOS, VTB HA LLEVADO A CABO LA INTEGRACIÓN CON EL PORTAL "SERVICIOS PÚBLICOS", PROPORCIONANDO UN SERVICIO PARA PERSONAS FÍSICAS QUE PERMITE LA ACTUALIZACIÓN REMOTA DE DATOS PERSONALES CON SOLO PRESIONAR UN BOTÓN, LAS PERSONAS PUEDEN ACTUALIZAR SU INFORMACIÓN DE IDENTIFICACIÓN SIN TENER QUE ACUDIR A LA OFICINA DEL BANCO

La complejidad del objeto de gestión se volvió tal que se requería una adecuada reingeniería de gestión, incluida la delegación de facultades y responsabilidades dentro de la unidad de compliance. Una parte de las tareas, tales como la metodología, digitalización, identificación de operaciones sospechosas y la presentación de informes, están completamente centralizadas en Moscú. Esto se debe tanto a la existencia en la organización central de una visión completa de lo que está ocurriendo, como a las competencias analíticas e informativas acumuladas durante años. Por otro lado, otra parte se ha delegado a las regiones, total o parcialmente; por ejemplo, el 70% de las operaciones obligatorias son identificadas por empleados regionales; el trabajo con solicitudes del Banco de Rusia y Rosfinmonitoring está completamente delegado a un Servicio ubicado en San Petersburgo. Actualmente, más del 50% de los empleados de la unidad de compliance están concentrados en las regiones, abarcando aproximadamente 1.300 puntos de venta en 79 regiones de Rusia. La delegación de una parte significativa de las tareas de monitoreo financiero a las sucursales se debe, entre otras cosas, a que los empleados de las filiales conocen mejor y entienden la especificidad de sus regiones, y a la ubicación de las oficinas de VTB en todos los husos horarios de Rusia, lo que permite tomar decisiones más rápidamente. Este tipo de delegación de facultades y responsabilidades no elimina el control adecuado sobre la calidad del trabajo desde la organización central.

La transformación gerencial fue necesaria también debido al aumento de las solicitudes operativas del Banco de Rusia y de Rosfinmonitoring. En 2018, el banco procesó 3.800 de estas solicitudes, mientras que en 2024 ya eran 8.700. Además, Rosfinmonitoring introdujo una categoría de solicitudes urgentes que deben ser respondidas en modo 24/7 dentro de 6 horas desde el momento de la solicitud, que se centran principalmente en el tratamiento de temáticas muy relevantes.

VTB estuvo orientado al principio a la realización de operaciones de actividad económica exterior en interés del Estado, por lo que una de las competencias específicas importantes del compliance en el ámbito de la seguridad financiera es la activa unificación de estándares y métodos de trabajo en el grupo en su conjunto, que integra más de 40 bancos y empresas financieras en 10 jurisdicciones extranjeras. La coordinación del trabajo de más de 200 oficiales de compliance en estas estructuras fortalece significativamente su potencial para cumplir con los riesgos regulatorios gracias al apoyo metodológico y gerencial de eficaces equipos de expertos de la empresa matriz en Moscú. Otro aspecto importante y fundamental del trabajo interno del grupo es el peritaje de compliance de los bancos que se planifica adquirir, y en caso de una decisión positiva, el acompañamiento de proyectos de integración de los activos financieros, con la necesaria conexión a los estándares de monitoreo financiero del VTB.

La componente analítica en la solución de tareas no triviales de compliance ha sido positivamente valorada también a nivel internacional. En 2022, en el marco del concurso del Grupo Euroasiático de lucha contra el Lavado de Activos y el financiamiento del terrorismo (EAG) a la mejor investigación financiera, el equipo de expertos del Banco VTB presentó ante el jurado un escenario complicado y no estándar de resolución, en el que se identificó y se detuvo la actividad de un casino online ilegal, disfrazado como una organización de microcréditos que realizaba pseudotransacciones de comercio electrónico por bienes digitales. Este ejemplo fue reconocido como la mejor investigación financiera entre las presentadas en el marco del concurso de EAG. En 2023, la investigación del equipo de oficiales de compliance del banco «Otkritie», tras la adquisición de este banco por parte de VTB, recibió una alta valoración en un concurso en China, donde esta investigación obtuvo el segundo premio. Considerando el desarrollo de la función de compliance, en 2023 y 2024, VTB realizó, a solicitud de Rosfinmonitoring dos seminarios de capacitación en el marco del programa «Nueva generación» para empleados de inteligencia financiera de los países de EAG, transmitiendo su experiencia acumulada de soluciones exitosas. También se debe destacar que el banco ha obtenido durante cuatro años consecutivos la máxima calificación de «AAA+++» en la evaluación anticorrupción del negocio ruso, realizada por la Unión Rusa de Industriales y Empresarios (URIE).

«EL BANCO HA OBTENIDO DURANTE CUATRO AÑOS CONSECUTIVOS LA MÁXIMA CALIFICACIÓN DE «AAA+++» EN LA EVALUACIÓN ANTICORRUPCIÓN DEL NEGOCIO RUSO, REALIZADA POR LA UNIÓN RUSA DE INDUSTRIALES Y EMPRESARIOS (URIE)

UNA NUEVA ETAPA DE INTERACCIÓN DEL VTB Y LOS REGULADORES FINANCIEROS REPRESENTADOS POR ROSFINMONITORING Y EL BANCO DE RUSIA

Además de la transición tecnológica, otra característica importante de la etapa post-evolutiva actual en el desarrollo de la supervisión financiera es el fortalecimiento de la interacción estrecha y sincronizada entre los reguladores y los bancos comerciales, lo que genera una sinergia en los mecanismos de control. El banco VTB participa regularmente en

proyectos piloto del Banco de Rusia y Rosfinmonitoring, enfocados en probar nuevos enfoques de regulación y en evaluar sus características tecnológicas.

El banco participa constantemente en el diálogo especializado durante la preparación de estos enfoques, apoyando la búsqueda de soluciones más efectivas para mejorar el control estatal y reforzar la seguridad financiera. Esta colaboración con la comunidad bancaria permite a los reguladores probar y ajustar las normas, y a los bancos, adaptar de manera proactiva sus mecanismos de supervisión a los cambios planificados, asegurando que, mediante soluciones digitales avanzadas, cumplan con los requisitos de un entorno regulador cambiante. Estas innovaciones importantes y en constante expansión por parte de los reguladores mejoran significativamente la coordinación y la eficacia en el ámbito de la seguridad financiera. Por ejemplo, actualmente se trabaja junto con los bancos en la implementación de herramientas unificadas que permitirán al regulador analizar las operaciones de los clientes de manera automatizada, lo cual reducirá las brechas entre las operaciones sospechosas y su correcta evaluación desde la perspectiva de riesgos.

Ya en 2021, VTB fue uno de los pocos bancos que respondió a la invitación del Banco Central de Rusia para pilotar la plataforma «Conozca a su cliente» (KYC), que ahora ha sido implementada con éxito. Se movilizó un amplio perfil de competencias profesionales de los oficiales de compliance del banco, y el análisis de escenarios de operaciones sospechosas propuesto por los especialistas de VTB, ayudó en muchos casos a eliminar plataformas y esquemas ilegales. Este trabajo en VTB se basa en las posibilidades proporcionadas por sus sistemas de información, las herramientas desarrolladas para procesar grandes volúmenes de datos, y la asignación específica de gerentes de TI para abordar las tareas de monitoreo financiero. La colaboración ha permitido mejorar significativamente la posición del banco en la reducción de la cantidad de clientes de alto riesgo: VTB ha logrado reducir, hasta la fecha, tanto el número total como la proporción de clientes de niveles medio y alto de riesgo en el volumen total de participantesde la plataforma KYC en un 12-13%.

CON LA IMPLEMENTACIÓN DE LA PLATAFORMA "KYC"

El Banco Central asumió ciertos riesgos que antes recaían sobre los bancos, y que, sin embargo, se compensaban con una mejora considerable en la eficacia de la seguridad financiera, gracias a la participación conjunta de la comunidad bancaria en la plataforma y bajo la supervisión diaria del Banco Central de Rusia. VTB al igual que otros bancos recibieron la oportunidad de:

- Evaluar el nivel de riesgo de las empresas que están siendo atendidas en otras organizaciones financieras; dicha información proporciona valiosos datos para la toma de decisiones al considerar la posibilidad de prestar servicios a una empresa que el banco aún no conoce, pero que ya ha sido evaluada por el Banco Central de Rusia.
- Identificar a clientes «dormidos», que aún no han mostrado actividades ilícitas en el banco, pero que ya han realizado operaciones sospechosas en otras organizaciones de crédito, lo cual ha sido detectado por el Banco Central de Rusia, quien ha informado a la comunidad bancaria; dichos clientes «dormidos» son bloqueados o se les somete a un control especial.

VTB está involucrado en el proyecto piloto del rublo digital, participando por segundo año en la iniciativa del Banco de Rusia para su implementación. En agosto de 2023, el banco se unió al grupo de 13 bancos que están probando operaciones con rublos digitales reales. Los empleados del compliance fueron de los primeros en abrir cuentas en rublos digitales y, a lo largo del año, realizaron las operaciones necesarias para las pruebas. Durante el piloto, se llevaron a cabo cientos de transacciones entre monederos digitales y transferencias en rublos digitales a entidades jurídicas para el pago de bienes y servicios, mientras se desarrollaban paralelamente procedimientos de control. La participación temprana en este proyecto permitió identificar posibles áreas de riesgo en las operaciones de los clientes con rublos digitales, y así preparar un modelo de sistema de monitoreo financiero para este segmento. De este modo, se ha establecido una base para los sistemas de TI del banco, en los cuales VTB podrá implementar los requisitos de identificación de clientes, evaluación de su nivel de riesgo de realización de operaciones sospechosas y análisis de pagos y transferencias cuando el rublo digital se despliegue a gran escala.

Otro proyecto de gran importancia de Rosfinmonitoring en el cual VTB participa desde el año 2022 es «Cadena de bloques transparente». El proyecto piloto persigue el objetivo de monitorizar y analizar operaciones con criptomonedas, incluyendo los sectores no trasparentes de Internet. En el año 2023 en el proyecto piloto, además de Rosfinmonitoring, BC de Rusia y VTB participaron 4 bancos rusos más. Los participantes desarrollaron una metodología conjunta, acordada con ambos reguladores; realizaron el análisis e identificaron un gran número de personas actualmente activas en este mercado, asignándoles los correspondientes niveles de riesgo. Además, iniciaron el intercambio

de experiencias acumuladas en la identificación de diferentes tipos de participantes del mercado de criptomonedas.

INTERACCIÓN EFICAZ ENTRE EL BANCO Y ROSFINMONITORING

En los últimos años, se ha incorporado toda una serie de proyectos piloto, tanto aquellos que ya se han implementado en la práctica como los que se realizarán en un futuro próximo:

- control de la integridad de las ventas de ingresos en divisa por los exportadores;
- control del uso previsto de los fondos estatales para pedidos relacionados con la defensa;
- control del uso previsto de fondos públicos y municipales designados a la lucha contra la pandemia;
- innovaciones en la lucha contra el financiamiento del terrorismo;
- innovaciones en el control del tráfico ilegal de drogas;
- otros proyectos piloto.

INTERACCIÓN EFICIENTE ENTRE LOS DEPARTAMENTOS DE COMPLIANCE Y DE NEGOCIOS PARA REDUCIR EL EXCESO DE REQUERIMIENTOS DE INFORMACIÓN CON EL OBJETIVO DE AUMENTAR LA CALIDAD Y LA COMODIDAD DEL SERVICIO

El enfoque fundamental de VTB es construir un posicionamiento adecuado de la función de compliance para apoyar el servicio al cliente, proporcionar una asesoría clara y precisa en la implementación de nuevos productos y servicios, mitigar los riesgos regulatorios y optimizar los requisitos de información para los clientes, trasladando la recolección de datos a un formato automatizado, incluso desde fuentes externas, lo que reduce la carga para los clientes.

De esta forma, actualmente el departamento de compliance actúa como un consultor activo y constante, enfocando sus esfuerzos no a la limitación, sino al apoyo del desarrollo de los negocios corporativos y de banca minorista del banco. Prácticamente a diario se brinda apoyo metodológico a las divisiones del banco, incluyendo la formulación de recomendaciones propias sobre las mejores opciones posibles para la implementación de productos, servicios y soluciones, manteniendo el equilibrio entre las exigencias regulatorias y los intereses de crecimiento del negocio.

Se han logrado resultados significativos con este modelo en diferentes áreas de negocios, incluida la verificación de clientes antes de la apertura de una cuenta. Por ejemplo, los clientes potenciales se evalúan de manera remota en cuanto a los riesgos de realizar operaciones sospechosas mediante un modelo de puntuación, que permite determinar la probabilidad de que los clientes realicen tales operaciones sin la intervención de empleados y sin que el nuevo cliente tenga que visitar una sucursal del banco. Utilizando herramientas de aprendizaje automático y simulación, el banco ha pasado a la implementación de un modelo predictivo que analiza más de 50 criterios de los clientes provenientes de diversas fuentes, detecta valores anómalos en el comportamiento operativo del cliente y determina riesgos potenciales. Gracias a la implementación de este enfoque, se ha logrado, en primer lugar, alcanzar un porcentaje de decisiones automáticas positivas del 90% al aceptar a personas jurídicas y empresarios individuales como clientes, y, en segundo lugar, reducir la carga para los clientes relacionada con la respuesta a solicitudes del banco y la presentación de diversos documentos de respaldo, al disminuir la cantidad de solicitudes y trasladar el proceso a un formato electrónico, lo que ha elevado significativamente el nivel de satisfacción del cliente y ha acortado los procesos de atención.

El banco ha implementado procedimientos similares para la recopilación automatizada de datos de clientes y su actualización, aliviando la carga para los clientes, lo que ha permitido simplificar los cuestionarios y eliminar solicitudes o comunicaciones adicionales con ellos. Así, por ejemplo, al combinar los formularios de cuestionario y las declaraciones de negocios, se han reducido significativamente los formularios que los clientes deben completar al solicitar tarjetas de nómina, lo que ha mejorado considerablemente la orientación al cliente y la velocidad del proceso. Para la evaluación de un nuevo cliente o la atención a uno existente, lo fundamental es el control de compliance al realizar la identificación y actualización de los datos del cliente. Estos procesos, en su mayoría, se han organizado de manera fluida e imperceptible, sin causar molestias a los clientes, y se han integrado en procesos mejorados.

«UTILIZANDO HERRAMIENTAS DE APRENDIZAJE AUTOMÁTICO Y SIMULACIÓN, EL BANCO HA PASADO A LA IMPLEMENTACIÓN DE UN MODELO PREDICTIVO QUE ANALIZA MÁS DE 50 CRITERIOS DE LOS CLIENTES PROVENIENTES DE DIVERSAS FUENTES, DETECTA VALORES ANÓMALOS EN EL COMPORTAMIENTO OPERATIVO DEL CLIENTE Y DETERMINA RIESGOS POTENCIALES

Otro ejemplo de la implementación de un control de compliance operativo en un nuevo producto y su rápido lanzamiento al mercado, cumpliendo plenamente con los requisitos regulatorios, son las transferencias transfronterizas de clientes minoristas a través del Sistema de Pagos Rápidos en la aplicación VTB Online.

Debido a la existencia de operaciones complejas y estructuradas en el banco, la consultoría de compliance es de gran importancia para el desarrollo de este tipo de negocio, asegurando el cumplimiento de una amplia gama de requisitos regulatorios.

RESULTADOS DE LOS CAMBIOS TRANSFORMACIONALES

Los cambios tecnológicos, metodológicos y de gestión descritos anteriormente, que están configurando un nuevo modelo de monitoreo financiero, han producido numerosos resultados específicos que reflejan la eficacia de estas innovaciones. Esto se evidencia en la experiencia de VTB:

1. Crecimiento acelerado de la productividad laboral. A pesar del aumento de la carga regulatoria (el número de mensajes enviados sobre operaciones, detalles de estas, solicitudes de los reguladores, etc.) en más de 30 veces, la cantidad de personal en el proceso de monitoreo financiero solo ha crecido 2,5 veces.
2. La transformación tecnológica ha mejorado la precisión y efectividad de los controles. En 2023, se logró reducir casi 20 veces el volumen de operaciones sospechosas de clientes en el Banco VTB en comparación con 2018. Esto representa un cambio cualitativo significativo a pesar del rápido crecimiento del balance y el número de operaciones de clientes. Otro indicativo de la efectividad de la digitalización de los procesos de monitoreo financiero es la disminución de la proporción de operaciones de clientes del banco dentro de la estructura nacional de operaciones sospechosas en más de 2,5 veces desde 2018, cuando el Banco de Rusia comenzó a publicar estos datos. Esto también se verifica con la evaluación independiente que el banco recibe de manera mensual.
3. En 2023, el volumen de operaciones sospechosas en términos monetarios en el sector bancario de la Federación Rusa se redujo en un 12% en comparación con 2022, mientras que en el Banco VTB la reducción fue del 27%.
4. La tasa de VTB en ciertas operaciones indeseadas del sistema bancario (retiro de efectivo, transferencias al extranjero, etc.) se redujo a un pequeño porcentaje, lo cual no es comparable con su peso relativo en la cantidad de clientes y el flujo de transacciones.
5. En 2023, se denegaron operaciones sospechosas desde cuentas de clientes del banco hacia sus contrapartes (es decir, hacia la economía del país en términos generales) por un monto total de alrededor de 132 mil millones de rublos, lo que refleja la contribución directa del banco a la limpieza del flujo financiero en el país.
6. Se incrementa constantemente la identificación de «ubicaciones virtuales» asociadas con casinos ilegales en línea, casas de apuestas y casas de cambio. Solo en 2023 se identificaron más de 6 mil de estas entidades y se suprimieron sus actividades.
7. Se establecieron controles específicos para el monitoreo de operaciones de clientes relacionadas con la implementación de subsidios estatales, la ejecución de contratos gubernamentales, contrasanciones de la Federación Rusa y resoluciones del Gobierno de la Federación Rusa.
8. Trimestralmente, VTB elabora y envía a Rosfinmonitoring nuevas tipologías y esquemas de actividades sospechosas de clientes, que son particularmente relevantes y representan un alto riesgo para su monitoreo y control.

Nuestros planes incluyen la continuación de la transformación digital de los procesos de monitoreo financiero en estrecha colaboración con Rosfinmonitoring y el Banco de Rusia.

EN MOSCÚ FUE SEDE DEL PROGRAMA «NUEVA GENERACIÓN 2024» CON LA PARTICIPACIÓN DE EMPLEADOS DE LOS SERVICIOS DE INTELIGENCIA FINANCIERA DE OCHO PAÍSES

En Moscú se llevó a cabo el programa «Nueva Generación 2024» enfocado al desarrollo de relaciones profesionales entre los jóvenes empleados de las unidades de inteligencia financiera de diferentes países

ESTE AÑO «NUEVA GENERACIÓN» UNIÓ A REPRESENTANTES DE 8 PAÍSES:

Azerbaiyán, Cuba, EAU, Egipto, Etiopía, India, Irán y Tailandia.

El programa se lleva a cabo por Rosfinmonitoring junto con Rossotrudnichestvo y el Centro Internacional de Capacitación y Métodos de Monitoreo Financiero (ITMCFM).

En el marco de la visita de cinco días los investigadores financieros visitaron el Banco de Rusia y VTB, el Servicio Federal de Impuestos y el ITMCFM. Los jóvenes especialistas participaron en mesas redondas, clases interactivas, simuladores de negocios y clases magistrales, incluyendo algunas con el empleo del sistema de formación «Graphus» (el sistema permite simular investigaciones financieras en tiempo real). Durante los eventos los participantes pudieron conocer las mejores prácticas de intercambio de información, aspectos de incremento del potencial de capital humano de los sistemas antilavado nacionales.

En los encuentros con empleados del Banco de Rusia y VTB, los representantes de las unidades de inteligencia financiera pudieron conocer el funcionamiento de la plataforma «Conozca a su cliente», con prácticas de prevención de la actividad ilícita en los mercados financieros, detección de riesgos de lavado de activos y financiamiento del terrorismo en el ámbito de divisas digitales. Además, los especialistas discutieron aspectos del análisis del grado de actividad de las transacciones de los clientes, detección de operaciones sospechosas, procedimientos de

«NUEVA GENERACIÓN 2024» NO ES SIMPLEMENTE UN INTERCAMBIO DE EXPERIENCIAS, ES EL NACIMIENTO DE UNA COMUNIDAD INTERNACIONAL DE JÓVENES ESPECIALISTAS UNIDOS POR UN OBJETIVO COMÚN: GARANTIZAR LA SEGURIDAD FINANCIERA

evaluación de riesgos y particularidades de la regulación del tráfico de criptomonedas.

En el Servicio Federal de Impuestos de Rusia, los representantes de la institución informaron a los invitados sobre los procesos de digitalización de los servicios públicos, ciertos aspectos de la administración tributaria y otros temas relevantes de la actividad.

Cada día de estancia en la capital finalizaba con eventos culturales: los participantes de «Nueva Generación 2024» visitaron la Exposición de los logros de la economía nacional (VDNJ), la Galería Tretyakov, la Plaza Roja, donde pusieron flores en la tumba del Soldado Desconocido en el jardín Alexandrovskiy.

MOSCÚ SE CONVIERTE EN UN CENTRO EXCLUSIVO DE COMUNICACIÓN E INTERCAMBIO DE EXPERIENCIAS INTERNACIONAL ENTRE EXPERTOS FINANCIEROS

«Nueva Generación» es un formato único de intercambio de experiencias, se podría decir, un intensivo de una semana que mejora las competencias profesionales de los empleados de las unidades de inteligencia financiera y los sumerge en el código cultural de Rusia. Rosfinmonitoring participa en este programa por segundo año consecutivo y muestra a los colegas soluciones avanzadas en el ámbito de la PLA/FT tanto en el sector público como en el privado. El trabajo de los departamentos de compliance de las instituciones financieras, al igual que el año pasado, fue demostrado por especialistas del grupo bancario VTB.

«Nueva Generación 2024» es un programa que ha reunido a más de 20 jóvenes especialistas de las unidades de inteligencia financiera de los países de la región Euroasiática, BRICS, Oriente Medio, Asia y África, sumergiéndolos en el sistema ruso de lucha contra el lavado de activos y el financiamiento del terrorismo.

«Es difícil de sobreestimar la utilidad del programa. Según confesaron algunos invitados, se enamoraron de la historia y la cultura de Rusia y prometieron regresar como turistas para disfrutar de las bellezas de Moscú, Sochi, San Petersburgo y otros rincones de nuestro país», destacó Maria Scherbakova, jefa del departamento de monitoreo de riesgos de los sujetos subordinados.

Comentarios de los participantes

REINO DE TAILANDIA

VEERAPORN SAMRITVIRIYAKUL,

INVESTIGADOR DE LA OFICINA DE PREVENCIÓN DEL LAVADO DE ACTIVOS DEL REINO DE TAILANDIA

Es mi primera visita a Rusia y estoy sinceramente agradecido por la posibilidad de unirme al programa «Nueva Generación». Valoro el conocimiento y la experiencia adquiridos gracias a este programa.

REPÚBLICA DE ETIOPÍA

SIMRET ANDARG KEBEDE,

ANALISTA SENIOR DEL SERVICIO DE INTELIGENCIA FINANCIERA DE LA REPÚBLICA DE ETIOPÍA

Vi lo maravillosa que es Moscú, especialmente sus lugares históricos. Aprendí mucho gracias a mi participación en diversos entrenamientos dedicados al sistema de administración tributaria y al trabajo de la unidad de inteligencia financiera de Rusia. Me encantaría tener la oportunidad de participar nuevamente en un programa como este.

EMIRATOS ÁRABE UNIDOS

MAHER ABDULLA MUBARAK ALAMUR ALKAABI,

ESPECIALISTA PRINCIPAL DE LA UNIDAD DE INTELIGENCIA FINANCIERA DE EAU

El papel de la cooperación internacional y la asistencia mutua en el ámbito de PLA/FT es muy importante. Rusia es uno de los países con los que cooperamos. Es un socio con el que siempre estamos contentos de trabajar, intercambiar y proporcionar información.

Visité Moscú y Rusia, por primera vez, y fue realmente impresionante. Participar en el programa «Nueva Generación 2024» fue una gran oportunidad para adquirir nuevos conocimientos. Además, fue una excelente oportunidad para conocer a colegas de otras unidades de inteligencia financiera.

La interacción entre los jóvenes profesionales es fundamental. Si garantizamos una buena preparación para la nueva generación, nos espera un gran futuro.

REPÚBLICA CUBA

LILIETT OTERO CAZO,

ANALISTA FINANCIERA DE LA UNIDAD DE INTELIGENCIA FINANCIERA DEL BANCO CENTRAL DE LA REPÚBLICA DE CUBA

Comencé a trabajar en el servicio de inteligencia financiera después de terminar mis estudios y me enamoré de este trabajo. Decidí quedarme porque me gusta ayudar al país y a su economía.

Me encantó Moscú, esta ciudad es muy hermosa. En cuanto al programa, me gusta porque nos permite compartir nuestra experiencia con colegas de todo el mundo, lo que nos brinda una visión más amplia del sistema de seguridad financiera.

Las relaciones entre las unidades de inteligencia financiera de Rusia y Cuba son excelentes. Tienen muchos sistemas modernos que nos proporcionan mucha información y conocimientos. Estamos impresionados con las tecnologías que utilizan y con la conexión que la inteligencia financiera de Rusia mantiene con todo el sistema financiero del país. También nos gustaría llegar a ese punto. Es un trabajo muy arduo, pero lo lograremos.

Conozco también el gran proyecto de la Olimpiada Internacional de seguridad financiera; la delegación de nuestro país participó en él. Creo que es muy importante poder compartir este tema con los jóvenes desde una edad temprana, desde el colegio o la escuela secundaria. No tuve la oportunidad de participar en las Olimpiadas, pero quizás si hubiera tenido esa oportunidad, mi preparación habría sido mejor y podría haber ayudado a mi país a alcanzar un mayor éxito. Me encantaría participar en las Olimpiadas, tal vez como mentor, ya que ya no estoy en edad para competir.

REPÚBLICA ISLÁMICA DE IRÁN

ZAHRA HAJPARAST NAZEM,

JURISTA DE LA UNIDAD DE INTELIGENCIA FINANCIERA DEL MINISTERIO DE ECONOMÍA Y FINANZAS DE IRÁN

¿Qué me inspiró a trabajar en la unidad de inteligencia financiera? Todos entendemos cómo el lavado de dinero puede afectar la economía de un país, a las personas y a su vida.

Por eso, para mí, como estudiante de la facultad de derecho, era importante tener la oportunidad de ayudarlos, compartir mis conocimientos en el ámbito de la PLA/FT. Sentía que podía ser una profesional eficaz en este campo.

Irán y Rusia son países casi vecinos. Estar en una misma región geográfica crea muchas cosas en común, como objetivos e intereses comunes, por lo que creo que con una estrecha cooperación realmente podemos resolver muchos problemas.

Gracias a la participación en el programa "Nueva Generación 2024", hemos demostrado que tenemos un gran potencial en el intercambio de datos.

Moscú es una ciudad muy bonita, y me gustó mucho estar aquí. Es mi primera vez en la capital rusa, y simplemente no puedo dejar de admirar las vistas y los edificios.

La visita a Rosfinmonitoring fue una experiencia inolvidable para mí. He visto cómo trabajan mis colegas en otro país y cómo funciona su sistema. Esto me ha proporcionado muchos nuevos conocimientos e ideas sobre cómo podemos prosperar en el ámbito de la PLA/FT y cómo podemos resolver nuestros desafíos, aprovechando la experiencia de Rosfinmonitoring.

REPÚBLICA DE LA INDIA

GAURAV SINGH,

SUBDIRECTOR DE LA UNIDAD DE INTELIGENCIA FINANCIERA DE LA REPÚBLICA DE LA INDIA

El programa «Nueva Generación» es maravilloso. Visitamos muchos lugares en Moscú y aprendimos mucho sobre delitos financieros, como el fraude con criptomonedas, el lavado de dinero, etc. Gracias a estas visitas y conferencias, conocimos cómo *Rosfinmonitoring* combate estos delitos financieros. Además, visitamos varias organizaciones y vimos cómo funcionan sus organismos estatales federales, cómo utilizan las tecnologías digitales.

Tuvimos la oportunidad de reunirnos con altos funcionarios de diversas agencias, lo cual, sin duda, enriqueció nuestro conocimiento. Nos esforzaremos por aplicar todo lo que aprendimos en esta conferencia en nuestro país y también recomendar a nuestros colegas que visiten Moscú para familiarizarse con la experiencia rusa en el ámbito de la PLA/FT.

Los empleados de *Rosfinmonitoring* nos hablaron sobre la Olimpiada internacional de seguridad financiera, que es algo realmente sorprendente. Felicitamos a los organizadores de este impresionante evento bajo los auspicios de *Rosfinmonitoring* y les deseamos lo mejor.

Las relaciones entre India y Rusia son muy importantes y beneficiosas, por lo que, si algo bueno sucede en Rusia, nos sentimos orgullosos y muy contentos. Espero que los representantes de la India también participen en esto (en la Olimpiada, nota Ed.).

Me gustaría destacar la importancia del intercambio de conocimientos y la cooperación internacional. Debemos organizar programas, seminarios y conferencias, incluso en formato virtual, donde podamos aprender unos de otros. Es necesario comprender cómo funcionan los sistemas financieros de otros países, ya que vivimos en un mundo globalizado.

REPÚBLICA ÁRABE DE EGIPTO

HESHAM HASSAN MOHAMED HUSSEIN,

ANALISTA FINANCIERO DE LA UNIDAD CONTRA EL LAVADO DE ACTIVOS Y EL FINANCIAMIENTO DEL TERRORISMO DEL BANCO NACIONAL DE EGIPTO

Un mes antes del viaje estaba trabajando en la oficina cuando se me acerco mi superior: «Hola, vas a viajar a Moscú el mes que viene», - me dijo. Pensé: «Vaya, voy a Moscú. Es un lugar estupendo. Escuché hablar de Moscú, pero nunca he estado allí». Esta es una ciudad asombrosa y seguro que volveré.

El programa «Nueva Generación 2024» superó todas mis expectativas. Inicialmente pensé que sería algo aburrido: más orientado a la teoría que a la práctica. Pero nada de eso. El programa está bien planificado y coordinado. Chicos, ustedes saben bien lo que están haciendo. Juntar a los participantes de diferentes países para un intercambio de experiencias es, sin duda, una idea perfecta.

La cooperación internacional en la lucha contra el lavado de dinero y la financiación del terrorismo es muy significativa, especialmente en lo que respecta a los delitos transfronterizos. Una cooperación internacional estrecha entre Egipto y Rusia, sin duda, beneficiará a ambas partes.

En lo referente a la juventud, es nuestro presente y futuro. Hay que invertir en la juventud, ya que los jóvenes representan nuestra vida. Los jóvenes realmente pueden cambiar nuestro mundo, ellos quieren aprender, tienen energía.

En Egipto, organizamos reuniones con estudiantes universitarios y los instruimos sobre temas de la PLA/FT, además de enseñarles a identificar a los estafadores y a no involucrarse en actividades relacionadas con el lavado de activos.

REPÚBLICA DE AZERBAIYÁN

AYSEL SHARIFOVA,

ESPECIALISTA PRINCIPAL DEL SERVICIO DE MONITOREO FINANCIERO DE LA REPÚBLICA DE AZERBAIYÁN

Considero que la inteligencia financiera tiene una gran responsabilidad en la lucha contra el crimen y el fraude. Pienso que la cooperación con cada país, incluyendo a Rusia, es importante para nuestro Servicio, ya que permite el intercambio de información y prácticas útiles.

Entre las prácticas interesantes para los jóvenes implementadas por nuestro Servicio, puedo mencionar el sitio web E-learning.fiu.az, así como los entrenamientos en línea impartidos por especialistas de diferentes departamentos. Al completar la formación, otorgamos un certificado a los participantes.

Moscú me encantó: es una ciudad cálida, soleada, vibrante y hermosa. Gracias a la participación en el programa, conocí a muchas personas de diferentes países que trabajan en el mismo campo que yo. Intercambiamos información útil.

PRESIDENTE DE LA ASOCIACIÓN DE BANCOS DE RUSIA

ANATOLII KOZLACHKOV:

LA TAREA DE AUMENTAR LA TRANSPARENCIA DEL ÁMBITO DE CRÉDITO Y FINANZAS ES DE TODOS

— Anatolii Anatolievich, la Asociación de Bancos de Rusia cumple una función importante en la búsqueda de un equilibrio entre los intereses del Estado y el sector bancario. En su opinión, ¿cómo se mantiene ese equilibrio actualmente en el ámbito de la seguridad financiera?

— Como usted sabe, el trabajo orientado a la modernización de los requisitos, mecanismos e instituciones del marco legislativo contra el lavado de dinero siempre ha sido una prioridad para la Asociación. Dentro de su estructura, se ha creado un Comité de Riesgos de Compliance y PLA/FT, que asegura la colaboración con la comunidad profesional, *Rosfinmonitoring* y el Banco de Rusia en toda la gama de temas relevantes, como la detección de actividades sospechosas de personas dirigidas al lavado de activos y el tráfico ilegal de drogas, la identificación de indicios de relaciones de corrupción, la lucha contra las actividades de participantes ilegales del mercado financiero, etc.

Se presta especial atención a las cuestiones de regulación, ya que la legislación contra el lavado de dinero es considerada una de las más dinámicas. Entendemos que el desarrollo constante de la base legislativa y normativa en este ámbito es una respuesta objetiva y, probablemente, la más adecuada a los cambios operativos en el panorama de riesgos. Todos comprenden que la tarea de aumentar la transparencia del ámbito de crédito y finanzas es de todos, y no solo el Estado tiene interés en ello. En respuesta a su pregunta, puedo decir con certeza que el equilibrio de intereses entre el Estado y la comunidad profesional se mantiene en la mayoría de las situaciones.

— ¿Qué aspectos trata el Comité de riesgos de Compliance y PLA/FT?

— En los últimos años, el Comité especializado de la Asociación ha centrado su atención en las siguientes áreas de trabajo principales: iniciativas legislativas, específicamente realizando el análisis de las normas legales y evaluando su aplicabilidad; formulación de propuestas para simplificar y mejorar la eficacia de los procesos de control; cumplimiento normativo de los requisitos anticorrupción y de sanciones, control de personas sancionadas, desarrollo de propuestas para mejorar el proceso de transmisión de información y la organización del flujo de documentos con *Rosfinmonitoring* y el Banco de Rusia. Al mismo tiempo, el Comité impulsa la difusión de las mejores prácticas en el mercado financiero con el objetivo de intercambiar experiencias en la implementación de diferentes tipos y mecanismos de control. Cabe destacar que el intercambio de experiencias para organizar diversos aspectos del control es una parte esencial del perfeccionamiento de los procedimientos de compliance, y planeamos continuar con esta práctica.

Por ejemplo, en una de las últimas reuniones del Comité se discutió la problemática del compliance anticorrupción, un tema muy relevante en la actualidad, en particular un análisis de los enfoques que utilizan los bancos para identificar señales de lavado de dinero proveniente de delitos de corrupción. Honestamente hablando, es una tarea nada sencilla. Al mismo tiempo, entendemos que los proveedores de servicios financieros pueden contribuir a la lucha contra la corrupción a nivel nacional. Finalmente, de ello depende la eficacia de la implementación de programas prioritarios para el desarrollo económico y social.

COOPERACIÓN PÚBLICO-PRIVADA COMO BASE DEL DESARROLLO DEL SISTEMA DE ANTILAVADO

En una entrevista para la revista «Seguridad Financiera», el jefe del Departamento de Organización de la Supervisión de Rosfinmonitoring, Alexandr Kurianov, la asesora principal en PLA/FT/FPADM del Secretariado del Grupo Euroasiático de Lucha contra el Lavado de Activos y el financiamiento del terrorismo (EAG), Nazerke Zhampeiis, y la secretaria del Consejo de Compliance y colaboradora de Rosfinmonitoring, Yana Bairachnaya, hablaron sobre los nuevos enfoques y herramientas de cooperación entre el sector bancario y las unidades de inteligencia financiera de distintos países. Los entrevistados destacaron el significativo potencial de la cooperación público-privada (CPP) para identificar y minimizar los riesgos de lavado de dinero y financiamiento del terrorismo

— Alexandr Mikhailovich, en los últimos tiempos se habla mucho de la cooperación público-privada en el ámbito de la lucha contra el lavado de dinero. En su opinión, ¿refleja este término de manera objetiva la naturaleza actual de la cooperación en este campo, o es más bien una visión idealizada?

— Si miramos a la historia reciente, vemos que la CPP comenzó a integrarse en la terminología antilavado en 2015-2016, cuando el GAFI organizaba foros con el sector privado para discutir, junto con los principales representantes del sector crediticio y financiero, los cambios en los estándares y documentos de orientación del Grupo.

En esencia, este formato es muy similar a la evaluación del impacto regulatorio. Al mismo tiempo, los países miembros de la red global del GAFI comenzaron a notar la utilidad de las consultas informales con los bancos sobre los temas de ROS y el intercambio de información sobre riesgos.

Sin duda, el término «cooperación» tiene una connotación positiva, pero cuando lo usamos, generalmente nos referimos a una cooperación comercial mutuamente beneficiosa. La experiencia sugiere que, en el ámbito de la lucha contra el lavado de dinero, una asociación verdaderamente efectiva se basa en otros principios, el principal de los cuales es la confianza. Creo que esta es, probablemente, la única base posible para establecer una comunicación sólida con los participantes del sistema.

Es muy importante que nuestros colegas del sector financiero también fortalezcan su comprensión de la importancia de las tareas que realizan en su área.

Los ejemplos están al alcance de la mano. Basta con observar los resultados del trabajo conjunto en

Alexandr Kurianov

Nazerke Zhampeiis

Yana Bairachnaya

temas presupuestarios durante la implementación del programa «Cinturón de Seguridad Financiera», iniciado hace dos años. Se pueden citar indicadores específicos, como el aumento del número de bancos que informan sobre riesgos en el ámbito de presupuesto público y los volúmenes de fondos públicos a los que se le ha bloqueado la entrada al mercado negro gracias a la aplicación de medidas preventivas. Los nuevos enfoques en el trabajo, que sin exagerar, han elevado a un nuevo nivel la labor de los bancos en la gestión de riesgos presupuestarios, se desarrollaron precisamente mediante una estrecha colaboración con expertos del sistema bancario. En especial me gustaría destacar en este sentido a los colegas de VTB, «Promsvyazbank», «Sberbank», «Alfa-Bank», «Gazprombank» y «T-Bank».

— ¿Podemos hablar de un cambio en la interacción entre Rosfinmonitoring y los bancos en los últimos años? Y si es así, ¿en qué se expresa este cambio?

— Creo que lo más importante que hemos logrado es un enfoque proactivo en nuestra colaboración. Muchos proyectos importantes se han llevado a cabo sin necesidad de establecer regulaciones especiales o lo que se conoce como "empujes administrativos", sino únicamente sobre la base de una cooperación voluntaria y asociativa. Por ejemplo, a partir de la información proporcionada por los bancos, se ha creado, podríamos decir, toda una biblioteca de tipologías, que la unidad de supervisión de la Agencia comunica sistemáticamente a todos los participantes del sistema.

Solo en los primeros ocho meses de este año, se ha recibido información sobre operaciones sospechosas y actividades de clientes vinculadas a estas tipologías por un monto superior a los 100 mil millones de rublos.

Hay también ejemplos de proyectos. A finales del año pasado, junto con los bancos, comenzamos a abordar el desarrollo de enfoques para el monitoreo de un área de riesgo como el tráfico ilegal de drogas. El crimen organizado demuestra un alto nivel de ingenio para ocultar sus actividades, incluyendo la infraestructura financiera que las sustenta. En estas condiciones, es fundamental actualizar constantemente los métodos y enfoques para su detección. El proyecto que hemos comenzado es multilateral. Esto incluye el desarrollo de un perfil de comportamiento financiero que pretende identificar signos transaccionales y conductuales característicos de ciertos actores del tráfico ilegal de drogas, como los «dealers» y los «ocultadores», entre otros.

Durante el proyecto, los colegas empezaron a comprender mejor los algoritmos de interacción de la Agencia con el bloque de seguridad y los parámetros que debe cumplir la información que nos proporcionan. Por iniciativa de los colegas, recibimos propuestas para proporcionar información sobre sitios en la *«darknet»* y canales temáticos en aplicaciones de mensajería que los delincuentes usan para la venta de drogas. Este tipo de datos se detectan mediante el análisis y monitoreo del entorno de internet realizado por las unidades de compliance de los bancos.

La información sobre estos canales de comunicación también ha sido utilizada en otros ámbitos de trabajo. Por ejemplo, el Banco de Rusia, basándose en información de Rosfinmonitoring, ha incluido en la lista de compañías con indicios de actividades ilegales en el mercado financiero a varios proyectos en línea que operan como esquemas piramidales. La información inicial fue proporcionada de manera proactiva por las organizaciones de crédito.

Ahora, con la experiencia adquirida, junto con el Banco de Rusia, planeamos modernizar los formatos de la presentación de reportes con la correspondiente ampliación de atributos.

— ¿Se prevé el desarrollo de proyectos interesantes iniciados conjuntamente con bancos también a nivel internacional?

— El desarrollo de la cooperación con nuestros socios de la EAG, la CEI y los BRICS a nivel de instituciones financieras se ha convertido en un elemento importante de la agenda internacional. Además del intercambio de experiencias y de la práctica de aplicar nuevos enfoques y soluciones tecnológicas en el compliance normativo, esto permite identificar con mayor precisión los puntos de convergencia y, de nuevo, aumentar el nivel de confianza mutua.

En abril de este año, en Nizhni Nóvgorod, se celebró un Foro Internacional Científico y Práctico sobre PLA/FT, que contó con la participación de numerosos expertos de las divisiones de compliance de los bancos. Los participantes del Foro confirmaron la naturaleza universal de los riesgos relacionados con la financiación del terrorismo, el tráfico ilegal de drogas y la corrupción, entre otros. Por ello, la configuración de los sistemas de monitoreo financiero y la cooperación con las unidades de inteligencia financiera sobre estos riesgos pueden considerarse temas prioritarios para la interacción de los bancos a nivel internacional. Proyectos de este tipo ya se están realizando en la línea del Grupo Euroasiático y el CJUIF.

— Nazerke Berikovna, en 2019, durante la sesión plenaria de la EAG, se tomó la decisión de crear el Consejo Internacional de Cumpliance. ¿Cuáles son actualmente las tareas que resuelve esta plataforma de interacción con el sector privado a nivel regional?

— El Consejo Internacional de Compliance (en adelante, CIC) fue creado para ampliar las posibilidades de diálogo con el sector privado a nivel internacional. Actualmente el CIC soluciona varias tareas clave entre las cuales se encuentran:

- el intercambio de experiencias y mejores prácticas en lo relacionado a la aplicación de medidas preventivas en el ámbito de PLA/FT por parte de instituciones financieras y entidades y profesiones no financieras establecidas;
- el establecimiento de una comunicación fluida entre representantes del sector privado, los órganos supervisores y las unidades de inteligencia financiera en el espacio de la EAG. Garantizar la retroalimentación y la participación del sector privado en la labor de identificar nuevos riesgos y mitigar los existentes, así como el desarrollo de tipologías actualizadas;
- la organización de la cooperación entre representantes del ámbito experto y profesional en el área de la PLA/FT, con el fin de identificar cuestiones estratégicas, temas de investigación y proyectos para su consideración en el marco de las actividades del CIC.

El CIC ofrece una oportunidad única para discutir problemas actuales de la asociación público-privada, la implementación de las últimas soluciones tecnológicas en el ámbito del compliance, así como el desarrollo de herramientas para monitorear el mercado de criptomonedas.

— Este año, con la participación de los miembros del CIC, se llevará a cabo la tercera edición del concurso del EAG al mejor ejemplo de análisis financiero. ¿Qué tan demandado considera este formato y qué beneficios ofrece a los participantes?

— El concurso del EAG al mejor ejemplo de análisis financiero se ha convertido en una iniciativa importante para las instituciones financieras. Este evento brinda a las organizaciones la oportunidad de intercambiar conocimientos y experiencias en la detección y prevención de esquemas de lavado de activos y financiamiento del terrorismo a nivel internacional.

El objetivo del concurso es fomentar la difusión de las mejores prácticas entre los profesionales de los países de la región Euroasiática, así como fortalecer la asociación público-privada en el ámbito de la PLA/FT. El concurso crea una plataforma para formar una biblioteca de los mejores ejemplos de identificación de esquemas de LA/FT, lo que contribuye al desarrollo del potencial de cooperación regional. Estos ejemplos también sirven como base para la formación y capacitación de especialistas en los sistemas nacionales de PLA/FT de los países miembros de la EAG.

Cada año, aumenta el número de instituciones financieras interesadas en participar en el concurso, lo que subraya la importancia y la demanda de este formato. Durante los años de su realización, se han presentado diversas tipologías de LA/FT, incluyendo el tráfico ilegal de drogas, delitos cibernéticos, fraudes fiscales, financiamiento del terrorismo, el uso de servicios de adquisición para actividades ilícitas, así como el lavado de dinero mediante activos virtuales, incluidas las criptomonedas.

El reconocimiento obtenido en el marco del concurso no solo mejora la reputación de las instituciones financieras, sino que también refuerza

«LOS NUEVOS ENFOQUES EN EL TRABAJO, QUE SIN EXAGERAR, HAN ELEVADO A UN NUEVO NIVEL LA LABOR DE LOS BANCOS EN LA GESTIÓN DE RIESGOS PRESUPUESTARIOS, SE DESARROLLARON PRECISAMENTE MEDIANTE UNA ESTRECHA COLABORACIÓN CON EXPERTOS DEL SISTEMA BANCARIO

el estatus internacional del país que representa a la organización ganadora. Este concurso no es solo una evaluación de los esfuerzos en el área del análisis financiero, sino también un reconocimiento a nivel internacional de la importancia del trabajo en la lucha contra los delitos financieros.

— Cuente, por favor, sobre los nuevos proyectos del CIC.

— La experiencia de trabajo de los órganos supervisores y del sector privado de los estados miembros del EAG en el ámbito de la lucha contra el lavado de dinero demuestra un significativo potencial en las asociaciones público-privadas. Esta colaboración se ha consolidado como un mecanismo eficaz para el intercambio rápido de información sobre riesgos, el aumento de la concienciación sobre esquemas actuales de blanqueo de capitales y financiación del terrorismo, así como para mejorar la interacción entre los principales actores en este ámbito.

Además de organizar el Concurso entre representantes del Consejo Internacional de Compliance, realizamos foros conjuntos con los órganos supervisores. Estos eventos desempeñan un papel importante en la promoción del enfoque basado en el riesgo, que es una de las prioridades del EAG.

La cooperación entre los órganos supervisores y el sector privado revela un gran potencial para el desarrollo futuro. Los formatos de esta colaboración ayudan a fortalecer el sistema de la PLA/FT, lo que permitirá una respuesta aún más rápida a las nuevas amenazas y riesgos emergentes.

— Yana Dmitrievna, el Consejoj de Compliance fue creado hace más de 8 años. ¿Cómo ha cambiado en este tiempo la composición de los participantes y el formato de interacción?

— El Consejo de Compliance, igual que antes, une a los jefes de las unidades de la PLA/FT de los bancos más grandes de Rusia.

Sin embargo el formato de interacción durante estos años se transformó. También se ha ampliado la lista de temas sobre los que se realizan comunicaciones. A menudo se escucha que el Consejo es un claro ejemplo de asociación público-privada, pero al mismo tiempo, sin exagerar, es también un modelo de enfoque basado en proyectos en el ámbito de la PLA/FT. Un ejemplo destacado en este caso es el trabajo conjunto con los colegas en la creación de perfiles de comportamiento financiero.

— Usted mencionó que el Consejo trabaja en diversas temáticas. ¿Cuáles de ellas son prioritarias para el Servicio y sistema antilavado?

— Probablemente, la más importante es la relacionada con el desarrollo de formatos de interacción informativa. Los bancos son los principales proveedores de datos, sobre la base de los cuales se inician investigaciones financieras y son la base para el macroanálisis. En este contexto, se lleva a cabo un trabajo conjunto continuo para optimizar los parámetros de dicha interacción. En este sentido, se pueden destacar tanto elementos estratégicos de este trabajo, como la implementación de enfoques y herramientas completamente nuevos, tales como el formato de información sobre actividades sospechosas de los clientes, el extracto unificado de cuentas de clientes, la metodología de criptocompliance, entre otros; así como elementos de carácter táctico, como por ejemplo, cuando, a partir de la evaluación de la situación operativa y la detección de nuevos esquemas de operaciones financieras ilegales, se inicia un monitoreo conjunto temático según ciertos criterios, entre otros.

Entre las nuevas áreas de trabajo del Consejo de Compliance, cabe destacar las actividades educativas sobre seguridad financiera que comenzaron a realizarse este año junto con expertos de los bancos. Los miembros del Consejo respondieron positivamente a nuestra iniciativa. Uno de los temas prioritarios de estas actividades es la problemática de la participación de los jóvenes en esquemas ilícitos y el combate a fenómenos como las «mulas de dinero». Más de 30 bancos demostraron así su responsabilidad social y delegaron a expertos para trabajar conjuntamente en este formato dentro del movimiento por la seguridad financiera.

— ¿Está prevista la participación de los miembros del Consejo de Compliance en la Olimpiada Internacional de seguridad financiera?

— Sí, tradicionalmente los expertos de las instituciones financieras establecen la agenda principal de la Olimpiada: paneles de discusión y talleres sobre los temas más interesantes y relevantes. La cuarta Olimpiada no será una excepción. Se planifican debates sobre nuevas soluciones tecnológicas utilizadas en los sistemas de compliance de los bancos, incluyendo inteligencia artificial y métodos de análisis de redes (grafos). Otro tema es la problemática de la participación de los jóvenes en actividades ilícitas, y en este caso hablamos del pensamiento crítico como un factor clave para prevenirlo. También son interesantes las iniciativas de algunos bancos que ven a los jóvenes como proveedores de conocimientos sobre seguridad financiera para las generaciones mayores. Esto es especialmente relevante en situaciones donde se utilizan nuevas tecnologías financieras en actividades ilegales y fraudes.

Participantes del concurso entre especialistas en compliance de entidades financieras de los Estados miembros del EAG

REPÚBLICA DE LA INDIA

SUSARLA RAMAKRISHNA,

EX DIRECTOR GENERAL DEL DEPARTAMENTO DE PLA/FT DEL BANCO ESTATAL DE LA INDIA, LAUREADO DEL 2.º CONCURSO DEL EAG ENTRE INSTITUCIONES FINANCIERAS

El concurso para los Estados miembros del EAG es una iniciativa sumamente importante, dirigida a destacar las mejores prácticas de las instituciones financieras y los participantes del sistema de la PLA/FT de los países miembros, así como a identificar los modelos de delitos prevalentes en diversas regiones geográficas y las investigaciones de calidad que llevan a cabo los especialistas en PBC dentro de las jurisdicciones correspondientes.

Además de la formación, los participantes disfrutaron de la oportunidad de presentarse en un escenario prestigioso. Los organizadores abordaron la realización del concurso con gran profesionalismo, haciendo que el evento fuera dinámico e interesante. Pido al EAG que no solo continúe organizando este evento anualmente, sino que también haga esfuerzos para atraer a un mayor número de participantes (solicitudes de participación) y premios, lo que, sin duda, aumentará la relevancia del evento.

Les deseo a los organizadores todo lo mejor.

REPÚBLICA DE KAZAJISTÁN

AITMUKHAMBET NURADIL DINMUKHAMEDULI,

JEFE DEL DEPARTAMENTO DE COMPLIANCE, JEFE DEL SERVICIO DE PLA/FT DE LA EMPRESA «ADVANCED PAYMENT SOLUTIONS», LAUREADO DEL 2.º CONCURSO DEL EAG ENTRE INSTITUCIONES FINANCIERAS

El concurso del EAG entre especialistas en compliance y la participación activa en el Consejo Internacional de Compliance no solo ofrecen la oportunidad de mostrar logros en el ámbito de la PLA/FT, sino también una plataforma única para fortalecer la colaboración entre las autoridades estatales y el sector privado. En un contexto de amenazas y riesgos en constante cambio, estos formatos de interacción se vuelven fundamentales para el funcionamiento exitoso de todo el sistema de la PLA/FT. Los seminarios y consultas bajo los auspicios del EAG no solo facilitan una comprensión más profunda de los estándares internacionales del GAFI, sino que también ayudan a desarrollar soluciones conjuntas dirigidas a minimizar los riesgos. Es importante señalar que iniciativas como estas crean un espacio para el intercambio de experiencias y mejores prácticas, lo que permite responder de manera más eficaz a los desafíos que enfrentan las instituciones financieras y las entidades no financieras.

REPÚBLICA POPULAR CHINA

DI LI,

GERENTE DE LUCHA CONTRA EL LAVADO DE DINERO EN ALIPAY, MIEMBRO DEL EQUIPO GANADOR DEL PRIMER CONCURSO DEL EAG ENTRE INSTITUCIONES FINANCIERAS

El concurso de la EAG se ha convertido en una plataforma transformadora, no solo para el reconocimiento de talentos excepcionales en el análisis de compliance financiero, sino también para la promoción de innovaciones y mejores prácticas en nuestro campo.

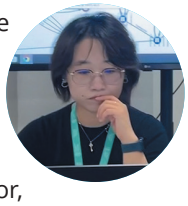
El concurso ha servido de estímulo para que los profesionales desafíen los enfoques tradicionales, exploren nuevas metodologías y compartan prácticas avanzadas que mejoren la efectividad de nuestras estrategias en el área de la PLA/FT. Mirando hacia el futuro, me alegra la perspectiva de continuar la colaboración y el potencial de iniciativas innovadoras que surgirán de nuestros esfuerzos conjuntos. Estoy dispuesta a contribuir a estos esfuerzos, en una búsqueda constante de perfeccionamiento de las políticas de compliance.

REPÚBLICA POPULAR CHINA

SHUHAN YUAN,

GERENTE DE LUCHA CONTRA EL LAVADO DE DINERO EN ALIPAY, MIEMBRO DEL EQUIPO GANADOR DEL PRIMER CONCURSO EAG ENTRE INSTITUCIONES FINANCIERAS

El concurso «Mejor Análisis Financiero», organizado por el EAG, ofrece una excelente oportunidad para



compartir experiencias, permitiendo que las instituciones de diferentes países conozcan las mejores prácticas nacionales en la lucha contra el lavado de dinero. Este evento amplía las perspectivas y fomenta un pensamiento innovador, facilitando así la cooperación e interacción internacional en el ámbito de la PLA entre instituciones.

Gracias a este concurso, las organizaciones financieras globales tienen la oportunidad de estudiar y adoptar experiencias y enfoques avanzados en la lucha contra los delitos financieros, asegurando la integridad del sistema financiero. Esto mejora considerablemente la coordinación y la comunicación transfronterizas en la labor de prevención del lavado de dinero, aumentando el potencial y la efectividad global en la lucha contra la legitimación de capitales ilícitos.

REPÚBLICA POPULAR CHINA

YUANYUAN WANG,

GERENTE DE LUCHA CONTRA EL LAVADO DE DINERO EN ALIPAY, MIEMBRO DEL EQUIPO GANADOR DEL PRIMER CONCURSO EAG ENTRE INSTITUCIONES FINANCIERAS

La participación en el concurso de la EAG fue una experiencia inspiradora. El concurso se convirtió en una valiosa plataforma para que las instituciones financieras intercambien ideas interesantes y conocimientos sobre el monitoreo de transacciones sospechosas y las prácticas nacionales de aplicación del servicio «Conozca a su cliente». Los conocimientos y la experiencia adquiridos en esta competencia nos han motivado enormemente. Ahora esperamos con ansias la oportunidad de participar en el tercer concurso del EAG entre instituciones financieras.

REPÚBLICA POPULAR CHINA

LIUMIN ZHOU,

GERENTE SENIOR DE LUCHA CONTRA EL LAVADO DE DINERO EN ALIPAY, MIEMBRO DEL EQUIPO GANADOR DEL PRIMER CONCURSO DEL EAG ENTRE INSTITUCIONES FINANCIERAS

El concurso del EAG y el Consejo Internacional de Compliance nos ofrecieron una valiosa oportunidad para mostrar nuestros logros profesionales y aprender de la experiencia de otros. Gracias a estas plataformas, nos convencimos aún más de que la colaboración y el intercambio de conocimientos son fundamentales para identificar y resolver de manera más efectiva los complejos problemas de la seguridad financiera. Estoy deseoso de continuar colaborando con nuestros colegas en el futuro, para contribuir a la seguridad y estabilidad del sistema financiero.

REPÚBLICA POPULAR CHINA

XIAOJÜAN XUE,

GERENTE DE LUCHA CONTRA EL LAVADO DE DINERO EN ALIPAY, GANADOR DEL CONCURSO AL MEJOR CASO (CONSEJO INTERNACIONAL DE COMPLIANCE, 2023)

La participación en el Consejo Internacional de Compliance fue una experiencia enriquecedora que nos brindó una oportunidad única de interactuar con una comunidad diversa de expertos en compliance. La atmósfera de cooperación en el consejo facilitó la formación de una postura más cohesionada y activa frente al cambiante panorama de amenazas a la seguridad financiera.

FEDERACIÓN RUSA

SHAIKHUTDINOVA AIDA RINATOVNA

AK BARS BANK

El concurso del EAG es un formato único que permite a los bancos intercambiar conocimientos y experiencias en el ámbito del monitoreo financiero y los procedimientos de compliance.

A mi parecer, el concurso también cumple una tarea importante: la promoción de la profesión de especialista en seguridad financiera. Los participantes de la Olimpiada pueden ver, a través de ejemplos prácticos, lo interesante que puede ser este campo profesional. En esencia, el profesional moderno en esta área debe tener conocimientos de economía, tecnología de la información, derecho, y comprender la especificidad sectorial de sus clientes.

INTERACCIÓN ENTRE LOS ORGANISMOS PÚBLICOS DE LA REPÚBLICA DE TAYIKISTÁN EN EL ÁMBITO DE LA PLA/FT

KHALIM MIRZOALIEV,
Director del Departamento de Monitoreo Financiero del Banco Nacional de Tayikistán

El terrorismo internacional es hoy en día una de las principales amenazas para la comunidad mundial. Una de las formas más efectivas de combatir este mal es cortar las vías de financiamiento de las organizaciones terroristas. De hecho, cualquier organización terrorista necesita financiamiento, y ningún acto terrorista puede llevarse a cabo sin medios. La comunidad internacional trabaja activamente en la limitación de las actividades terroristas, incluyendo el bloqueo de posibles flujos financieros

Las tecnologías modernas y el rápido desarrollo del mercado financiero global han creado nuevas oportunidades para el financiamiento de actividades terroristas. La comunidad internacional se enfrenta a nuevas fuentes y mecanismos de transferencia de dinero fuera del control de las instituciones nacionales e internacionales. En primer lugar se trata del uso de criptomonedas.

La República de Tayikistán, como país con una larga historia de lucha contra el terrorismo y el extremismo, está desarrollando e implementando activamente medidas para contrarrestar estas amenazas. mediante la cooperación con sus socios internacionales, los órganos estatales juegan un papel clave en este proceso para garantizar la seguridad nacional y global.

Ya en los primeros años de su independencia, la República de Tayikistán se enfrentó a amplios intentos de imponer al pueblo ideas y visiones extremistas y ajenas. Como resultado de la guerra civil, según datos oficiales, miles de personas perdieron la vida, y el daño material al país superó los 10 mil millones de dólares estadounidenses.

En el periodo posterior, Tayikistán continuó con los principios fundamentales y las tradiciones de su política exterior, abordando tareas prioritarias para el desarrollo del país, especialmente en la consolidación de la paz y la concordia nacional, y el fortalecimiento de las

reformas políticas, económicas y sociales. La República de Tayikistán ha consolidado su posición en la arena internacional, contribuyendo a la resolución de problemas globales, estableciendo relaciones con numerosos países y manteniendo un equilibrio entre sus intereses nacionales y los intereses globales en su política exterior.

En la República de Tayikistán, las fuerzas de seguridad, junto con otros órganos estatales, colaboran activamente en el intercambio de información, la coordinación de acciones operativas y la realización de operaciones especiales para la detención y neutralización de extremistas y terroristas.

La unidad de inteligencia financiera del país, el Departamento de Monitoreo Financiero del Banco Nacional de Tayikistán (DMF), actúa como centro nacional para la recopilación y análisis de reportes de operaciones sospechosas (ROS), así como de otra información relacionada con el lavado de activos, delitos subyacentes y financiamiento del terrorismo. Este departamento transmite los resultados de sus análisis a los órganos competentes, ya sea por solicitud o de forma proactiva.

EL DMF REALIZA

la regulación y supervisión de los sujetos subordinados en cuanto al cumplimiento de la legislación en materia de lucha contra el blanqueo (lavado) de activos procedentes de actividades delictivas, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva (PLA/FT/FPADM).

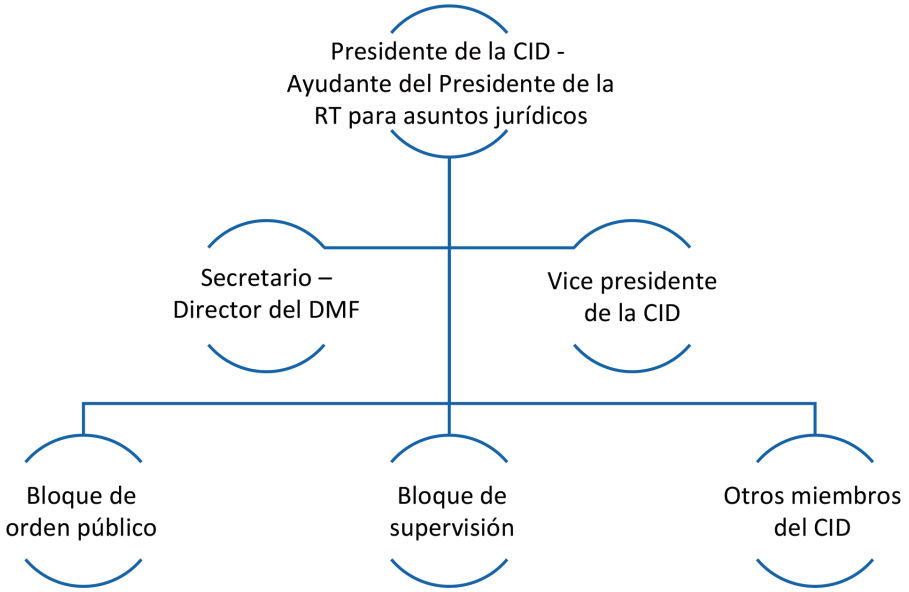
Durante los años de funcionamiento de la estrategia nacional de PLA/FT/FPADM de nuestro país, se

han logrado resultados significativos, como el perfeccionamiento del marco legal y la legislación del país, el fortalecimiento de la capacidad del personal de los organismos públicos y del sector privado que son participantes del sistema PLA/FT/FPADM, la cooperación internacional fructífera, y la implementación de estándares internacionales, entre otros.

Tayikistán comprende estas amenazas globales y hace esfuerzos importantes para luchar contra el terrorismo y el tráfico ilícito de drogas durante muchos años; esto incluye la aprobación de Estrategias nacionales para la prevención del extremismo y terrorismo en la República de Tayikistán 2021-2025 y para el control de drogas en la República de Tayikistán 2021-2030, así como también del concepto nacional de la lucha contra el blanqueo (lavado) de activos procedentes de actividades delictivas, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva 2018-2025.

Además, la República de Tayikistán, como miembro pleno del Grupo Euroasiático de lucha contra el lavado de activos y el financiamiento del terrorismo (EAG), ha incorporado las 40 Recomendaciones del GAFI en su normativa legal. En 2018, Tayikistán pasó por la segunda ronda de evaluaciones mutuas, en la que expertos de otros países evaluaron el sistema de lucha contra el lavado de dinero y la financiación del terrorismo del país. Esta evaluación permitió identificar las ventajas y debilidades del sistema nacional PLA/FT/FPADM, y tomar medidas para corregir las deficiencias detectadas.

El gobierno de Tayikistán hace un llamado a la comunidad mundial para eliminar los factores de apoyo político, militar y financiero al terrorismo internacional, tomando medidas integrales para prevenir



la implicación de los ciudadanos en grupos terroristas y extremistas.

Con el fin de coordinar las actividades de los órganos estatales de Tayikistán y armonizar sus acciones en la lucha contra el blanqueo (lavado) de activos procedentes de actividades delictivas y el financiamiento del terrorismo, se creó una comisión interinstitucional permanente mediante el decreto del gobierno del 4 de octubre de 2013.

Asimismo, para identificar y prevenir riesgos en el área de la PLA/FT y fortalecer el sistema nacional, el Departamento de Monitoreo Financiero del Banco Nacional de Tayikistán, junto con los organismos correspondientes de la República de Tayikistán realizó una evaluación nacional de riesgos, destinada a cumplir con los requisitos de la Recomendación 1 del GAFI. Este informe de evaluación fue aprobado por los miembros de la comisión interdepartamental en 2017.

Tayikistán coopera activamente con otros países, organizaciones internacionales y alianzas en la lucha contra el terrorismo y el extremismo. La colaboración dentro del Grupo Euroasiático de lucha contra el lavado de activos y el financiamiento del terrorismo, la Organización de Cooperación de Shanghái, la Organización de Lucha contra el Crimen, entre otras estructuras, favorece el intercambio de experiencias, la transmisión de información sobre posibles amenazas y la realización de operaciones conjuntas para la contención de la actividad terrorista.

Las autoridades estatales de Tayikistán participan activamente en conferencias internacionales, seminarios y entrenamientos destinados a mejorar la cooperación en la prevención de actos terroristas y la radicalización de la población.

La cooperación de los órganos estatales en la lucha contra el terrorismo y el extremismo en Tayikistán es un requisito indispensable para asegurar la estabilidad y seguridad en la región. Gracias a los esfuerzos conjuntos y la coordinación de diversas agencias, el país ha logrado ciertos éxitos en la prevención de amenazas y la protección de los intereses de sus ciudadanos. La mejora continua de las medidas para combatir el terrorismo y el extremismo sigue siendo un enfoque esencial para las autoridades estatales, con el objetivo de garantizar el desarrollo estable de la sociedad.

« GRACIAS A LOS ESFUERZOS CONJUNTOS Y LA COORDINACIÓN DE DIVERSAS AGENCIAS, EL PAÍS HA LOGRADO CIERTOS ÉXITOS EN LA PREVENCIÓN DE AMENAZAS Y LA PROTECCIÓN DE LOS INTERESES DE SUS CIUDADANOS.

EL CONCURSO DE ANALISTAS COMO MÉTODO DE DESARROLLO DEL PERITAJE DE LAS UNIDADES DE MONITOREO FINANCIERO

La eficiencia y efectividad del trabajo de un departamento moderno de monitoreo financiero de una organización de crédito depende en gran medida de la rapidez y precisión con la que su equipo analítico identifica a los clientes de alto riesgo que intentan utilizar los servicios bancarios para actividades ilegales. En esencia, estos factores son clave para el éxito de la gestión del riesgo de lavado de activos por parte de la organización de crédito en sus operaciones diarias

MIKHAIL PRONIN,
eVicepresidente, director del Departamento de Monitoreo Funanciero del Banco PSB, candidato a doctor en Ciencias Económicas

Para desarrollar las competencias de los analistas expertos, las organizaciones de crédito utilizan en la práctica diversas herramientas: la actualización sistemática de los empleados con materiales metodológicos del Banco de Rusia y Rosfinmonitoring, cursos de formación programados y especializados con posterior evaluación de conocimientos, y el sistema de mentores, en el cual un analista experto ayuda a los principiantes a desarrollar las habilidades analíticas necesarias para realizar su trabajo con la calidad necesaria.

Todos estos enfoques suelen dar buenos resultados al inicio, pero cuando se usan de forma continua, tienden a volverse rutinarios y su efectividad disminuye. En este sentido, el trabajo del equipo analítico del Departamento de Monitoreo Financiero del Banco PSB no es una excepción, y nos enfrentamos a las mismas dificultades en el desarrollo de la experiencia del equipo que nuestros colegas.

A mediados de 2023, en un momento en que el trabajo se estaba volviendo cada vez más una repetición rutinaria convencional, relevando cada vez menos de esa «magia» del análisis que lleva a muchos a elegir la profesión de analista de monitoreo financiero, nos surgió la idea de organizar un concurso para analistas.

▲ Ganadores del segundo concurso por equipos

Desde agosto hasta noviembre del 2023 celebramos el primer concurso individual de analistas. Cualquier analista sin exclusión podía participar en el concurso. El objetivo del certamen consistía en detectar y bloquear clientes sospechosos con riesgos de blanqueo de ingresos ilícitos.

Podría parecer que, en estas condiciones, existe el riesgo de una interpretación excesivamente amplia de la sospecha y que podrían tomarse medidas injustificadas contra clientes honestos. Por supuesto, confiamos en el alto nivel de ética de nuestros analistas, pero también establecimos una medida adicional en el concurso: si un cliente identificado durante el concurso resultaba ser rehabilitado tras una apelación, el analista recibiría una penalización doble en puntos.

Y a la inversa, se otorgaban puntos positivos dobles si el cliente sospechoso identificado durante el concurso posteriormente era clasificado de alto riesgo por el Banco de Rusia en la plataforma «Conozca a su cliente».

Para equilibrar el trabajo regular de los analistas con una participación eficaz en el concurso, también incluimos incentivos. Según las condiciones del concurso, los analistas que ocuparan el primer, segundo y tercer lugar recibirían un pago en efectivo del fondo del director del departamento como parte de la bonificación trimestral del banco, así como premios conmemorativos.

Otra interesante condición del concurso era que un analista solo podría recibir su premio si, en una reunión conjunta con otros analistas, presentaba detalladamente los métodos utilizados para lograr sus resultados: herramientas, patrones, áreas de riesgo, etc.

Algunas palabras sobre cómo el concurso influyó en la eficacia general del equipo analítico del Departamento de Monitoreo Financiero.

> ***«EL OBJETIVO DEL CERTAMEN CONSISTÍA EN DETECTAR Y BLOQUEAR CLIENTES SOSPECHOSOS CON RIESGOS DE BLANQUEO DE INGRESOS ILÍCITOS***

En primer lugar, durante el concurso aumentó la rapidez de respuesta ante los riesgos emergentes, y la mayoría de los clientes eran identificados antes de ser «etiquetados» en la plataforma «Conozca a su cliente» del Banco de Rusia. Este aceleramiento se debió tanto al aumento de la motivación de los especialistas como al uso de nuevos métodos originales de monitoreo de riesgos.

En segundo lugar, pudimos identificar una serie de puntos vulnerables en el proceso analítico, ya que los analistas, al buscar riesgos, exploraban las áreas de otros especialistas, lo que les permitía mirarlas desde una perspectiva fresca.

En tercer lugar, logramos elevar el nivel general de peritaje y ampliar el conjunto de herramientas y métodos analíticos que emplea el equipo. Esto fue posible porque los ganadores del concurso cumplieron con la condición de presentar sus secretos de éxito en la reunión general.

Impulsados por los resultados obtenidos, desde diciembre de 2023 hasta febrero de 2024 organizamos un segundo concurso individual de analistas, en el cual aumentamos los requisitos de fundamentación de los riesgos de lavado de dinero de los clientes identificados. En el resto, las condiciones básicas del concurso no se modificaron.

Los efectos positivos de este concurso fueron similares a los del primero, aunque menos destacados. Se hizo evidente que las vulnerabilidades en el proceso analítico ya habían sido subsanadas, se habían dominado herramientas de monitoreo eficientes, se había igualado el nivel de pericia del equipo y se había limpiado bastante bien la base de clientes de riesgos.

Parecía que habíamos extraído todo el valor posible de estos concursos, pero no queríamos poner el punto final. Entonces, ideamos una nueva versión del concurso, transformándolo de un formato individual a uno de equipos.

No hubo dificultades para formar equipos, ya que nuestros departamentos y grupos analíticos están organizados por áreas, con grupos de entre 3 y 6 analistas.

Entre las novedades del concurso por equipos, redujimos la duración del concurso a 6 semanas, y el resultado evaluado no era solo la identificación de un cliente sospechoso, sino la preparación de una investigación analítica en forma de un esquema de operaciones sospechosas, con una descripción detallada y materiales adicionales que corroboraran los riesgos identificados.

El equipo ganador sería aquel que preparara el mayor número de estas investigaciones analíticas. Todos los integrantes del equipo ganador recibían un pago en efectivo del fondo del director del departamento como parte de la bonificación trimestral del banco, así como un trofeo de equipo.

> ***«EN JULIO Y AGOSTO DE 2024, SE ENVIARON A ROSFINMONITORING MÁS DE 180 INVESTIGACIONES ANALÍTICAS DE ALTA CALIDAD REALIZADAS DURANTE EL CONCURSO***

La elaboración de esquemas con investigaciones no es una parte estándar del trabajo de los analistas en materia de PLA/FT, y al inicio del concurso parecía que esto podría suponer un desafío. Sin embargo, la realidad fue que los equipos rápidamente se adaptaron a las nuevas herramientas.

Trabajando en equipo, los líderes de área pudieron equilibrar la distribución de la carga de trabajo entre las tareas regulares de los especialistas y las tareas del concurso. Además, el enfoque de equipo permitió una distribución eficiente de las responsabilidades: algunos miembros se concentraban en identificar clientes sospechosos, mientras que otros se enfocaban en la visualización de sus operaciones en los esquemas.

Al concluir el primer concurso por equipos, que tuvo lugar de marzo a abril de 2024, los equipos lograron elaborar más de 100 investigaciones.

Después de un breve descanso, organizamos un segundo concurso por equipos de junio a julio, con el objetivo de mejorar la calidad de las investigaciones analíticas hasta un nivel en el que pudiéramos enviarlas con confianza a Rosfinmonitoring. Así nació el proyecto «ARGUMENTO». Y lo logramos: en julio y agosto de 2024, se enviaron a Rosfinmonitoring más de 180 investigaciones analíticas de alta calidad realizadas durante el concurso.

Sin dudas, este es el resultado de un arduo trabajo de todo nuestro equipo analítico. Pero es importante no olvidar, que este resultado podría no existir sin esta idea de probar realizar el concurso de analistas, nacida en el verano del 2023.

LA PROTECCIÓN DE CIUDADANOS Y EL SISTEMA FINANCIERO: EN EL CENTRO DE ATENCIÓN

EL BANCO DE RUSIA PROTEGE LA SEGURIDAD FINANCIERA: SOBRE LAS MEDIDAS DE PROTECCIÓN REGULATORIA DE LOS CIUDADANOS ANTE LAS TRAMPAS DE LOS ESTAFADORES

Las medidas que están tomando los propios bancos, ya permiten aislar un importante volumen de ataques de defraudadores; lo vemos en las estadísticas

MIKHAIL MAMUTA,
miembro de Consejo de Directores del Banco de Rusia, gerente del Servicio de protección de los derechos del consumidor y accesibilidad a los servicios financieros

El Banco de Rusia está construyendo un sistema equilibrado para combatir a los estafadores y proteger a los consumidores de servicios financieros. Por un lado, nuestro objetivo es fomentar la cultura financiera entre la gente, es decir, desarrollar habilidades y hábitos de comportamiento financiero sensato y seguro. Esta tarea está integrada en la Estrategia de mejora de la alfabetización financiera, que se extiende hasta el año 2030 y que llevamos a cabo junto con el Gobierno de la Federación Rusa.

Por otro lado, como regulador del mercado financiero, el Banco de Rusia trabaja junto con los participantes del mercado para desarrollar un sistema de medidas de protección regulatoria a distintos niveles. Y puedo señalar con satisfacción que el mercado participa en este trabajo entendiendo la importancia e inevitabilidad de las medidas adoptadas.

Así, para luchar contra las «mulas» tenemos organizado un intercambio de información sobre las operaciones realizadas sin el consentimiento de los clientes entre todas las partes involucradas. Los bancos y la policía transmiten los datos de las personas involucradas en esquemas fraudulentos a la base de datos unificada de "mulas"

> «PARA LUCHAR CONTRA LAS «MULAS» TENEMOS ORGANIZADO UN INTERCAMBIO DE INFORMACIÓN SOBRE LAS OPERACIONES REALIZADAS SIN EL CONSENTIMIENTO DE LOS CLIENTES ENTRE TODAS LAS PARTES INVOLUCRADAS. LOS BANCOS Y LA POLICÍA TRANSMITEN LOS DATOS DE LAS PERSONAS INVOLUCRADAS EN ESQUEMAS FRAUDULENTOS A LA BASE DE DATOS UNIFICADA DE "MULAS" DEL BANCO DE RUSIA

del Banco de Rusia (ver el artículo de V.A. Uvarov en la revista «Seguridad Financiera», n.º 41). A esta base están conectadas todas las organizaciones de crédito del país.

La protección de ciudadanos y el sistema financiero: en el centro de atención Ellos limitan el acceso remoto de las «mulas» a las cuentas, bloquean las transferencias a sus cuentas y advierten a los remitentes que, con mucha probabilidad, están enviando dinero a una cuenta fraudulenta. Esto crea barreras adicionales para los estafadores y sirve como una lección amarga para las «mulas».

«EL PRÓXIMO AÑO ENTRARÁ EN VIGOR UNA LEY SOBRE LA AUTO-PROHIBICIÓN, DESARROLLADA A PARTIR DE NUESTRAS PROPUESTAS, QUE PERMITIRÁ A LA PERSONA ESTABLECER EN SU HISTORIAL CREDITICIO UNA PROHIBICIÓN DE OTORGAMIENTO DE PRÉSTAMOS Y CRÉDITOS

Para proteger a la población de mayor edad, el Banco de Rusia ha emitido recomendaciones a los bancos sobre la prestación de un servicio de «segunda mano». Con base en estas recomendaciones, actualmente se ha desarrollado un proyecto de ley federal. Este proyecto permitirá a las personas mayores o a aquellas con discapacidad designar a un asistente, una persona de confianza que también sea cliente del mismo banco. El asistente tendrá el derecho de rechazar transferencias sospechosas y ayudar a su protegido a comprender la situación. Sabemos que este servicio ya está en fase de implementación o está operativo en algunos de los principales bancos.

Existe el problema de los préstamos que los ciudadanos contratan bajo la influencia de estafadores, y no solo realizan transferencias a través de canales a distancia, sino que a veces también entregan efectivo a mensajeros. El próximo año entrará en vigor una ley sobre la auto-prohibición, desarrollada a partir de nuestras propuestas, que permitirá a la persona establecer en su historial crediticio una prohibición de otorgamiento de préstamos y créditos.

Ahora comenzamos a discutir con los participantes del mercado la posibilidad de introducir un periodo de enfriamiento entre la celebración del contrato de préstamo y la recepción del dinero. Si el banco sospecha que el prestatario ha sido influenciado por estafadores, se necesita un margen de tiempo para que la persona pueda calmarse, pensar, consultar con sus seres cercanos y entender qué ha sucedido. Se prevé que este periodo debería durar desde varias horas hasta varios días, dependiendo del importe del préstamo.

Otra iniciativa importante se refiere a informar al prestatario a través del portal «Gosuslugi» sobre la celebración del contrato de crédito y sobre la posibilidad de que pueda rechazarlo. Una de las estafas más populares es cuando un crédito o préstamo a nombre de una persona se formaliza sin su conocimiento.

Las medidas que están tomando los bancos por sí mismos, ya permiten aislar un importante volumen de ataques de defraudadores; lo vemos en las estadísticas. Pero para construir una protección verdaderamente efectiva, sin duda, es imprescindible una solución integral y la cooperación de todas las partes interesadas.

LOS BANCOS APRENDIERON A REACCIONAR DE MANERA OPERATIVA A LOS ESQUEMAS SUMERGIDOS

La Asociación de Bancos Rusos (ABR) está desarrollando e implementando activamente programas de lucha contra el fraude en el ámbito financiero; un paso importante ha sido el fortalecimiento de la cooperación interdepartamental e interdisciplinaria en la lucha contra las «mulas», así lo declaró el presidente de la ABR, académico de la Academia Rusa de Ciencias (RAS) Garegin Tosunyan. En su entrevista a los corresponsales de la revista «Seguridad Financiera», el experto habló sobre los desafíos que enfrentan las organizaciones de crédito en el ámbito de la prevención de lavado de activos y financiamiento del terrorismo (PLA/FT) y cómo se está desarrollando hoy el diálogo entre la comunidad bancaria y la inteligencia financiera de Rusia

— Estimado Garegin Ashotovich, la Asociación que usted dirige ha prestado tradicionalmente gran atención a cuestiones de seguridad financiera. ¿Cuán eficaces considera Ud. que son los bancos modernos en el cumplimiento de la tarea de garantizar la seguridad de sus clientes? ¿Y qué más se debería hacer para aumentar la efectividad de su trabajo?

— Cabe señalar que la cuestión de la seguridad financiera de los clientes se está trabajando en estrecha colaboración con las autoridades competentes.

Se están llevando a cabo discusiones activas sobre esta problemática en el marco de grupos de trabajo interdepartamentales, creados en las correspondientes autoridades gubernamentales, así como comités de la Asociación de Bancos Rusos sobre el aumento de la alfabetización financiera y sobre cuestiones de PLA/FT y riesgos de compliance.

Por ejemplo, como resultado de la conferencia interregional «Aumento de la protección de los consumidores de servicios bancarios contra acciones fraudulentas», celebrada en octubre de 2023 en la sucursal de la Región de Ryazan de la Oficina Central del Banco de Rusia en el Distrito Federal Central, se creó un grupo de trabajo conjunto con la participación de representantes del Banco de Rusia, Rosfinmonitoring, el Ministerio del Interior de Rusia, la ABR, organizaciones financieras y la comunidad científica.

Las tareas de este Grupo de Trabajo incluyen no solo el desarrollo de programas para contrarrestar la implicación de ciudadanos en esquemas financieros delictivos, sino también programas de formación para organizaciones financieras sobre los métodos para trabajar con clientes que han sido influenciados por estafadores y con representantes del llamado sector económico informal. Los miembros del Grupo de Trabajo prepararon un programa de formación basado en factores psicológicos y la evaluación del comportamiento financiero de los clientes. También han emitido recomendaciones para identificar operaciones sospechosas y están implementando varios proyectos adicionales que actualmente están siendo probados por organizaciones de crédito, en particular, un proyecto para identificar clientes que están bajo la influencia de ingeniería criminal en las etapas de atención en las sucursales bancarias, y proyectos para identificar «mulas».

En el ámbito de la lucha contra el lavado de dinero, se puede mencionar la plataforma «Conozca a su cliente» (el llamado «Semáforo»), que el Banco de Rusia ha implementado junto con Rosfinmonitoring recientemente.

Este programa demostró su eficiencia. Este mecanismo permite detectar de manera eficiente y reducir el número de entidades de alto riesgo. Las estadísticas muestran que el mercado está siendo constantemente limpiado, y ha aparecido una buena herramienta para el cierre forzoso de empresas «fantasma».

Un trabajo importante está siendo realizado por la comisión interdepartamental creada en el Banco de Rusia con la participación de representantes del mercado financiero. Esto permite la rehabilitación de empresas que por error pudieron haber sido incluidas en la lista «roja».

«LOS MIEMBROS DEL GRUPO DE TRABAJO PREPARARON UN PROGRAMA DE FORMACIÓN BASADO EN FACTORES PSICOLÓGICOS Y LA EVALUACIÓN DEL COMPORTAMIENTO FINANCIERO DE LOS CLIENTES. TAMBIÉN HAN EMITIDO RECOMENDACIONES PARA IDENTIFICAR OPERACIONES SOSPECHOSAS Y ESTÁN IMPLEMENTANDO VARIOS PROYECTOS ADICIONALES QUE ACTUALMENTE ESTÁN SIENDO PROBADOS POR ORGANIZACIONES DE CRÉDITO

— Garegin Ashotovich, sabemos que la Asociación implementa un programa completo para contrarrestar la implicación de ciudadanos en esquemas financieros sumergidos. ¿Podría contarnos sobre ello, y cuáles son, en su opinión, las razones de fenómenos como el «droppers»? ¿Por qué es tan frecuente entre los jóvenes?

— La Asociación de Bancos Rusos está desarrollando y ejecutando activamente programas de lucha contra el fraude en el ámbito financiero. Esto incluye ayuda metodológica y práctica, no solo para los representantes del mercado financiero, sino también para los ciudadanos.

En este sentido, la Asociación lleva a cabo una serie de actividades prácticas importantes. Como se mencionó anteriormente, los representantes de la Asociación participan en las actividades del Grupo de Trabajo conjunto, creado con el fin de fortalecer la cooperación interdepartamental e interdisciplinaria en la lucha contra los «droppers». Además, la Asociación organiza seminarios y reuniones con ciudadanos, incluidos en el marco del trabajo del Comité de la ABR para aumentar la alfabetización financiera, así como organiza la capacitación de representantes de los bancos sobre la prevención de la implicación deciudadanos en esquemas financieros informales y sobre el aumento de la alfabetización financiera de los ciudadanos, clientes de los bancos.

Hay varias causas de la actividad de los «droppers».

Según los especialistas, la principal razón es la creencia en dinero fácil, combinada con un bajo nivel de cultura financiera, ya que la oferta de ganar dinero a través de la entrega de su tarjeta bancaria para realizar transferencias suena tentadora:

— ¡No tienes que hacer nada! Solamente enviarás a través de tu tarjeta el dinero que te voy enviando. Eso es todo. ¡Te quedarás con el 20%!

Este tipo de ofertas pueden ser interesantes no solo para adolescentes.

Entre los jóvenes la velocidad de propagación de la información es muchísimo más alta. Los adolescentes

se comunican, comparten noticias, incluyendo las ofertas para convertirse en un «dropper». Es por eso los jóvenes son más propensos ser involucrados en la actividad sumergida. El desconocimiento de consecuencias legales de la actividad de «droppers» también es una de las causas de este fenómeno.

Para luchar contra los «droppers», además del trabajo realizado por el Ministerio del Interior de Rusia, Rosfinmonitoring, el Banco de Rusia y la comunidad bancaria, así como, lo que es importante, escuelas y universidades, probablemente serán necesarios cambios legislativos.

Al mismo tiempo hay que implementar activamente el modelo de una conducta financiera responsable. El trabajo para promover la cultura financiera se lleva a cabo por la Asociación de Bancos de Rusia. Se espera que todos los participantes del mercado financiero se unan a nuestras actividades en esta dirección.

— La Asociación de Bancos Rusos tiene una larga historia de interacción con la inteligencia financiera. ¿Qué cree que se ha logrado en todos estos años y cuál es su evaluación del cambio en el trabajo de los bancos en el marco de la lucha contra el lavado de dinero?

— Después de la adopción de la Ley Federal n.º 115-FZ «Sobre la lucha contra el blanqueo (lavado) de activos procedentes de actividades delictivas y financiamiento del terrorismo» el 7 de agosto de 2001 y el nombramiento del primer director de Rosfinmonitoring, Viktor Alekseyevich Zubkov, la Asociación de Bancos Rusos inmediatamente se involucró en el trabajo de lucha contra los ingresos delictivos.

A lo largo de los años, se han logrado resultados significativos en el sistema de lucha contra el lavado de dinero. Los bancos que no pudieron luchar adecuadamente contra el lavado de dinero abandonaron del mercado. Los bancos están mejorando su conocimiento y experiencia en la lucha contra operaciones financieras ilegales, y se está desarrollando activamente la base tecnológica de monitoreo financiero. La elaboración de propuestas para mejorar la normativa siempre se realiza con la participación de representantes de la comunidad bancaria.

Los bancos están en el diálogo estrecho con Rosfinmonitoring Los colegas han logrado crear una atmósfera única de confianza en el trabajo con los proveedores de servicios financieros. Como ejemplo se puede indicar el trabajo para informar sobre los riesgos. Así, los bancos envían a la inteligencia financiera descripciones de nuevos esquemas que han detectado, y Rosfinmonitoring elabora esos esquemas y los comunica a los demás participantes del mercado en forma de tipologías.

Los bancos aprendieron a reaccionar de manera operativa a las modificaciones rápidas de los esquemas, que en la actualidad son desmantelados y prevenidos muy rápidamente.

Los principales desafíos a los que se enfrentan los bancos en el ámbito de la PLA/FT son los siguientes:

Lucha contra el financiamiento del terrorismo. Objetivamente, debemos aumentar la efectividad de la función preventiva y de advertencia de los bancos en este área tan importante.

Desarrollo acelerado de la economía digital e implementación del rublo digital. Esto requiere mejorar la legislación para un uso adecuado de nuevas tecnologías en la lucha contra operaciones financieras ilegales y nuevos esquemas de lavado de dinero.

Aparición de monederos electrónicos, herramientas electrónicas de pago y criptomonedas. Los delincuentes, con la ayuda de tecnologías modernas intentan ocultar las fuentes de origen de activos. La comunidad bancaria y el Estado están en la estrecha colaboración para resolver este problema. Un ejemplo puede ser las recomendaciones metodológicas publicadas a principios de este año por el Banco de Rusia para fortalecer el control sobre las operaciones con criptomonedas, así como el desarrollo por parte de *Rosfinmonitoring* de la concepción de cripto compliance.

«LOS BANCOS ENVÍAN A LA INTELIGENCIA FINANCIERA DESCRIPCIONES DE NUEVOS ESQUEMAS QUE HAN DETECTADO, Y ROSFINMONITORING ELABORA ESOS ESQUEMAS Y LOS COMUNICA A LOS DEMÁS PARTICIPANTES DEL MERCADO EN FORMA DE TIPOLOGÍAS

JEFA DEL SERVICIO DE COMPLIANCE DE SBERBANK

LARISA ZALOMIKHINA:

¿EN QUÉ TRAMPA CAEN LAS «MULAS DE DINERO»? COMO NO CONVERTIRSE EN UNA VÍCTIMA DEL ESQUEMA SUMERGIDO

El involucramiento de ciudadanos en la satisfacción de las demandas de la economía sumergida mediante transferencias P2P dudosas es un tema actual. Cómo los ciudadanos de a pie se convierten en parte de la cadena de lavado de activos y cómo luchar contra ello, es un tema de investigación para los especialistas del sector bancario

— ¿Cómo un cliente ordinario se convierte en «mula»?

— Los «conductores de mulas» generan un conjunto de tarjetas y luego las utilizan en el procedimiento sumergido. Ellos piden a clientes ordinarios transferir dinero o retirar efectivo, venderles la tarjeta bancaria. Normalmente lo hacen en Internet, en las proximidades de las sucursales bancarias, de los cajeros automáticos, e incluso en los colegios y universidades.

Por ejemplo, se puede encontrar este tipo de anuncios en redes sociales: «Buscamos personas responsables que desean trabajar con seriedad e intensidad. Hacemos ingresos en tarjeta. 50% para nosotros y 50% para Ud».; «Transfiero dinero a la tarjeta para retirarlo en efectivo. Transferencia mínima de 100.000 rublos, 2% de remuneración para usted».

El precio de la tarjeta bancaria de la «mula» puede alcanzar varios miles de rublos, dependiendo de la región, y al principio, las personas se sienten atraídas por la posibilidad de «ganar dinero rápido», especialmente si las ofertas de «trabajo» provienen de conocidos.

Así lo explicó un cliente, estudiante de una prestigiosa universidad: «Me ofrecieron una ganancia pasiva pero no me explicaron la esencia, me lo propuso un conocido, que me presentó a su familiar, quien me ofreció colaborar con sus amigos y recibir 10.000 rublos al mes "sin hacer nada", y yo acepté. Fuimos a la oficina local del Servicio Federal de Impuestos, él dijo que abriera un negocio individual, luego me ordenó hacer la tarjeta en el banco y entregáserla a él. Ya entonces empecé a sospechar que había algo raro, intenté dar marcha atrás, pero tenía miedo del uso de la violencia por parte de mis "empleadores"».

La intimidación y el chantaje son herramientas comunes utilizadas por los «domadores de mulas»: «Lo que más temo es que mis padres pronto se enterarán de todo y que mi mamá no lo soportará».

— ¿Ayuda el grado de información de los clientes a prevenir la transferencia de tarjetas a terceros?

— El establecimiento de un sistema de control efectivo será más exitoso cuando exista un suficiente grado de concienciación de los ciudadanos sobre la necesidad de seguir las reglas básicas para realizar operaciones bancarias, ya que a menudo

las personas, por ignorancia, se convierten en parte de esquemas de lavado de dinero:

«Le presté 7 millones de rublos a mi amigo. Como él vive en otra ciudad, me pidió transferir el dinero de los clientes de su tienda a mi tarjeta. Sabía que tenía una tienda grande y que paga impuestos, por eso accedí».

Publicaciones en los medios de comunicación, redes sociales y revistas especializadas; para diferentes clientes se seleccionan diferentes canales de información. Cerca del 60% de las «mulas» son jóvenes menores de 24 años, y para trabajar con la juventud se ha creado un recurso educativo específico del banco: SberSova.ru.

— ¿Los clientes comprenden que «algo va mal» y cuál es el sentido de las preguntas que hace el banco?

— Si la naturaleza de las operaciones no es evidente, el banco pedirá que se presenten documentos que confirmen el origen del dinero y explicaciones sobre el significado de las operaciones. La atención del banco es atraída por múltiples transferencias con diferentes contrapartes.

Al cliente a veces le resulta difícil orientarse sobre qué documentos puede proporcionar, por lo que simultáneamente con la solicitud, el banco envía una nota[1] que enumera ejemplos de documentos según diversas situaciones cotidianas.

Por ejemplo, si la fuente de ingresos son los pagos de personas o empresas por contrato de préstamo, compraventa, prestación de servicios o cesión, serán adecuados los siguientes documentos:

- contrato, con todos los anexos y acuerdos adicionales;
- acta de entrega y recepción, acta de prestación de servicios, pagaré, albarán de entrega, recibí, etc.
- documentos que confirman el título de propiedad de bienes o servicios que generan ingresos;
- documentos que confirmen el préstamo: resguardos de recibos de caja, orden de pago, extracto de cuenta abierta en otro banco, pagarés, talones;
- documentos que confirmen la fuente de activos para la contratación o liquidación del préstamo.

Cuando la fuente de ingresos está relacionada con operaciones en criptomoneda:

- dirección de la web, bolsa/casa de cambio dónde se compró o se vendió la criptomoneda;
- nombre de usuario o alias, utilizados para la realización de las transacciones;
- captura de pantalla o impreso del perfil o área personal que permiten identificar de manera inequívoca al titular de la cuenta;
- registro de transacciones con criptomoneda en forma de extracto: fecha de la transacción, tipo de cambio, importe de criptomoneda comprada/vendida;
- Informe PNL (informe de pérdidas y ganancias) para cada divisa digital.

Los clientes pueden organizar la recolecta de dinero para fines benéficos u otras necesidades. El banco pide presentar:

- capturas de pantalla o enlaces a la página de la recolecta;
- explicación escrita sobre los fines de la recolecta;
- documentos que confirmen los gastos para los fines declarados.

En dependencia de la fuente de ingresos pueden ser necesarios otros documentos.

Recomendamos a los clientes que no ignoren las solicitudes del banco.

Incluso si los documentos resultan insuficientes para responder a todas las preguntas, la interacción con el banco puede permitir continuar con la cooperación exitosa.

— ¿Qué documentos puede proporcionar el cliente, cuya tarjeta personal fue utilizada para transacciones comerciales?

— Si los pagos comerciales se realizaron a través de una tarjeta personal sin tener el alta como empresario individual o autónomo, al cliente le resulta realmente problemático reunir los documentos. Pero el banco se esfuerza no solo por detectar violaciones, sino también por dar a los clientes una oportunidad de rehabilitación.

Si el cliente se compromete a no usar tarjetas bancarias personales para realizar actividades empresariales, podrá continuar trabajando sin que se bloqueen sus cuentas. Por lo general, los clientes ante las preguntas por parte del banco siguen las recomendaciones del banco sobre cómo llevar a cabo su negocio. Cerca del 80% de los clientes rechazan operaciones dudosas. Es un indicador alto.

— ¿Cómo los «conductores de mulas» intentan proteger contra el bloqueo las tarjetas que usan?

— Las estrategias de los «conductores de mulas» están en constante evolución, incluida la popular llamada «calentamiento» de la tarjeta, que simula una actividad normal en la cuenta y lo que busca es aumentar la confianza del banco en el cliente y reducir el riesgo de bloqueo. Tal «cautela» no ayudará, ya que la actividad transaccional de las personas involucradas en los esquemas difiere significativamente de los pagos cotidianos normales. En cuanto empiecen a realizarse en la cuenta operaciones típicas de los «conductores de mulas», la tarjeta será bloqueada.

Recomendamos a los clientes que hayan entregado sus tarjetas a terceros que de inmediato bloqueen el acceso a estas.

[1] https://www.sberbank.ru/common/img/uploaded/files/pdf/komplaens/document_115fz.pdf.

SEGURIDAD FINANCIERA DE LOS CONSUMIDORES DE SERVICIOS FINANCIEROS

En los últimos años, el gobierno y las organizaciones financieras han trabajado conjuntamente para mejorar la educación financiera de los ciudadanos. A finales de 2023, se aprobó la Estrategia actualizada de Educación Financiera, que amplió este objetivo hacia la formación de una cultura financiera. A fin de cuentas, el desarrollo de las competencias financieras de los ciudadanos beneficia tanto a las organizaciones financieras como a los consumidores de servicios financieros y a la economía del país en general

SVETLANA TOLKACHEVA,
Alto directivo en el Grupo VTB

Al enseñar a los clientes a mantener un comportamiento financiero adecuado cuando utilizan productos bancarios, nos esforzamos por explicar de la manera más sencilla y accesible posible sus particularidades. Cuando un cliente ingresa al mercado de valores y sabe cómo elegir correctamente los instrumentos financieros para su portafolio, es más probable que logre sus objetivos. Y lo más importante, se evita que el cliente se quede sin comprender qué producto ha adquirido.

Si la persona tiene un colchón de seguridad financiera, es poco probable que recurra a un crédito o préstamo en situaciones imprevistas. Es más probable que sepa planificar su presupuesto, sea racional en sus gastos y controle su nivel de endeudamiento. Así, un producto como el crédito será utilizado por esa persona de manera beneficiosa para sí misma. Para el banco, la probabilidad de que un cliente responsable con sus finanzas incurra en mora será mínima.

Uno de los aspectos importantes y al mismo tiempo difíciles de la seguridad financiera es la capacidad de planificar el presupuesto personal a largo plazo. Desde el punto de vista de las finanzas personales, cada etapa de la vida tiene sus propios retos y ventajas. Su comprensión, permite a la persona mejorar sus habilidades a tiempo y aumentar su nivel de ingresos. Diseñar su plan de jubilación y mantener el mismo nivel de ingresos después del retiro, es un desafío bastante complejo para cualquier persona. El programa de ahorros a largo plazo, lanzado recientemente, ayuda a los ciudadanos a formar un recurso financiero adicional para estos objetivos a largo plazo. Y nuestra tarea es comunicar a los clientes la importancia y las ventajas de estos productos, para que tengan confianza en su seguridad.

Sin embargo, para la mayoría de los ciudadanos, el tema de la seguridad financiera se asocia principalmente con el fraude. Según las estadísticas del Banco de Rusia, las principales víctimas de los estafadores son ciudadanos que trabajan, de entre 25 y 44 años, y con un buen nivel de estudios.

> «*EL PROGRAMA DE AHORROS A LARGO PLAZO, LANZADO RECIENTEMENTE, AYUDA A LOS CIUDADANOS A FORMAR UN RECURSO FINANCIERO ADICIONAL PARA ESTOS OBJETIVOS A LARGO PLAZO. Y NUESTRA TAREA ES COMUNICAR A LOS CLIENTES LA IMPORTANCIA Y LAS VENTAJAS DE ESTOS PRODUCTOS, PARA QUE TENGAN CONFIANZA EN SU SEGURIDAD*

Los estafadores idean nuevos esquemas, utilizan temas de actualidad para que su historia parezca lo más creíble posible. Así, cualquiera de nosotros puede caer en la trampa de los estafadores, especialmente si se encuentra en un estado emocional negativo.

La gran mayoría de los incidentes (el 85%) se realizan mediante métodos de ingeniería social. Los propios clientes proporcionan a los estafadores información financiera importante sobre ellos mismos (contraseñas, códigos, números de tarjetas, etc.). Al caer en esta trampa, el cliente tiende a culpar a cualquiera, incluido al banco. Por eso, estamos muy interesados en educar a personas de todas las edades sobre las medidas para combatir el fraude.

Con la transición de la mayoría de las operaciones financieras al entorno digital, el tema de la seguridad financiera se ha vuelto especialmente relevante. Además, las bases de la seguridad financiera se pueden enseñar desde una edad muy temprana. En cuanto un niño toma un smartphone, ya debería conocer las reglas básicas. Desde hace cuatro años, VTB lleva a cabo el proyecto «Abecedario Financiero» en colaboración con el programa «¡Buenas noches, pequeños!». Según los índices de visualización y retención, el proyecto supera todas las ediciones actuales del programa. Esto muestra un gran interés tanto por parte de los padres como la accesibilidad del material para los propios niños.

En los últimos años, las lecciones de educación financiera han comenzado a aparecer cada vez con más frecuencia en los programas escolares, aunque esta asignatura no es obligatoria. Las reglas básicas de comportamiento financiero establecidas en la familia y en la escuela ayudarán al niño durante toda su vida. Yo misma soy autora de un libro de texto de educación financiera para estudiantes de 10º y 11º grado y entiendo la importancia de un enfoque sistemático en la organización del aprendizaje.

> ***«EN EL DESARROLLO DE LAS COMPETENCIAS FINANCIERAS DE LOS CLIENTES, PARTIMOS DE LOS PRINCIPIOS DE SISTEMATICIDAD, ACCESIBILIDAD Y TRANSPARENCIA. LAS DIFERENTES MODALIDADES DE FORMACIÓN PERMITEN SATISFACER LAS NECESIDADES DE TODAS LAS EDADES***

Para que los conocimientos se traduzcan en aplicación práctica, el banco organiza regularmente eventos educativos tanto para clientes minoristas como para empleados de empresas que son clientes del banco. Los empleadores también están interesados en mejorar la educación financiera de sus trabajadores. Ya nadie se sorprende cuando durante el proceso de contratación laboral el empleador solicita el consentimiento del solicitante para obtener información de la oficina de historial crediticio. Al fin y al cabo, tener dificultades financieras reduce significativamente la productividad de un trabajador.

Por cierto, el tema más popular para la realización de eventos educativos es la protección contra fraudes en el entorno digital. En este tema, la posición proactiva del cliente en la gestión de sus finanzas es muy importante. Esto incluye, por ejemplo, la capacidad de crear contraseñas complejas y usar la autenticación de dos factores, gestionar su consentimiento para el tratamiento y uso de datos personales, verificar regularmente los recursos importantes y su historial crediticio, así como revisar la configuración de sus smartphones y cuentas.

En el desarrollo de las competencias financieras de los clientes, partimos de los principios de sistematicidad, accesibilidad y transparencia. Las diferentes modalidades de formación permiten satisfacer las necesidades de todas las edades. Por ejemplo, en los grupos de mayor edad, se priorizan los formatos presenciales. Debido a aspectos relacionados con la edad, no siempre es posible adquirir suficientes conocimientos sobre tecnologías digitales. La audiencia joven requiere una mayor organización e implicación en el proceso de aprendizaje. Los clientes que trabajan prefieren la formación en el momento que les resulta conveniente, en breves sesiones en formato online. Una discusión abierta de las ventajas y limitaciones de productos específicos no solo ayuda al cliente a elegir la mejor opción para alcanzar sus objetivos, sino que también aumenta la confianza en el banco.

NUEVAS TECNOLOGÍAS DE LOS BANCOS COMO HERRAMIENTA DE MITIGACIÓN DE LAS AMENAZAS FINANCIERAS

LUCHA CONTRA LAS TIPOLOGÍAS DEL COMERCIO ILÍCITO EN EL SISTEMA DEL OPERADOR DE MONEDA ELECTRÓNICA

Entre los factores clave que determinan hoy en día la especificidad de los servicios de dinero electrónico, entre los que se incluyen las billeteras electrónicas «YooMoney», se encuentran la simplicidad y la alta velocidad de las transacciones. Sin embargo, la naturaleza remota de los servicios prestados incrementa los riesgos asociados a la participación de sujetos deshonestos en el servicio. No es casualidad que, según la evaluación nacional de riesgos de Rusia sobre la legalización de ingresos delictivos (2022), la actividad de los operadores de billeteras electrónicas se haya clasificado como de alto riesgo

DMITRII GRONIN,
Jefe del Servicio de Control Interno de la OSFL «YooMoney», S.L., miembro del Consejo Internacional de Compliance

ELIZAVETA DEMIDOVA,
Jefa del Departamento de Monitoreo Financiero de la OSFL «YooMoney», S.L.

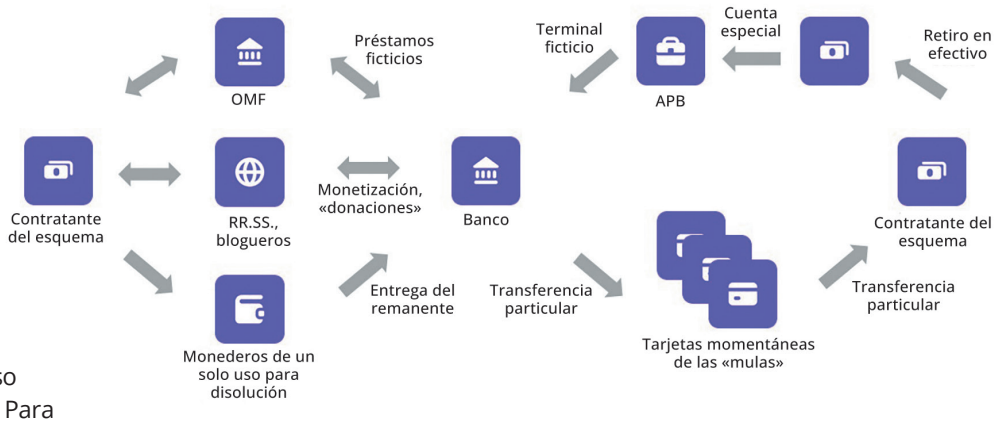
DMITRII POKROVSKIY,
Analista del Departamento de Seguridad Informática y Lucha Contra el Fraude de la OSFL «YooMoney», S.L.

Si hablamos de tipologías comúnmente identificadas, entre los delincuentes hay tanto vendedores de bienes y servicios comunes que evaden el registro y la tributación adecuados, como personas que llevan a cabo actividades criminales más graves: infractores de regímenes especiales y de licencias, como intercambiadores de criptomonedas ilegales, casinos, narcotraficantes, vendedores de productos falsificados y esquemas piramidales financieros. Otro grupo importante lo constituyen los esquemas relacionados con el fraude (falsificación de dinero y documentos, hackeos de cuentas e ingeniería social), así como el proceso de lavado de ingresos ilícitos previamente acumulados, por ejemplo, provenientes de sobornos y malversación, infracciones fiscales y presupuestarias, y la utilización de documentos judiciales falsos.

En el ámbito del comercio ilegal, representan interés los esquemas que intentan camuflar actividades ilegales de alto volumen transaccional, con múltiples vendedores y compradores, como el intercambio de criptomonedas, los juegos de azar y las pirámides financieras, dándoles la apariencia de actividades legales (ver figura 1). En calidad de cobertura, pueden, por ejemplo, utilizarse compañías microfinancieras que registran las transacciones como préstamos otorgados y reembolsados por prestatarios ficticios.

Es importante destacar los esquemas que utilizan plataformas de *marketplace*, redes sociales y plataformas de *blogging* con fines ilegales, incluyendo la circulación de criptoactivos bajo la apariencia de «donaciones» y la monetización de contenido de video. Una parte significativa de estos recursos se identifica de inmediato durante su proceso de conexión y autorización. Para retirar los fondos acumulados, se utiliza la estrategia de «reconocimiento de culpa» de una persona ficticia, el titular de la billetera, lo que conlleva al cierre inmediato de la misma. La actualización de las reglas del motor analítico, los rechazos automatizados de fondos entrantes a cuentas bloqueadas y el aumento del tiempo de procesamiento de solicitudes de retiro de saldo han hecho que este esquema sea poco atractivo. Una nueva tendencia es el renacimiento de la involucración de agentes bancarios de pago en esquemas ilícitos, aprovechando la comodidad de integración de su software con los bancos que los han atraído, lo que vuelve a ser aprovechado por los delincuentes. Observamos que el megaregulador actúa de manera eficaz para identificar este tipo de situaciones y tomar medidas, incluyendo la revocación de licencias. Las medidas activas y sistemáticas de las organizaciones de crédito, del regulador y de Rosfinmonitoring respecto al uso de pagos electrónicos en esquemas ilegales han llevado a que hoy en día este tipo de actividad ilegal haya sido prácticamente erradicada del segmento B2C (servicios de caja y adquisición). A esto ha contribuido, en particular, una serie de recomendaciones del Banco de Rusia, que han aumentado la atención sobre la adquisición comercial y la asignación de códigos MCC. La práctica de monitoreo muestra que el nuevo estándar para los organizadores del comercio ilegal son las transacciones C2C personales, que involucran ampliamente operaciones con billeteras, transacciones de card2card y transferencias a través del Sistema de Pagos Rápidos (SPR). Tras registrar los parámetros de la operación en la plataforma del organizador de comercio ilegal (por ejemplo, el monto y la tasa de compra de criptomonedas, los medios de pago para abonar y recibir), se proporcionan al comprador los detalles de adónde debe realizar la transferencia C2C en un tiempo limitado. El organizador identifica el pago según el cumplimiento de este plazo y los datos del remitente. No se requiere información adicional, como el concepto de pago, para estas transacciones, lo que las hace completamente opacas para el banco que las procesa y las hace indistinguibles de una transferencia personal privada. Los organizadores del comercio ilegal logran evadir los indicadores formales de actividad masiva utilizando personas ficticias («mulas») y emitiendo a su nombre instrumentos de pago instantáneo, cada uno de los cuales se utiliza para transacciones con un comprador real no más de una o dos veces, lo que hace inútil la creación de listas negras con estos datos.

▸ Figura 1. **Proceso sumergido de comercio ilícito**



La creciente actividad de este esquema en el mercado del comercio ilegal indica la necesidad de un mayor control por parte de las organizaciones de crédito sobre la emisión de instrumentos de pago instantáneo, los procesos de identificación de clientes (personas físicas) y la implementación de medidas adicionales para combatir el uso indebido de datos personales por parte de terceros («mulas»), ya sea sin el conocimiento y consentimiento de sus propietarios, o con la participación voluntaria de estas personas en actividades delictivas mediante el uso desleal de sus datos.

PARA CORTAR LOS ESQUEMAS ILÍCITOS SE PRACTICA EL ENFOQUE INTEGRAL

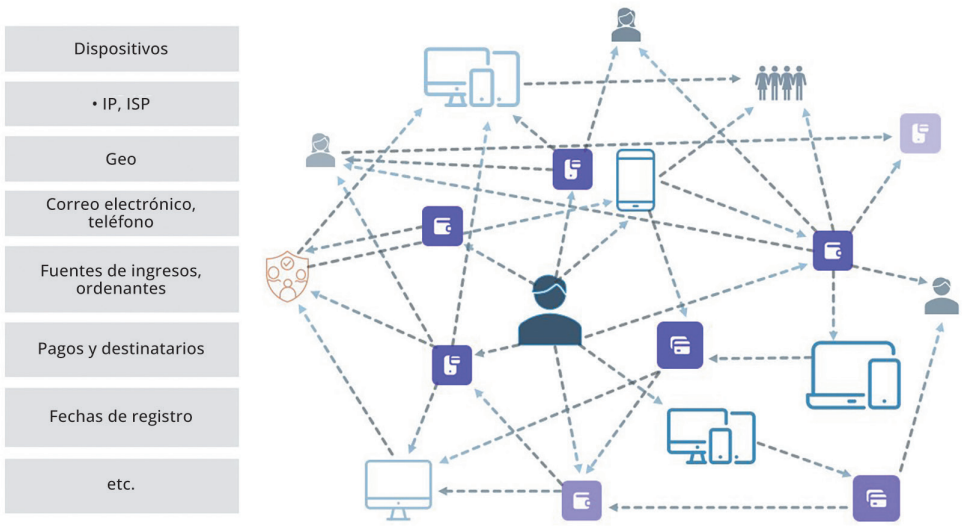
Esto implica la combinación de métodos de monitoreo expertos, basados en el análisis regular de muestras orientadas al riesgo, con el control en línea de los flujos de pagos, incluyendo los criterios propuestos por el Banco de Rusia y las propias reglas analíticas desarrolladas con el uso de aprendizaje automático.

PUNTOS IMPORTANTES DE CONTROL TANTO EN CASO DE SELECCIONES MANUALES COMO EN SISTEMAS AUTOMATIZADOS DE CONTROL SON:

- comentarios negativos y que señalan a actividades ilegales, sobre los sitios web conectados al sistema de adquisición (recibidos por las OSFL o en foros de opiniones independientes);
- las relaciones entre directivos, representantes y propietarios, así como las huellas digitales de los dispositivos utilizados, direcciones IP predominantes, registros de cookies, números de teléfono, correos electrónicos, patrones de creación de inicios de sesión, geografía de uso de cajeros automáticos y terminales, y otros datos relacionados con clientes previamente identificados en actividades ilegales;
- importantes vínculos entre pagadores de diferentes tiendas que formalmente pertenecen a personas independientes, sin indicios de vínculo propio (por ejemplo, pagos sincronizados a nuevas direcciones de pago por parte de consumidores de drogas o jugadores compulsivos detectados anteriormente);
- cambios significativos en el contenido del sitio donde se ubican los formularios de pago, como la aparición de términos que sugieren actividades ilegales (por ejemplo, sustancias prohibidas) o productos y servicios sujetos a licencias o regulaciones especiales;
- el volumen de operaciones o el promedio de los pagos exceden los niveles esperados para la actividad declarada, o no coinciden con la descripción de los productos y servicios ofrecidos en el sitio web del cliente;
- otros patrones de comportamiento en los pagos característicos de clientes previamente identificados en actividades ilegales y otras anomalías de pagos, teniendo en cuenta las cantidades, la frecuencia, la geografía de los pagos y otros factores.

Otra tarea importante para frenar el comercio ilegal con el uso de criptomonedas es establecer enfoques y algoritmos para vincular la actividad transaccional del cliente con sus operaciones en el ámbito no fiduciario. Actualmente, diversas plataformas tecnológicas, como «Cadena de bloques transparente», en cuyas pruebas de operación participamos recientemente, permiten realizar esta sincronización. La plataforma permite analizar el movimiento de criptomoneda, encontrar vínculos peligrosos y realizar la evaluación del riesgo de las operaciones. Esto en gran medida aumenta la relevancia de la evaluación del riesgo del cliente.

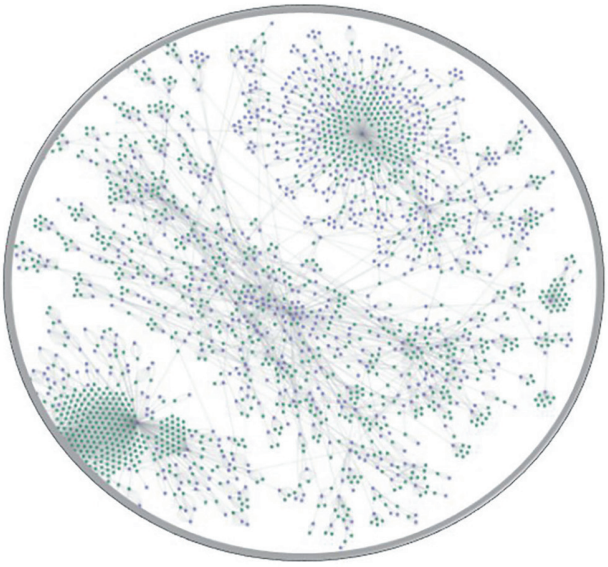
▶ Figura 2. **Intersecciones y vínculos considerados para determinar el clúster**



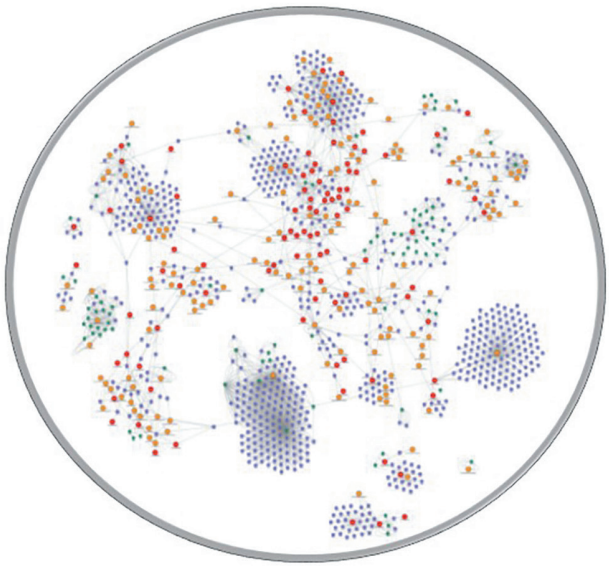
El conjunto de reglas automáticas de acción continua abre nuevas posibilidades para la detección operativa y erradicación de tipologías ilícitas. Para que muchas funciones del analista de compliance sean trasladadas a la máquina es necesario describir los indicadores de sospecha mediante algoritmos, definir los factores más relevantes y aprender a etiquetar de forma automática, rápida y confiable las cuentas sospechosas. Para detectar redes de clientes deshonestos interrelacionados, utilizamos grandes volúmenes de datos: registros de usuarios, información de acceso, recargas y pagadores, velocidad de retiro de fondos, pagos en comercios, uso de cajeros automáticos, dispositivos y direcciones IP, datos sobre el uso de diferentes proxys y VPN, entre otros (ver figura 2).

Para trabajar con el volumen de datos resultante, enlazado por relaciones de muchos a muchos, una solución adecuada son las bases de datos de grafos. Un grafo es un sistema de objetos de naturaleza arbitraria (vértices) y enlaces (aristas) que conectan algunos objetos, lo que lo convierte en un sistema conveniente y comprensible para la descripción de datos. En nuestra práctica, hemos elegido y utilizamos el sistema de gestión de bases de datos Neo4j. En nuestra aplicación, los nodos de grafos, por ejemplo, pueden ser cuentas y tarjetas, identificadores de dispositivos, direcciones IP, etc. Los enlaces pueden ser operaciones, autorizaciones, conexiones con correo electrónico o teléfonos.

▸ Figura 3. **Visualización de clústeres de bajo y alto riesgos**



Los colegas en varias oficinas recolectan dinero para los cumpleaños



Clúster de usuarios de casas de cambio de criptomoneda

Las bases de datos de grafos son excelentes para detectar y analizar conexiones complejas y poco evidentes entre entidades, transacciones y otros eventos característicos de esquemas ilegales, lo que ofrece las siguientes ventajas significativas:

- Análisis: simplicidad de solicitudes para búsqueda de vínculos. El lenguaje simple de consultas, permite añadir nuevas entidades fácilmente.
- Visualización e interpretabilidad de resultados.
- Multitud de algoritmos conocidos para las tareas de clusterización.
- Enfoque único para la solución de problemas diferentes. Para evaluar y marcar los clústeres de riesgo, analizamos, en particular, los siguientes indicadores:
  - porcentaje de usuarios bloqueados en el clúster;
  - porcentaje de usuarios con alto flujo de caja;
  - fechas cercanas de registro;
  - existencia de transferencias de ordenantes que anteriormente pagaban a otros clústeres de riesgo.

Sobre la base del conjunto de clústeres con una evaluación negativa identificada, el análisis posterior de todo el conjunto de datos se lleva a cabo utilizando redes neuronales de grafos (GNN).

Al observar la representación visual de los grafos (ver figura 3), se puede ver la diferencia evidente entre la actividad de recaudar dinero para cumpleaños en las oficinas de «YooMoney» y el comercio de criptomonedas (en la gráfica, los usuarios de bajo riesgo se representan en morado, los de alto riesgo en rojo y amarillo, y los dispositivos en verde). Esta diferencia puede ser detectada también por el algoritmo programado de manera independiente. En los clústeres de las cuentas vinculadas de los empleados de «YooMoney» (Figura 3, arriba) no hay ningún usuario bloqueado. Las cuentas están conectadas porque todas usan las mismas direcciones IP en tres ciudades, tienen dispositivos similares y realizan transferencias regulares entre sí para celebraciones de cumpleaños.

En conclusión, a pesar de la amplia gama de problemas existentes, las metodologías aplicadas por el Banco de Rusia, la participación en proyectos piloto de Rosfinmonitoring y nuestros propios desarrollos, incluyendo el uso de bases de datos de grafos, nos permiten ajustar rápidamente el sistema para identificar y frenar de manera efectiva un amplio conjunto de esquemas ilegales.

PERSPECTIVAS DE LOS SERVICIOS BIOMÉTRICOS Y SU PAPEL EN EL AUMENTO DE LA SEGURIDAD DE LOS CLIENTES DE LOS BANCOS

Las tecnologías biométricas se están convirtiendo en una parte integral del sistema financiero moderno. En un contexto de digitalización creciente de los servicios bancarios, garantizar la seguridad de los clientes alcanza un nuevo nivel. Los métodos tradicionales de protección, como contraseñas y códigos SMS, ya no pueden enfrentar de manera efectiva las amenazas provenientes de los ciberdelincuentes. En esta situación, los servicios biométricos se presentan como una herramienta confiable, capaz de resolver el problema de la identificación del usuario y mejorar significativamente la seguridad de las operaciones

NIKITA CHUGUNOV,
Vicepresidente senior, jefe del Departamento de Negocio Digital del Banco VTB

EVOLUCIÓN DE LAS AMENAZAS FRAUDULENTAS

En los últimos años, los ciberdelincuentes han cambiado considerablemente sus enfoques. Si antes los principales métodos de fraude eran el phishing y las llamadas desde números falsos de bancos, ahora los malhechores recurren cada vez más a esquemas complejos de ingeniería social. Su objetivo principal es obtener acceso a los datos personales del cliente, que pueden ser utilizados para robar dinero de sus cuentas.

Según datos[1] del Banco de Rusia, durante los últimos 7 años el número de operaciones sin el consentimiento de los clientes aumentó de manera importante: desde casi 300.000 hasta 1.165 millones al año. En términos monetarios, las pérdidas han aumentado casi 16 veces, alcanzando los 15,8 mil millones de rublos cada año. El número de ataques de los estafadores también sigue creciendo: por ejemplo, en el segundo trimestre se realizaron casi 260 mil operaciones fraudulentas, y se sustrajeron 4,7 mil millones de rublos de los clientes, un 23% más que el promedio de los 4 trimestres anteriores. Además, el número total de intentos de los delincuentes alcanza alcanzó 16,3 millones.

Estas cifras indican que los métodos tradicionales de protección, tales como contraseñas y códigos de un solo uso, ya no son efectivos frente a las crecientes amenazas. Los defraudadores ahora no se limitan a los intentos de robar el dinero a través de llamadas o cartas falsas. Los delincuentes utilizan esquemas híbridos que combinan phishing, robo de datos personales y manipulación directa de las personas.

En estas condiciones, el uso de datos biométricos(de características exclusivas de cada persona, como el rostro, la voz o las huellas dactilares) se convierte en una necesidad. La biometría no solo permite identificar al cliente con mayor precisión, sino que también reduce los riesgos de robo de datos, ya que estos son más difíciles de falsificar o robar en comparación con las contraseñas tradicionales o los códigos de un solo uso.

VENTAJAS DE LA BIOMETRÍA

Los sistemas de identificación biométrica, como el reconocimiento facial y de voz, permiten a los bancos

[1] https://cbr.ru/analytics/ib/operations_survey/2023/.

y otras instituciones financieras aumentar significativamente la seguridad de sus servicios. La principal ventaja de estos sistemas es la capacidad de distinguir de manera precisa y rápida a un usuario real de un estafador, incluso si este último ha obtenido acceso a parte de los datos del cliente.

Cada vez más, los bancos implementan soluciones biométricas, desde la apertura de cuentas a distancia hasta la confirmación de transacciones. Las tendencias dirigidas al uso de la biometría comenzaron a formarse mucho antes de la pandemia, pero las condiciones de crisis de 2020 aceleraron la implementación de servicios sin contacto y a distancia. Un ejemplo de ello son los proyectos piloto de adquisición biométrica, donde para confirmar un pago el cliente solo necesita una mirada. Además, desde hace varios años, la biometría se utiliza como medio de pago y acceso en el metro de Moscú, y más de 340 mil personas utilizan[1] este servicio. Cada día laborable, se realizan cerca de 150 mil accesos mediante biometría en el metro.

Los servicios biométricos también permiten elevar la comodidad en el uso de los servicios bancarios, incluso fuera de los límites del sector bancario. Los clientes ya no necesitan recordar contraseñas complejas, buscar un código QR o introducir numerosos códigos de un solo uso. Basta con usar una huella digital o un escaneo facial para confirmar cualquier operación. Esto simplifica significativamente la experiencia del usuario, haciéndola más rápida y cómoda, algo especialmente importante en un contexto donde se busca la máxima optimización del tiempo.

Por ejemplo, desde julio de 2024, los rusos pueden acceder a las salas VIP de los aeropuertos mediante biometría, gracias a un nuevo servicio implementado por el Centro de Tecnologías Biométricas, SNTP y el Banco VTB, en colaboración con VisionLabs y MILE-ON-AIR. Este servicio permite a los usuarios de Mir Pass, registrados en el Sistema Unificado de Biometría (SUB), acceder a las salas VIP simplemente mirando un terminal biométrico en la entrada. Para los clientes, esto no solo representa comodidad, sino también un ahorro significativo de tiempo, ya que no es necesario buscar el teléfono o el código QR, ni esperar a que un operador esté disponible, basta con registrarse de manera remota a través del portal de «Gosuslugi».

El servicio está disponible en los aeropuertos de Moscú, San Petersburgo, Kazán y Vladivostok, y en 2025 se sumarán a la iniciativa decenas de otros aeropuertos en todo el país.

Esta expansión demuestra que las tecnologías biométricas encuentran aplicación en diversos aspectos de la vida, confirmando su eficacia y fiabilidad.

LAS TECNOLOGÍAS BIOMÉTRICAS OFRECEN MUCHAS VENTAJAS:

1. Seguridad avanzada.
La biometr a proporciona un nivel de protecci n m s alto en comparaci n con los m todos tradicionales, ya que utiliza caracter sticas f sicas nicas, dif ciles de falsificar.

2. Mejor prevenci n del fraude.
La biometr a dificulta la copia de datos personales y ayuda a prevenir el robo de información.

3. Mejor experiencia de usuario.
Los clientes no necesitan recordar contrase as complejas, ya que la biometr a permite un acceso r pido y sencillo a los servicios.

4. Rentabilidad.
La biometr a ayuda a disminuir los gastos operacionales, sustituyendo los m todos tradicionales de identificaci n por otras soluciones m s eficientes.

5. Incremento de la eficiencia.
La optimizaci n de procesos a trav s de la biometr a ahorra tiempo y disminuye la necesidad de m todos manuales de control.

6. Inclusividad.
La biometr a facilita el acceso a los servicios para personas con discapacidad, haciendo que el servicio sea m s accesible.

RIESGOS Y DESAFÍOS EN EL CAMINO DE LA IMPLEMENTACIÓN

Sin embargo, la implementación de los sistemas biométricos conlleva no solo oportunidades, sino también desafíos. Uno de los principales riesgos es la seguridad de las bases de datos que contienen la información biométrica. Estos

[1] https://www.interfax.ru/moscow/958062.

datos tienen un alto valor para los ciberdelincuentes, y su filtración puede tener graves consecuencias tanto para los clientes como para los bancos.

Por ello, los bancos deben prestar especial atención a la protección de sus sistemas biométricos.

Esto incluye el uso de métodos de cifrado avanzados, protección multicapa y estrictas medidas de control de acceso. Es fundamental que los datos biométricos se almacenen y procesen en condiciones seguras, y que los propios sistemas se sometan a actualizaciones regulares y pruebas de resistencia a las amenazas.

La legislación también desempeña un papel importante en la regulación del uso de los datos biométricos. En Rusia, los requisitos para la recolección, almacenamiento y procesamiento de información biométrica se están endureciendo constantemente, lo que crea barreras adicionales para su uso en el sector financiero. Sin embargo, estas medidas están destinadas a minimizar los riesgos y garantizar la máxima protección de los datos de los clientes.

Además, las tecnologías biométricas enfrentan nuevos desafíos, como la aparición de *deepfakes* y tecnologías de creación de avatares digitales. Para combatir estas amenazas, se están desarrollando activamente tecnologías de aprendizaje automático (ML) e inteligencia artificial (IA). Estos sistemas pueden mejorar significativamente la precisión de las soluciones biométricas, reduciendo la cantidad de coincidencias erróneas. Los algoritmos avanzados son capaces de adaptarse a pequeños cambios en los datos biométricos, proporcionando una identificación más confiable. El aprendizaje automático y la inteligencia artificial pueden aumentar la seguridad de los sistemas biométricos, detectando amenazas y enfrentándolas antes de que puedan causar daño. Estas tecnologías pueden enriquecer la experiencia del usuario, simplificando y optimizando el proceso de autenticación. Así, la integración del aprendizaje automático y la inteligencia artificial representa una tendencia prometedora para el futuro de la biometría.

> ***EL APRENDIZAJE AUTOMÁTICO Y LA INTELIGENCIA ARTIFICIAL PUEDEN AUMENTAR LA SEGURIDAD DE LOS SISTEMAS BIOMÉTRICOS, DETECTANDO AMENAZAS Y ENFRENTÁNDOLAS ANTES DE QUE PUEDAN CAUSAR DAÑO. ESTAS TECNOLOGÍAS PUEDEN ENRIQUECER LA EXPERIENCIA DEL USUARIO, SIMPLIFICANDO Y OPTIMIZANDO EL PROCESO DE AUTENTICACIÓN.***

PERSPECTIVAS DEL DESARROLLO DE LA BIOMETRÍA EN EL SECTOR BANCARIO

A pesar de los riesgos existentes, las tecnologías biométricas tienen un enorme potencial tanto en el sector bancario como más allá. En el futuro, su uso se volverá más común. Podemos esperar un desarrollo continuo de los sistemas de adquisición biométrica y un aumento en el número de servicios donde la biometría se convertirá en el estándar para la verificación de identidad o la confirmación de operaciones.

El desafío clave para los bancos consistirá en asegurar la confianza de los clientes hacia las nuevas tecnologías. Los bancos deben informar activamente a sus clientes sobre las ventajas y la seguridad de las soluciones biométricas. Cuanto más comprendan las personas cómo funcionan estas tecnologías y cómo protegen sus finanzas, mayor será el nivel de confianza y disposición para utilizar estos servicios.

***

Los servicios biométricos ya desempeñan un papel clave en el desarrollo de las tecnologías bancarias, proporcionando tanto comodidad como un alto nivel de seguridad. En un entorno de amenazas cambiantes y de crecientes requisitos de ciberseguridad, su importancia solo continuará creciendo. Las instituciones financieras no solo deben continuar trabajando en la mejora de estos sistemas, sino también interactuar activamente con sus clientes para aumentar la confianza en las nuevas tecnologías.

CRIPTOCOMPLIANCE: PRIMERA EXPERIENCIA Y PERSPECTIVAS

Desde el 1 de septiembre de 2024, en Rusia ha comenzado la implementación de un régimen legal experimental para el uso de monedas digitales en la realización de pagos transfronterizos. Se están abordando cuestiones relacionadas con la creación de un mercado regulado de criptomonedas y su uso para pagos internacionales.
Una de las tareas clave de este régimen legal experimental es el ajuste de los mecanismos regulatorios, así como el estudio de los riesgos, el desarrollo de medidas para minimizarlos y la evaluación del impacto de estas innovaciones en el sistema financiero del país

ALEXANDR SKOTIN,
Jefe del Departamento de Organización y Análisis de la Dirección de Organización de Control de ***Rosfinmonitoring***

MARIA SCHERBAKOVA
Jefa del Departamento de Monitoreo de Riesgos de Sujetos Subordinados de la Dirección de Organización de Control de ***Rosfinmonitoring***

A principios de agosto de este año se aprobó una ley[1] federal que obliga a las personas que se dedican a la minería de monedas digitales y a quienes organizan pools de minería a cumplir con la legislación antilavado. Las novedades legislativas correspondientes requerirán la sincronización de los procedimientos de compliance y el ajuste de los mecanismos necesarios para el monitoreo financiero.

Los problemas de rastreo y evaluación del uso de criptomonedas en diversas operaciones, incluidas las ilegales, ya se habían planteado anteriormente. Con el crecimiento de la popularidad de las criptomonedas, se ha vuelto necesario entender y evaluar no solo el origen de los activos fiduciarios, sino también analizar los criptoactivos para garantizar la seguridad en el sector financiero.

La actividad de los representantes de la criptoindustria y la circulación de criptomonedas, según los resultados de la evaluación nacional de riesgos de legalización (lavado) de ingresos ilícitos, se consideran de alto riesgo y, por lo tanto, están bajo constante vigilancia de los participantes del sistema antilavado.

El trabajo para crear condiciones que aseguren los procedimientos de "KYC", la transparencia de las operaciones con criptomonedas y su vinculación con las transacciones en moneda fiduciaria se realiza de forma continua y actualmente se enfoca en el desarrollo de casos prácticos para la realización del monitoreo financiero y la adopción de medidas para reducir riesgos.

[1] Ley federal del 08.08.2024 № 222-FZ «Sobre modificaciones de algunas normas jurídicas de la Federación Rusa».

«CADENA DE BLOQUES TRANSPARENTE»

es una herramienta que permite analizar transacciones entre diferentes monederos teniendo en cuenta sus riesgos. La plataforma permite trazar el camino de la criptomoneda desde un monedero a otro.

Por ejemplo, utilizando materiales de *Rosfinmonitoring*, basados en el análisis de datos de la plataforma «Cadena de bloques transparente», se desmanteló un grupo organizado que distribuía drogas a través de una tienda en línea y ocultaba las sustancias en escondites. Para ocultar su actividad delictiva, los miembros de la organización desarrollaron un esquema de venta de drogas sin contacto y la posterior legalización de los ingresos obtenidos de estas ventas.

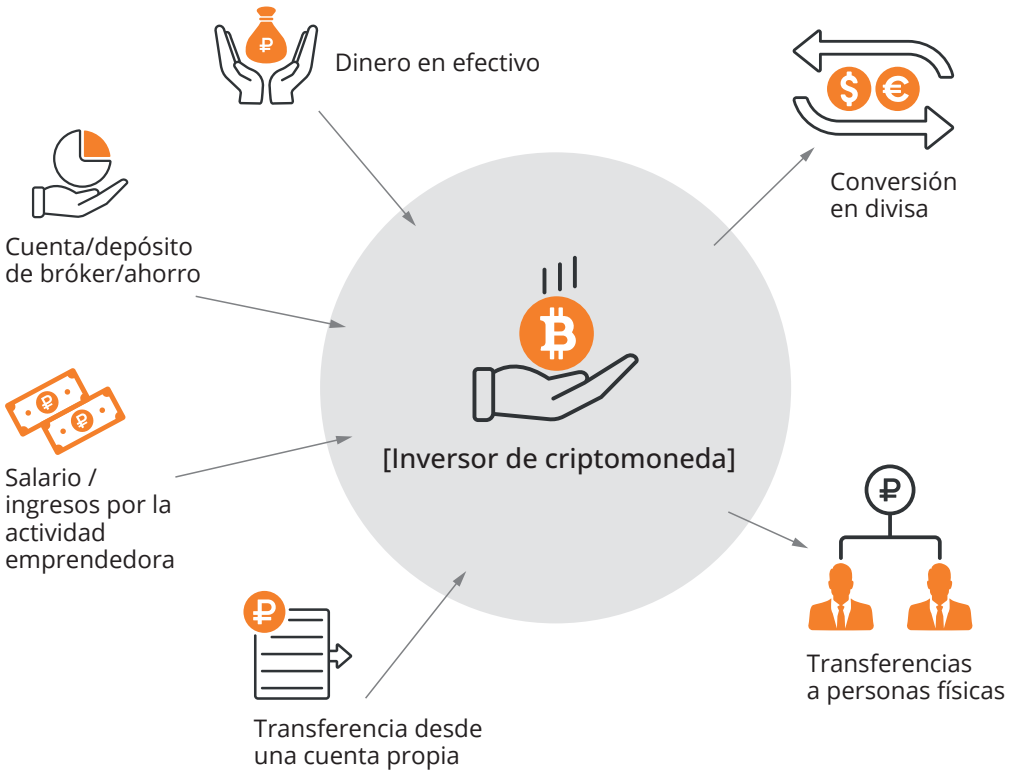
Los ingresos delictivos en forma de activos virtuales, recibidos como pago por la participación en el tráfico ilegal de drogas, se acumulaban en una billetera de criptomonedas. Para dar una apariencia legítima a la posesión de estos fondos, parte de los activos virtuales se transferían a otras billeteras de criptomonedas y luego se convertían en rublos rusos, que se depositaban en cuentas bancarias a nombre de familiares cercanos, quienes no estaban al tanto del origen de los fondos.

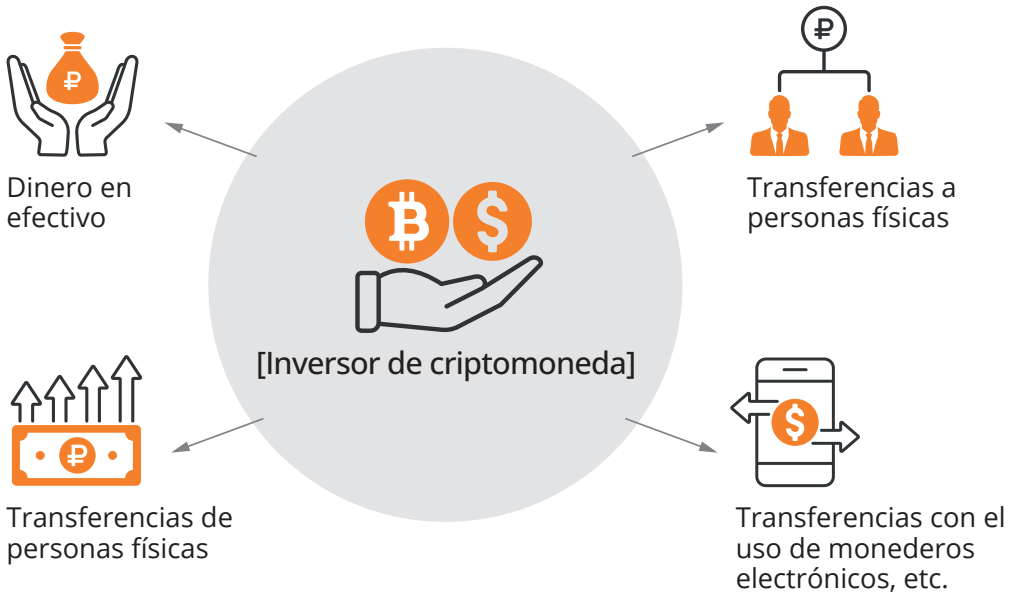
Contra los miembros del grupo delictivo, las fuerzas del orden iniciaron procesos penales por el delito de lavado de dinero según el p. 1 art. 174.1 del Código Penal de la Federación Rusa (legalización de ingresos criminales).

Además, se han aplicado medidas relacionadas con el uso de criptomonedas por parte de personas que abusan de su autoridad. Un ejemplo notable son las investigaciones en el marco de un caso penal iniciado por el hecho de recibir un soborno de gran magnitud. En este caso, el acusado, con la mediación de terceros, recibió un soborno en forma de una billetera de criptomonedas con más de 1.000 bitcoins (equivalente a más de 1.000 millones de rublos).

Como resultado del monitoreo de criptodirecciones utilizando el servicio «Cadena de bloques transparente», se identificó que parte de estos activos fueron retirados a través de un intercambio de criptomonedas con oficinas en varios países, y actualmente se han embargado estos activos virtuales.

Uno de los primeros pasos fue garantizar la posibilidad de que los sujetos de la Ley Federal del 07.08.2001 n.º 115-FZ «Sobre la lucha contra el blanqueo (lavado) de activos procedentes de actividades delictivas y financiamiento del terrorismo» informen a *Rosfinmonitoring* sobre operaciones relacionadas con la circulación de criptomonedas.





Sin embargo, con el creciente uso de las criptomonedas, incluyendo su uso para pagos de bienes y servicios ilegales, se ha requerido la sistematización de la información proporcionada al Servicio. Con la participación de representantes del Consejo de Compliance, *Rosfinmonitoring* desarrolló recomendaciones para los participantes del mercado para una definición más clara de las personas que realizan operaciones fiduciarias relacionadas con la circulación de criptomonedas, clasificándolos en dos segmentos: «criptoinversores» y «criptointercambiadores». Por «criptoinversores» se entienden personas físicas reales que compran criptomonedas con fines de inversión o para su sustento.

> ***DESDE 2023, ROSFINMONITORING JUNTO CON EL BANCO DE RUSIA Y CON LA PARTICIPACIÓN DE LAS PRINCIPALES INSTITUCIONES DE CRÉDITO, ESTÁ IMPLEMENTANDO UN PROYECTO PILOTO PARA LA INTRODUCCIÓN DE LA HERRAMIENTA «CADENA DE BLOQUES TRANSPARENTE» EN LAS ACTIVIDADES DE LAS ÁREAS DE COMPLIANCE DE LAS INSTITUCIONES FINANCIERAS***

Un «criptointercambiador», por otro lado, es generalmente un testaferro, conocido como «mula», cuyas cuentas bancarias y tarjetas se utilizan para el funcionamiento de una plataforma en línea (sitio web, aplicación móvil, bot de Telegram, entre otros) para la compra y venta de monedas digitales.

Esto permitió sistematizar y estructurar el flujo de información que llega a *Rosfinmonitoring*. Sin embargo, esta clasificación se basó en el análisis de operaciones fiduciarias y el comportamiento de los clientes, pero no abarcó la identificación de riesgos en el manejo de criptomonedas vinculadas a monederos específicos.

Dada la naturaleza de las monedas digitales y la falta de experiencia en conectar las operaciones fiduciarias de los clientes con transacciones de criptomonedas, las instituciones financieras enfrentaron dificultades para evaluar los riesgos de los clientes que participan en el comercio de criptomonedas. Por ello, desde 2023, *Rosfinmonitoring* junto con el Banco de Rusia y con la participación de las principales instituciones de crédito, está implementando un proyecto piloto para la introducción de la herramienta «Cadena de bloques transparente» en las actividades de las áreas de compliance de las instituciones financieras.

El proyecto piloto para la implementación de esta solución tecnológica en las actividades de los departamentos contra el lavado de dinero es un proceso complejo y de varias etapas, cuyo objetivo es no solo probar la funcionalidad del componente de software y determinar sus vías de desarrollo, sino también, basándose en los resultados de su uso, desarrollar un conjunto básico de algoritmos (escenarios) de monitoreo de operaciones y enfoques metodológicos para el compliance en relación con las criptomonedas.

En el proyecto piloto, las organizaciones de crédito enriquecieron la información sobre operaciones sospechosas con datos adicionales, como las direcciones de los monederos de criptomonedas

utilizados para realizar la transacción vinculada, su hashtag, el nombre de la bolsa de criptomonedas o del intercambio donde se realizó la transacción, así como una descripción de los riesgos asociados a su actividad.

En un contexto de mayor uso de las criptomonedas con fines delictivos, la identificación temprana de la actividad relacionada con criptomonedas de los clientes bancarios durante la realización de operaciones fiduciarias vinculadas es fundamental para la prevención de actividades delictivas, la financiación del terrorismo y el extremismo.

También se realizó un análisis adicional de las operaciones fiduciarias entre «mulas», cuyas herramientas de pago se utilizaron para el funcionamiento de un punto de intercambio de criptomonedas, y sus «clientes» dentro de la institución de crédito, con el fin de identificar a nuevas personas involucradas en dichas actividades.

En el futuro, se planea expandir la capacidad de monitoreo de las operaciones fiduciarias de los clientes de las instituciones financieras con los criptointercambiadores y durante

«EL PROYECTO PILOTO PARA LA IMPLEMENTACIÓN DE ESTA SOLUCIÓN TECNOLÓGICA EN LAS ACTIVIDADES DE LOS DEPARTAMENTOS CONTRA EL LAVADO DE DINERO ES UN PROCESO COMPLEJO Y DE VARIAS ETAPAS, CUYO OBJETIVO ES NO SOLO PROBAR LA FUNCIONALIDAD DEL COMPONENTE DE SOFTWARE Y DETERMINAR SUS VÍAS DE DESARROLLO, SINO TAMBIÉN, BASÁNDOSE EN LOS RESULTADOS DE SU USO, DESARROLLAR UN CONJUNTO BÁSICO DE ALGORITMOS (ESCENARIOS) DE MONITOREO DE OPERACIONES Y ENFOQUES METODOLÓGICOS PARA EL COMPLIANCE EN RELACIÓN CON LAS CRIPTOMONEDAS

la realización de operaciones entre diferentes bancos.

Desde el punto de vista metodológico, uno de los desafíos del proyecto piloto fue la identificación de la actividad de criptomonedas de los clientes, en particular, la identificación de los criptomonederos que utilizan.

El proyecto piloto también mostró la necesidad de mejorar los formatos de interacción informativa entre las organizaciones de crédito y *Rosfinmonitoring*. Los mensajes electrónicos formales se complementaban con datos obtenidos de la «Cadena de bloques transparente». Sin embargo, para un uso pleno de esta información durante la realización de investigaciones financieras y la automatización del macroanálisis de la información recibida, es necesario modificar los formatos de los mensajes, incluyendo indicadores de datos identificativos sobre la actividad en criptomonedas.

Los resultados obtenidos representan un avance hacia un objetivo más amplio: el compliance relacionado con criptomonedas debe convertirse en una práctica común para todas las instituciones financieras.

GALINA KUZNETSOVA:
GRACIAS AL USO DE MODELOS ML EN EL COMPLIANCE SE REDUCE EL RIESGO DEL ERROR HUMANO

En el ámbito de la seguridad financiera cada vez más se emplea la inteligencia artificial (IA) para la solución de sus tareas. Sobre cómo los modelos de ML (aprendizaje automático) ayudan a prevenir amenazas financieras, qué problemas se pueden abordar con su uso y por qué las máquinas no pueden reemplazar completamente el juicio profesional, cuenta la directora de compliance de "T-Bank", vicepresidenta Galina Kuznetsova

EL MODELO de ML es un modelo matem tico que se entrena a partir de datos y se utiliza para predicciones, clasificaciones, segmentaci n y otras tareas de procesamiento de la informaci n. Estos modelos son la base para desarrollar sistemas y aplicaciones capaces de procesar grandes vol menes de informaci n, permitiendo que los analistas trabajen con datos ya procesados.

7 AÑOS DE EXPERIENCIA EN EL USO DE MODELOS ML EN COMPLIANCE

Una característica distintiva de nuestro banco es el enfoque claramente minorista de su negocio y la prioridad de los formatos de interacción a distancia con los clientes. Esta especificidad genera un paisaje de riesgos particular y la necesidad de configurar adecuadamente los sistemas de compliance, así como los modelos utilizados para identificar actividades anómalas de los clientes.

En el banco, existe una enorme cantidad de procesos, productos y segmentos, y en cada uno de ellos implementamos de manera activa diferentes soluciones de ML, desde simples regresiones lineales hasta modernos transformadores generativos.

Durante todo el período de colaboración con «T-Bank», nuestros clientes se encuentran

bajo el control y monitoreo de modelos ML. En el departamento de compliance, llevamos más de 7 años desarrollando y aplicando modelos especializados de ML, adaptándolos a diversos requisitos y necesidades.

CUMPLIMIENTO DE LAS NORMAS DEL REGULADOR

La Ley Federal 115-FZ impone al banco la obligación de identificar operaciones sospechosas relacionadas con el financiamiento del terrorismo, el tráfico ilegal de drogas, la corrupción, la extracción de dinero en efectivo, la optimización fiscal y la fuga de capitales al extranjero.. Nuestra misión es asegurarnos de que los clientes no involucren al banco en la realización de tales operaciones. Los criterios y modelos desarrollados para identificar transacciones sospechosas han demostrado ser bastante eficaces, como lo confirman los datos del Banco de Rusia y la retroalimentación proporcionada por *Rosfinmonitoring*. Trabajamos de manera proactiva para identificar estas actividades de la forma más rápida posible.

Algunas de las operaciones sujetas a control tienen criterios claros para identificar riesgos. Sin embargo, un número significativo de clientes y sus transacciones no pueden ser evaluados solo con estos criterios, aunque existe la posibilidad de que sean ilegales, lo cual depende de diversos indicios. Dado el gran volumen de datos, cumplir con todos los requisitos del banco y garantizar la seguridad de los clientes y socios sería imposible sin el uso de inteligencia artificial. En condiciones de limitación de recursos, abordar estos desafíos sólo con el personal humano sería extremadamente difícil: hay que tener en cuenta y procesar una inmensa cantidad de información multidimensional para tomar decisiones. Aquí es donde entran en juego los modelos de puntuación ML, que permiten evaluar rápidamente a los clientes y las transacciones según múltiples parámetros.

VENTAJAS DE LOS MODELOS ML EN COMPLIANCE: RÁPIDO, DE CALIDAD Y SIN MOLESTIAS PARA EL CLIENTE

La empresa maneja muchas transacciones de clientes y está en constante crecimiento en términos de clientes y productos. Nuestros reglamentos internos exigen verificar a todos los clientes. Diariamente, la inteligencia artificial revisa todas las características de los clientes y registra cambios en la imagen del cliente, como modificaciones en los datos personales, transacciones salientes o apertura de nuevos productos. Monitorear esto manualmente de manera exhaustiva y sin errores sería imposible. Los modelos de ML lo hacen sin incomodar a nuestros clientes y detectan problemas de manera más precisa.

Gracias al uso de modelos ML para el control de clientes y transacciones se reduce el riesgo del error humano. Este es un momento crítico para el compliance, porque no podemos equivocarnos. Necesitamos mejorar constantemente la calidad de los controles.

Además, el modelo ML realiza un análisis instantáneo de situaciones específicas y permite actuar de manera preventiva, evaluando los posibles riesgos en función de los datos disponibles.

Otra ventaja de los modelos ML es su relativa simplicidad y rapidez para reentrenarse con nuevos datos. Esto permite adaptarse rápidamente a la realidad cambiante.

Es importante señalar que los modelos ML funcionan solamente con grandes volúmenes de datos. Si fuéramos un banco con solo 13 clientes, no tendría sentido utilizar inteligencia artificial. Sin embargo, para nosotros, los modelos ML son una herramienta clave en la detección inicial de transacciones sospechosas, permitiendo identificar de forma precisa una operación dudosa. La decisión final la toma una persona, y esta preselección inicial agiliza significativamente su trabajo y minimiza los errores humanos. La persona termina de comprobar la transacción marcada y toma la decisión.

> ***«DIARIAMENTE, LA INTELIGENCIA ARTIFICIAL REVISA TODAS LAS CARACTERÍSTICAS DE LOS CLIENTES Y REGISTRA CAMBIOS EN LA IMAGEN DEL CLIENTE, COMO MODIFICACIONES EN LOS DATOS PERSONALES, TRANSACCIONES SALIENTES O APERTURA DE NUEVOS PRODUCTOS***

CONTROL DE CALIDAD DEL TRABAJO DE LOS EMPLEADOS

En el área de compliance tenemos un departamento de control de calidad cuya función es mejorar la eficiencia de los empleados en las investigaciones manuales. El modelo ML detecta posibles errores en las primeras etapas, y los especialistas del departamento de calidad los revisan y corrigen. Esto ayuda a minimizar los errores potenciales de los empleados, evitar una mala experiencia para el cliente y reducir el número de transacciones sospechosas.

Al trabajar con operaciones vinculadas al blanqueo de capitales, el porcentaje de errores en los análisis manuales realizados por los empleados era bastante elevado, lo que afectaba negativamente la percepción que los clientes tenían de nosotros y generaba preguntas por parte del regulador.

Para corregir esta situación, empezamos a aplicar un modelo ML que puede evaluar si un empleado ha cometido un error y reducir el número de fallos, ofreciendo recomendaciones: «Es posible que te hayas equivocado aquí, revisa de nuevo».

NUEVOS DESAFÍOS

Antes, al recibir una señal sobre una operación negativa, bloqueábamos al cliente. Ahora es importante prevenir acciones ilícitas en la etapa cuando el cliente todavía lo está pensando. El modelo ML sabe predecir todas las acciones potencialmente peligrosas de los clientes. Para nosotros, este es un nuevo desafío, ya que nuestros planes de crecimiento y desarrollo exigen prevención, mitigación y minimización de riesgos. El modelo ML permite resaltar aspectos que requieren una revisión adicional incluso al momento de abrir una cuenta, solicitando documentación adicional cuando sea necesario.

El desarrollo de soluciones tecnológicas en el área de compliance es una prioridad para el banco. En el banco se implementan activamente los enfoques modernos para la integración, despliegue, monitoreo, almacenamiento, creación de versiones y reciclaje profesional, entre otros.

El banco presta una especial atención al desarrollo de criptocompliance. Actualmente, junto con *Rosfinmonitoring* y el Banco de Rusia, estamos desarrollando diferentes escenarios para detectar operaciones sospechosas de clientes que participan en el comercio de criptomonedas, utilizando la plataforma «Cadena de bloques transparente». Esta es una tarea extremadamente compleja, pero entendemos que sin solucionarla, el progreso en el monitoreo financiero sería limitado. Nos alegra que nuestros colegas de la inteligencia financiera mantengan un contacto constante y colaboren en diferentes cuestiones. Estoy convencida de que la atmósfera de confianza que se ha logrado en este proyecto permitirá obtener buenos resultados en el futuro cercano.

*«EL BANCO PRESTA UNA ESPECIAL ATENCIÓN AL DESARROLLO DE CRIPTOCOMPLIANCE. ACTUALMENTE, JUNTO CON **ROSFINMONITORING** Y EL BANCO DE RUSIA, ESTAMOS DESARROLLANDO DIFERENTES ESCENARIOS PARA DETECTAR OPERACIONES SOSPECHOSAS DE CLIENTES QUE PARTICIPAN EN EL COMERCIO DE CRIPTOMONEDAS, UTILIZANDO LA PLATAFORMA «CADENA DE BLOQUES TRANSPARENTE»*

LA OLIMPIADA INTERNACIONAL DE SEGURIDAD FINANCIERA COMO COMIENZO DE LA CARRERA EN EL ÁMBITO DE LA PLA/FT

NURSULUU KOZHONAZAROVA,
Especialista senior del Departamento de Monitoreo Financiero de la dirección de compliance del Optima Bank, República de Kirguistán

El área de prevención del lavado de activos y financiamiento del terrorismo (PLA/FT) desempeña un papel fundamental en la defensa de la seguridad financiera del estado y de la comunidad internacional. Como una joven profesional que está empezando en este campo, quiero compartir mi experiencia y observaciones, contar cómo la participación en las olimpiadas me ayudó en mi carrera, así como los retos actuales y las perspectivas del trabajo en el ámbito de la PLA/FT

Mi participación en la Olimpiada Internacional de seguridad financiera y mi formación en el Centro de Formación del Servicio Estatal de Inteligencia Financiera de la República de Kirguistán (CF SEIF RK) fueron etapas clave en mi desarrollo profesional. El centro de formación no solo me brindó los conocimientos necesarios para participar en la olimpiada a nivel internacional, sino que también sentó las bases para mi crecimiento profesional futuro. Es importante destacar que el programa de formación del CF SEIF RK estaba orientado a la aplicación práctica de los conocimientos, lo que resultó muy útil en mi trabajo posterior.

Mi participación en la Olimpiada Internacional de Seguridad Financiera fue un pilar fundamental para mi carrera en el ámbito del antilavado. La Olimpiada me permitió no solo probar mis conocimientos a nivel internacional, sino también intercambiar experiencias con colegas de otros países. Esta experiencia amplió mi comprensión de los desafíos globales en el ámbito de la PLA/FT y me brindó habilidades valiosas que ahora aplico en mi trabajo.

Fue especialmente gratificante recibir el reconocimiento por mis logros en el ámbito internacional. Esto no solo fortaleció mi confianza, sino que también me abrió nuevas oportunidades en mi desarrollo profesional. Fue tras mi participación en la Olimpiada que recibí una oferta de trabajo en el Servicio Estatal de Inteligencia Financiera de la República de Kirguistán.

EXPERIENCIA DE TRABAJO EN EL SERVICIO ESTATAL DE INTELIGENCIA FINANCIERA DE LA REPÚBLICA DE KIRGUISTÁN

El trabajo en el Servicio Estatal de Inteligencia financiera de la República de Kirguistán me aportó una experiencia única en el ámbito de la PLA/FT. Aquí aprendí a reaccionar de manera operativa ante amenazas financieras, analizar los datos y cooperar con diferentes instituciones públicas e internacionales.

Algunas de las tareas clave con las que me he enfrentado han sido el monitoreo de operaciones financieras y la identificación de transacciones sospechosas. Este proceso requiere de una gran concentración y atención a los detalles, ya que el éxito de toda la investigación depende de la calidad del análisis realizado. Trabajar en la Agencia también me enseñó que, en el ámbito de la PLA/FT es crucial mantener la confidencialidad y seguir normas éticas. La experiencia invaluable adquirida en la SEIF de la República de Kirguistán me ayudó a construir mi carrera en el área de compliance.

PARTICULARIDADES ACTUALES DEL TRABAJO EN LA PLA/FT Y COMPLIANCE

Mi trabajo actual en el campo del compliance es una continuación lógica

de mi trayectoria en la PLA/FT. En mi labor, me enfrento a un amplio rango de desafíos, siendo los principales el monitoreo de operaciones financieras y la detección de transacciones sospechosas. Este proceso incluye el análisis de datos, la recopilación de pruebas y la preparación de informes para ser enviados a las autoridades competentes. Los aspectos relacionados con la introducción de criptomonedas y la tecnología de cadena de bloques son particularmente relevantes, lo que requiere que los especialistas actualicen constantemente sus conocimientos y habilidades.

También es esencial participar en el desarrollo y la implementación de políticas y procedimientos internos para prevenir el lavado de activos y la financiación del terrorismo, lo cual incluye la capacitación de empleados, la realización de investigaciones internas y la colaboración con los organismos reguladores.

Una de las tareas clave es la gestión de riesgos. En un entorno legal que cambia constantemente y ante la aparición de nuevas amenazas, como la ciberdelincuencia y el uso de nuevas tecnologías en fraudes financieros, los especialistas en compliance deben ser capaces de identificar y minimizar los riesgos de manera oportuna.

Mi experiencia en la Agencia Estatal de Inteligencia Financiera de la República de Kirguistán me ayuda a enfrentar eficazmente estos desafíos.

Además, en el compliance, aplico activamente las habilidades adquiridas durante mi participación en la Olimpiada Internacional de seguridad financiera y la formación en el Centro de Formación de la SEIF RK, tales como el pensamiento analítico, la capacidad de tomar decisiones rápidamente y la atención al detalle. Estas cualidades son cruciales en un entorno donde el compliance se vuelve cada vez más complejo y el trabajo exige un alto nivel de profesionalismo.

Trabajando en el ámbito de PLA/FT, noto una tendencia hacia una mayor cooperación internacional. La globalización de la economía requiere de esfuerzos coordinados de todos los participantes del mercado financiero mundial. Esto significa que los especialistas en PLA/FT no solo deben estar familiarizados con la legislación nacional, sino también mantenerse al tanto de los estándares y prácticas internacionales, como las Recomendaciones del GAFI.

¿POR QUÉ MERECE LA PENA ELIGIR LA PLA/FT COMO PROFESIÓN?

Trabajar en la PLA/FT ofrece oportunidades únicas para el crecimiento y desarrollo profesional. En primer lugar, por la alta relevancia social de la profesión. Los especialistas que trabajan en PLA/FT están en la primera línea de la seguridad financiera, combatiendo a los delincuentes y detectando esquemas ilícitos, lo que garantiza la estabilidad económica.

En segundo lugar, la profesión ofrece la oportunidad de un aprendizaje y desarrollo continuos. El ámbito de la PLA/FT exige que los especialistas actualicen constantemente sus conocimientos y habilidades, lo que hace que el trabajo sea interesante, dinámico y especialmente atractivo para quienes buscan crecer profesionalmente. Cada nueva tarea representa un reto que requiere un enfoque integral y un pensamiento creativo.

Además, el campo de la PLA/FT ofrece amplias perspectivas de carrera. Los especialistas con experiencia en este ámbito son altamente valorados no solo en las organizaciones financieras, sino también en empresas de consultoría, organismos gubernamentales y organizaciones internacionales.

¿CÓMO ATRAER A LOS JÓVENES AL ÁMBITO DE LA PLA/FT?

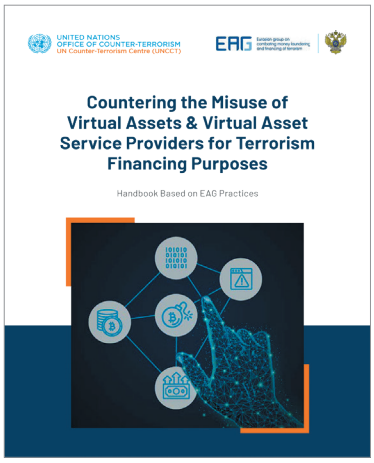
Para atraer a la juventud, es importante promover activamente las profesiones del área de lucha contra el blanqueo de dinero mediante olimpiadas, concursos y otros eventos. Otra forma eficaz es ofrecer prácticas y pasantías en organizaciones especializadas. La experiencia laboral real ayuda a comprender mejor las particularidades de la profesión y a vislumbrar oportunidades para el desarrollo futuro.

También es necesario fortalecer los programas educativos orientados a la formación de especialistas, como los que ofrece el Centro de Formación de la SEIF RK. Esto ayudará a los jóvenes a adquirir los conocimientos y habilidades necesarios para una carrera exitosa.

En conclusión, quiero decir que mi camino en la PLA/FT, desde mi participación en la Olimpiada Internacional de seguridad financiera, la formación en el CF SEIF RK y el trabajo en el Servicio Estatal de Inteligencia Financiera de la República de Kirguistán, hasta mi labor actual en el área de compliance, me ha permitido adquirir una experiencia valiosa y ha sido fundamental para mi desarrollo profesional. Esta profesión exige un aprendizaje constante y la disposición a enfrentar nuevos desafíos, pero a cambio ofrece oportunidades únicas de crecimiento personal y profesional. Es importante que los jóvenes profesionales comprendan que la PLA/FT no solo es un campo interesante y dinámico, sino también una oportunidad para contribuir de manera significativa a la seguridad y estabilidad del sistema financiero.

NOTICIAS DEL SISTEMA ANTILAVADO

NUEVA YORK:
EL PRESIDENTE DE EAG YURI CHIJANCHIN INTERVINO EN UN EVENTO DE LA ONU



En el evento se presentó la Guía para la prevención del uso de activos virtuales y proveedores de servicios de activos virtuales para el financiamiento del terrorismo, elaborada en el marco de la ONU, teniendo en cuenta la experiencia y la participación de la EAG y *Rosfinmonitoring*. Yuri Chijanchin destacó la indudable utilidad práctica del documento presentado.

MOSCÚ:
ENCUENTROS BILATERALES ENTRE ROSFINMONITORING Y COLEGAS EXTRANJEROS

Delegaciones de la Fiscalía de la República de Mozambique, la Autoridad de Responsabilidad de los Emiratos Árabes Unidos, y unidades de inteligencia financiera de Madagascar, Turkmenistán y la República Árabe Siria visitaron *Rosfinmonitoring* en visitas de trabajo.

Durante estas reuniones, la parte rusa presentó la experiencia de su sistema nacional contra el blanqueo de dinero y se discutieron temas de interés mutuo, así como agendas regionales e internacionales.

MARRAKECH:
EN LA OFICINA DE PROGRAMACIÓN DE LA ONU PARA LA LUCHA CONTRA EL TERRORISMO EN MARRUECOS TUVO LUGAR UN ENTRENAMIENTO PARA LA PREVENCIÓN DEL FINANCIAMIENTO DEL TERRORISMO

Olga Tisen, jefa del Departamento Jurídico de Rosfinmonitoring fue la encargada de impartir el entrenamiento. Se destacaron las mejores prácticas internacionales y rusas para la prevención del financiamiento del terrorismo, incluyendo el seguimiento de transacciones en criptomonedas utilizando tecnologías y logros nacionales.

EREVÁN:
EN ARMENIA TUVO LUGAR UN EVENTO FORMATIVO PARA EL INTERCAMBIO PRÁCTICO DE EXPERIENCIAS EN EL ÁMBITO DE LA PLA/FT

La formación se centró en el intercambio de experiencias sobre la construcción de un sistema nacional de PLA/FT, del estudio de las mejores prácticas de supervisión basada en riesgos, de los métodos de análisis operativo y estratégico, así como de la recopilación y procesamiento de información sobre operaciones financieras.

La delegación rusa estuvo encabezada por el jefe del Departamento de Supervisión, Alexandr Kurianov.

UZBEKISTÁN:
CONFERENCIA DE LA CEI PARA LA LUCHA CONTRA EL TERRORISMO Y CONFERENCIA CIENTÍFICO-PRÁCTICA EATR-OCS

El evento se desarrolló en formato de sesión plenaria y cinco sesiones especializadas con la participación de autoridades competentes de 20 estados miembros de la CIS y la OCS.

En la sesión plenaria, el Secretario de Estado y Subdirector de *Rosfinmonitoring*, German Neglyad, presentó un informe sobre cooperación internacional contra el terrorismo.

VIENA:
EVENTO ESPECIAL DE LA OFICNA DE LA ONU PARA LAS DROGAS Y DELINCUENCIA

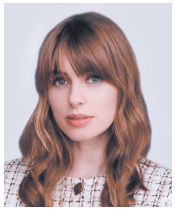
Representantes de la inteligencia financiera de Rusia participaron, mediante videoconferencia, en la presentación del Informe Mundial sobre Drogas 2024. Los participantes de la discusión subrayaron la importancia de la recopilación de datos, la realización de investigaciones y el análisis como base para el desarrollo e implementación de políticas para combatir el tráfico ilegal de drogas.

COMITÉ EDITORIAL

Presidente del Comité Editorial
Yuri Chijanchin

Vicepresidente del Comiteé Editorial
Vladimir Ovchinnikov

Vicepresidente del Comiteé Editorial
German Negliad



Editor jefe
Irina Ryazanova

MIEMBROS DEL COMITÉ EDITORIAL

Galina Bobrysheva

Ivan Kornev

Oleg Krylov

Anton Lisitsin

Sergei Teterukov

Alexei Petrenko

Evgeni Gileta

Marina Shemyakina

Rosfinmonitoring e ITMCFM en Telegram y VKontakte

Editorial
Centro Internacional de Capacitación y Métodos de Monitoreo Financiero (ITMCFM),
calle Staromonetniy pereulok, 31, edif. 1, CP119017 Moscú
c/electrónico: info@mumcfm.ru
Tirada 600 ejemplares

ITMCFM
2024