

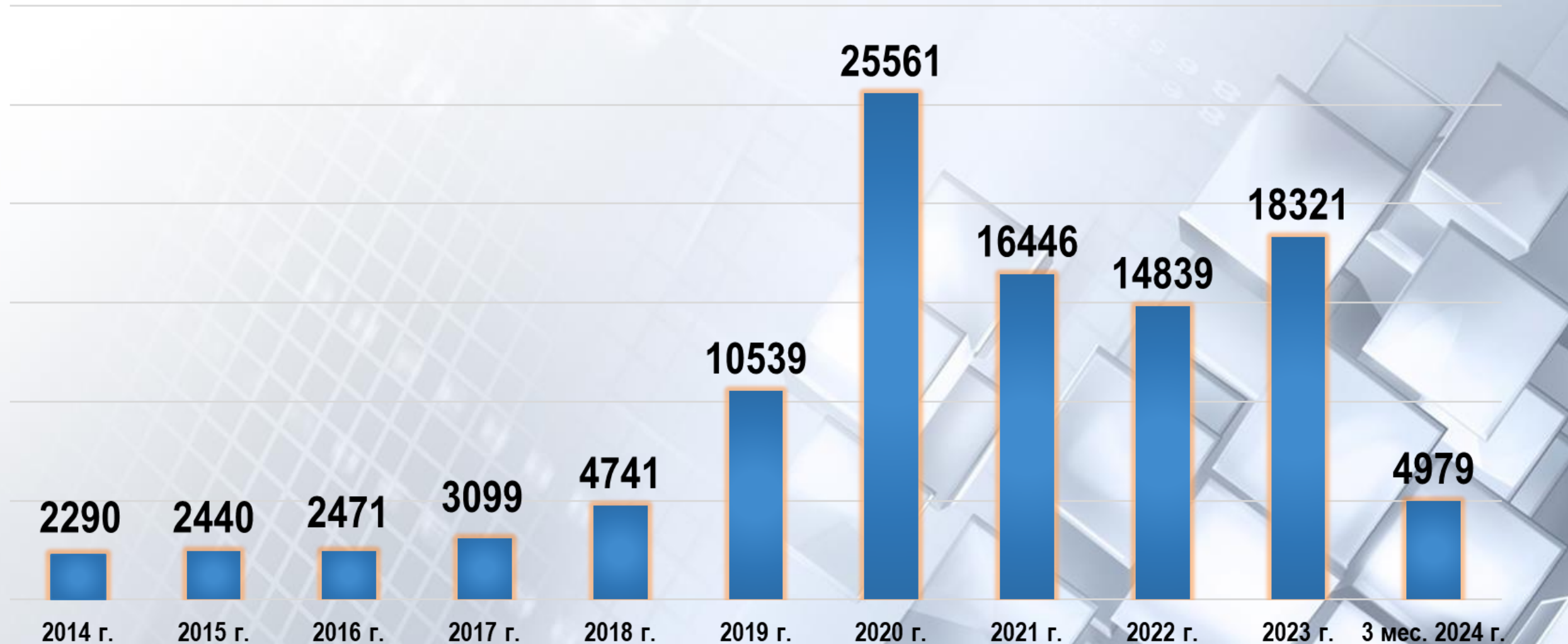


ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛАХТИКОВ ДМИТРИЙ НИКОЛАЕВИЧ
начальник кафедры
информационного права ФКМ
учреждения образования «Академия
Министерства внутренних дел
Республики Беларусь»
кандидат юридических наук, доцент
полковник милиции



Сведения о количестве зарегистрированных преступлений (ИБ) в 2014 – 2023 гг.





Сведения об удельном весе преступлений (ИБ) от общего количества регистрируемых преступлений в 2014–2023 гг.





ТРАНСФОРМАЦИЯ ПРЕСТУПНОСТИ

изменение
механизма
совершения
преступления
(использование
информационно-
коммуникационных
технологий
при
подготовке,
совершении,
сокрытии
преступлений)

1. Развитие дистанционных способов совершения

- отсутствие непосредственных контактов;
- развитие торговых площадок в Даркнет;
- социальная инженерия.

2. Анонимизация

- использование VPN и др. технологий;
- подмена (сокрытие) цифровых следов.

3. Использование виртуальных активов в криминальных расчетах

- легализация (отмывание) преступных доходов;
- дистанционный сбыт запрещенных к обороту объектов;
- мошенничество, вымогательство.

4. Использование зарубежной сетевой инфраструктуры

- сокращение международной правовой помощи;
- появление криминальных «анклавов».

5. Формирование криминального рынка услуг «преступление как услуга»

- аренда ботнетов;
- реклама услуг в Telegram и Даркнет-форумах.

6. Использование технологий искусственного интеллекта

- технологии синтеза изображений;
- технологии синтеза речи.



Указ

Президента Республики Беларусь

29 августа 2023 г. № 269

г. Минск

О мерах по противодействию несанкционированным платежным операциям

В целях предупреждения, выявления несанкционированных операций на платежном рынке Республики Беларусь и противодействия им:

1. Установить, что Национальный банк организует информационное взаимодействие между правоохранительными органами и поставщиками платежных услуг по обмену информацией о несанкционированных платежных операциях и попытках их совершения (далее – инциденты).

Сбор, получение, систематизация, накопление, хранение, изменение, обезличивание, блокирование, использование, передача, предоставление, распространение, удаление, иная обработка информации об инцидентах, включающая сведения, составляющие банковскую тайну, и персональные данные, осуществляются посредством автоматизированной системы обработки инцидентов Национального банка (далее – АСОИ) с соблюдением требований законодательства об информации, информатизации и защите информации, в том числе о персональных данных.

Передача информации об инцидентах Национальному банку от поставщиков платежных услуг осуществляется посредством АСОИ. Поставщики платежных услуг обязаны обеспечить своевременность, полноту и достоверность информации, передаваемой в АСОИ.

2. Национальный банк:

определяет виды платежных услуг, поставщики которых передают и получают информацию об инцидентах;

устанавливает для поставщиков платежных услуг состав, форму, порядок и срок передачи ими в Национальный банк информации об инцидентах, а также состав передаваемой правоохранительными органами в Национальный банк информации об инцидентах;

устанавливает состав, форму, порядок и сроки передачи Национальным банком поставщикам платежных услуг информации об инцидентах, а также состав передаваемой правоохранительным органам информации об инцидентах;

предоставляет из АСОИ поставщикам платежных услуг и правоохранительным органам информацию об инцидентах;

определяет порядок и сроки реагирования поставщиков платежных услуг на полученные посредством АСОИ инциденты и дальнейшее предоставление ими информации о результате рассмотрения инцидента в АСОИ;

заключает соглашения об информационном сотрудничестве с правоохранительными органами в части взаимного предоставления информации об инцидентах.

Поставщики платежных услуг используют информацию, получаемую из АСОИ, для противодействия несанкционированным платежным операциям.

Финансовые организации обеспечивают проверку совершения платежей на соответствие признакам несанкционированного перевода денежных средств (электронных денег), установленным Национальным банком, используя информацию, представленную им пользователями платежных услуг при осуществлении платежей, а также информацию о технических параметрах устройств, с помощью которых осуществляются эти платежи.

Правоохранительные органы имеют право передавать информацию об инцидентах, установленных в ходе своей деятельности, посредством АСОИ в Национальный банк и поставщикам платежных услуг. Правоохранительные органы используют информацию, содержащуюся в АСОИ, исключительно в рамках своих полномочий. Передача сведений из АСОИ третьим лицам запрещена, за исключением случаев, предусмотренных законодательными актами.

Информация об инцидентах из АСОИ предоставляется поставщикам платежных услуг и правоохранительным органам на безвозмездной основе.

Предоставление информации об инцидентах из АСОИ правоохранительным органам и поставщикам платежных услуг не является нарушением банковской тайны. Обработка персональных данных, содержащихся в информации об инцидентах, осуществляется без согласия физического лица.

3. Предоставить Генеральной прокуратуре, Комитету государственной безопасности, Следственному комитету и Министерству внутренних дел право на принятие решения о приостановлении на срок до 10 суток расходных операций по банковскому счету, счету по учету вкладов (депозитов), электронному кошельку пользователя платежных услуг, являющегося участником инцидента, в отношении которого у названных правоохранительных органов имеется информация (подозрения), свидетельствующая о его участии в совершении противоправных деяний.

4. Для целей настоящего Указа:

под несанкционированными платежными операциями понимаются платежные операции, которые на момент передачи информации о них в Национальный банк признаются поставщиками платежных услуг:

неавторизованными, в том числе несанкционированные переводы денежных средств (электронных денег) без согласия пользователя платежной услуги;



ПОСТАНОВЛЕНИЕ ПРАВЛЕНИЯ НАЦИОНАЛЬНОГО БАНКА
РЕСПУБЛИКИ БЕЛАРУСЬ
15 декабря 2023 г. № 453

**О несанкционированных переводах денежных средств
(электронных денег)**

выявления признаков несанкционированного перевода;

1.2. при выявлении признаков несанкционированного перевода, перечисленных в абзацах втором–четвертом части первой подпункта 1.1 настоящего пункта, приостановление перевода по платежу пользователя платежной услуги осуществляется финансовой организацией, заключившей с этим пользователем платежной услуги договор на оказание платежных услуг, в следующем порядке:

при наличии технической возможности исполнение платежной инструкции (платежного указания) **приостанавливается на срок не более двух рабочих дней** (без учета дня инициации перевода)

платежной
и в порядке
перевода
возобновляе

1.3. поставщики платежных услуг, оказывающие платежные услуги, указанные в абзацах втором–девятом статьи 9 Закона Республики Беларусь «О платежных системах и платежных услугах», предоставляют в электронном виде в Национальный банк посредством АСОИ информацию об инцидентах в течение одного часа с момента их выявления в режиме 24/7 в соответствии с информационной технологией одним из следующих способов:

- личный кабинет;
- открытые интерфейсы программирования приложений;

1.4. поставщики платежных услуг предоставляют информацию о результате рассмотрения инцидента, полученную посредством АСОИ от правоохранительных органов или иных поставщиков платежных услуг, в течение одного часа с момента получения в режиме 24/7 с дальнейшим предоставлением информации по ним в АСОИ;

1.5. Национальный банк предоставляет информацию об инцидентах из АСОИ четыре раза в сутки в соответствии с информационной технологией поставщикам

ублики Беларусь
услугах» и части
е Национального

онных денег) без
кционированного

льпате которого



Правовые основы функционирования АИС «ГУПК» и АСОИ

1. Указ Президента Республики Беларусь № 269 от 29.08.2023 «О мерах по противодействию несанкционированным платежным операциям»;
2. Постановление Правления Нацбанка Республики Беларусь № 453 от 15.12.2023 «О несанкционированных переводах денежных средств (электронных денег)»;
3. Постановление Правления Нацбанка Республики Беларусь № 454 от 15.12.2023 «О предоставлении информации об инцидентах и нарушениях безопасности в сфере защиты информации»;
4. Приказ МВД Республики Беларусь от 17.03.2022 № 64 «О функционировании автоматизированной информационной системы «ГУПК»
5. Приказ МВД Республики Беларусь от 27.02.2024 № 43 «О порядке взаимодействия по обмену информацией о несанкционированных платежных операциях».



Схема обмена информацией о подозрительных операциях посредством АИС «ГУПК» и АСОИ

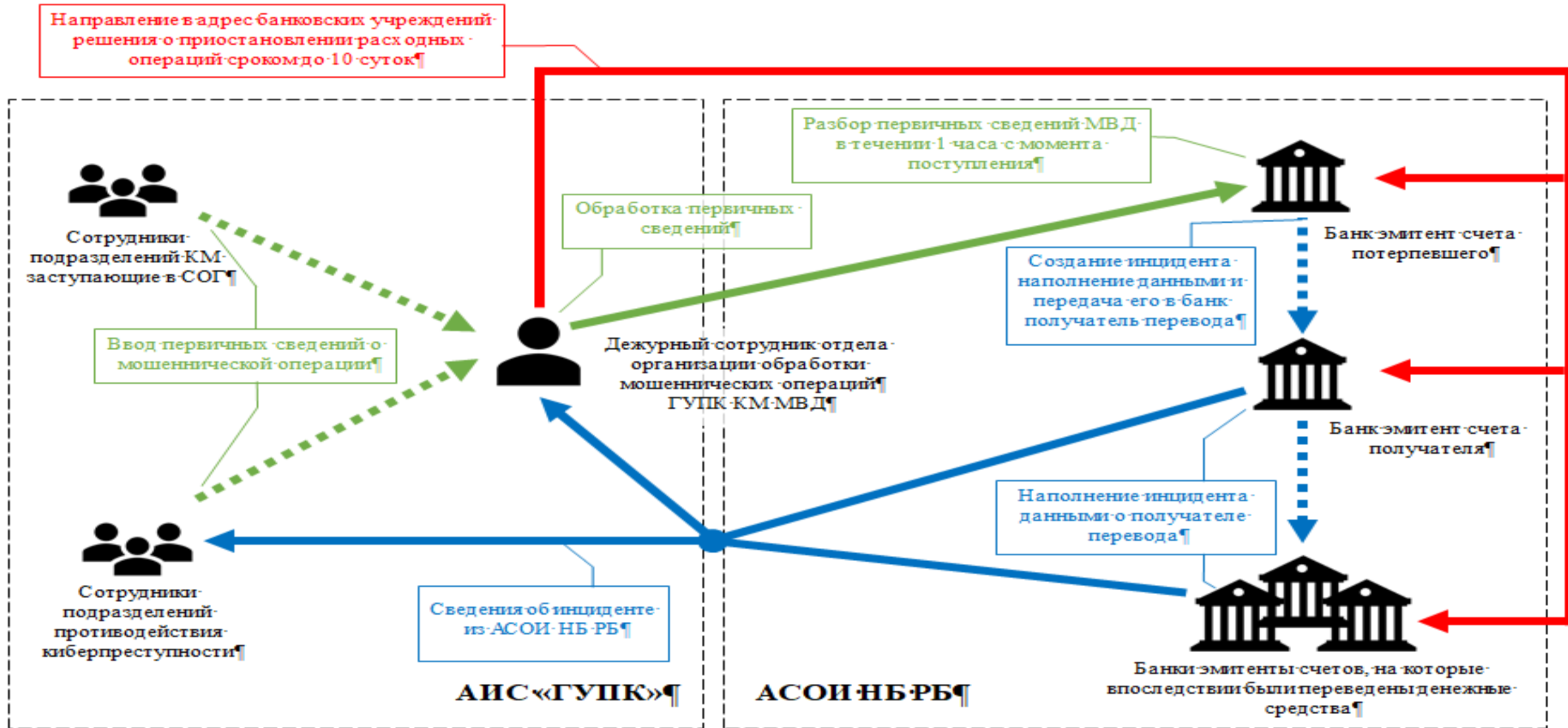
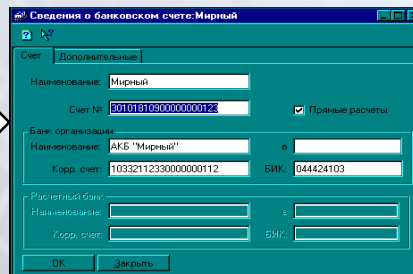
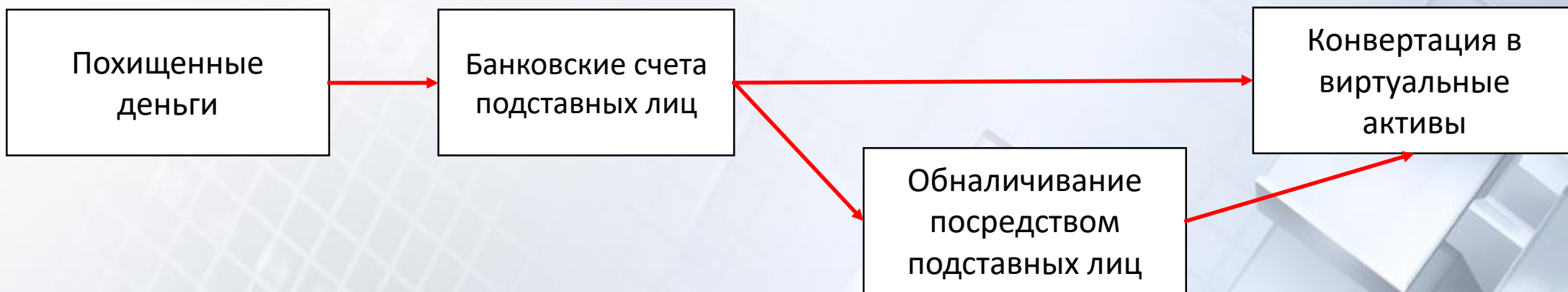




СХЕМА ВЫВОДА ПОХИЩЕННЫХ ДЕНЕЖНЫХ СРЕДСТВ



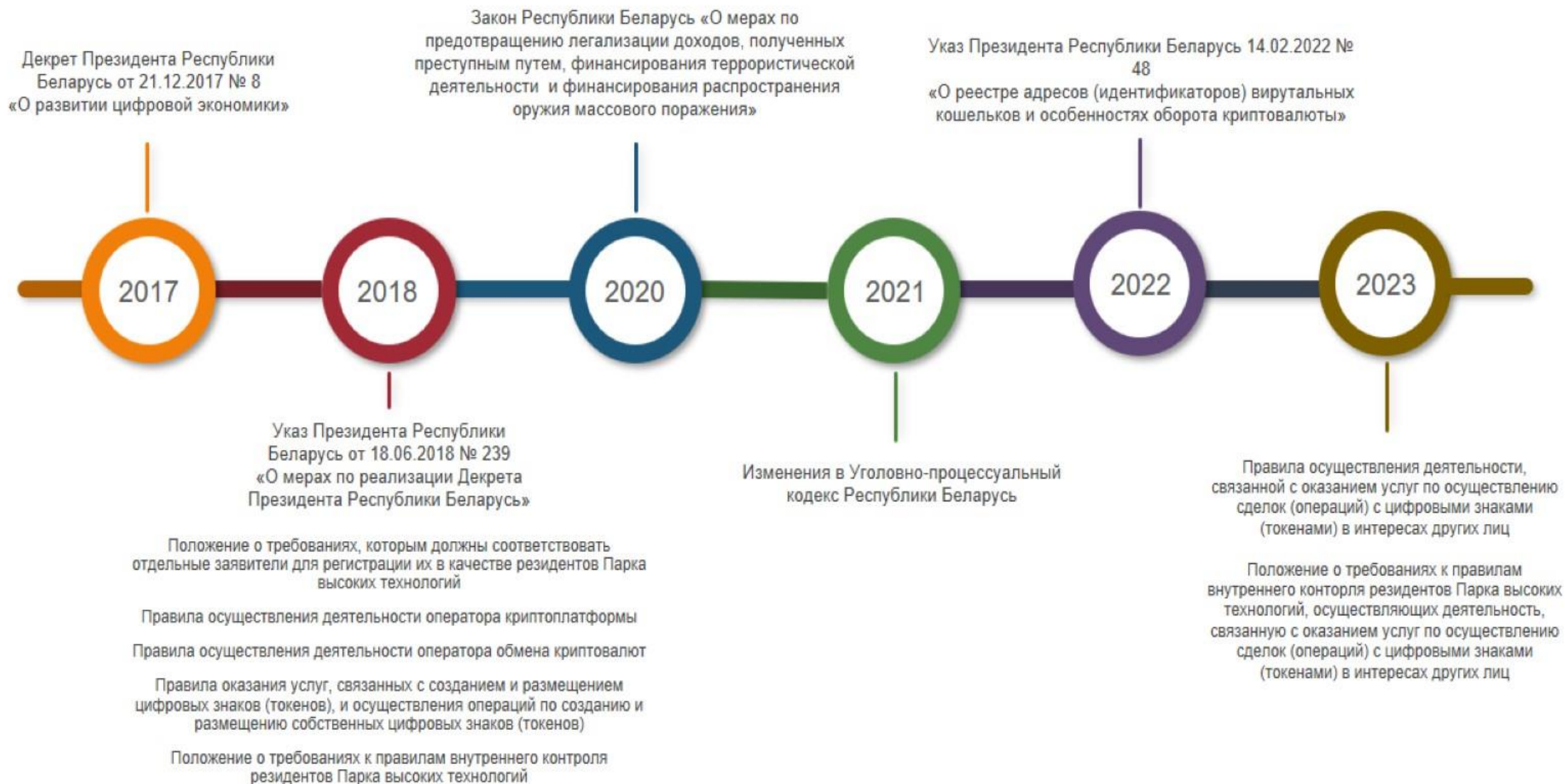


ПРАВОВОЕ РЕГУЛИРОВАНИЕ

- Закон Республики Беларусь «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения»
- Декрет Президента Республики Беларусь «О развитии цифровой экономики»
- Указ Президента Республики Беларусь «О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты»



Развитие системы правового регулирования сферы токенов





ТЕХНОЛОГИИ, ОБЛЕГЧАЮЩИЕ СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ АКТИВОВ

масштабное применение криптомиксеров

использование анонимных криптобанкоматов

использование теневых ПУВА

совершение операций напрямую без ПУВА

использование анонимных виртуальных активов

использование подменных IP-адресов

конспирация преступной деятельности в рамках общего пула транзакций



АНАЛИТИЧЕСКАЯ ФИНАНСОВАЯ РАЗВЕДКА





**РАЗВИТИЕ ПРАВОВЫХ
МЕХАНИЗМОВ
УСЛОЖНЕНИЯ
ФИНАНСИРОВАНИЯ
ПРЕСТУПНОЙ
ДЕЯТЕЛЬНОСТИ,
ЛЕГАЛИЗАЦИИ
ДЕНЕЖНЫХ
СРЕДСТВ,
ПОЛУЧЕННЫХ
ПРЕСТУПНЫМ
ПУТЁМ, В ТОМ ЧИСЛЕ
В ВИДЕ
ВИРТУАЛЬНЫХ
АКТИВОВ**

преступная деятельность: финансовое обеспечение (как в самом начале, так и процессе ее осуществления)

за непродолжительное время денежные средства могут быть переведены с выявленного счета (кошелька)

основные меры принимаются в рамках уголовного дела

распространение правовых механизмов на более ранние этапы



СХЕМА ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ ПУТЕМ ПЕРЕВОДОВ P2P



Осуществление сделок по обмену виртуальных активов на иностранной криптобирже

Предлагается:

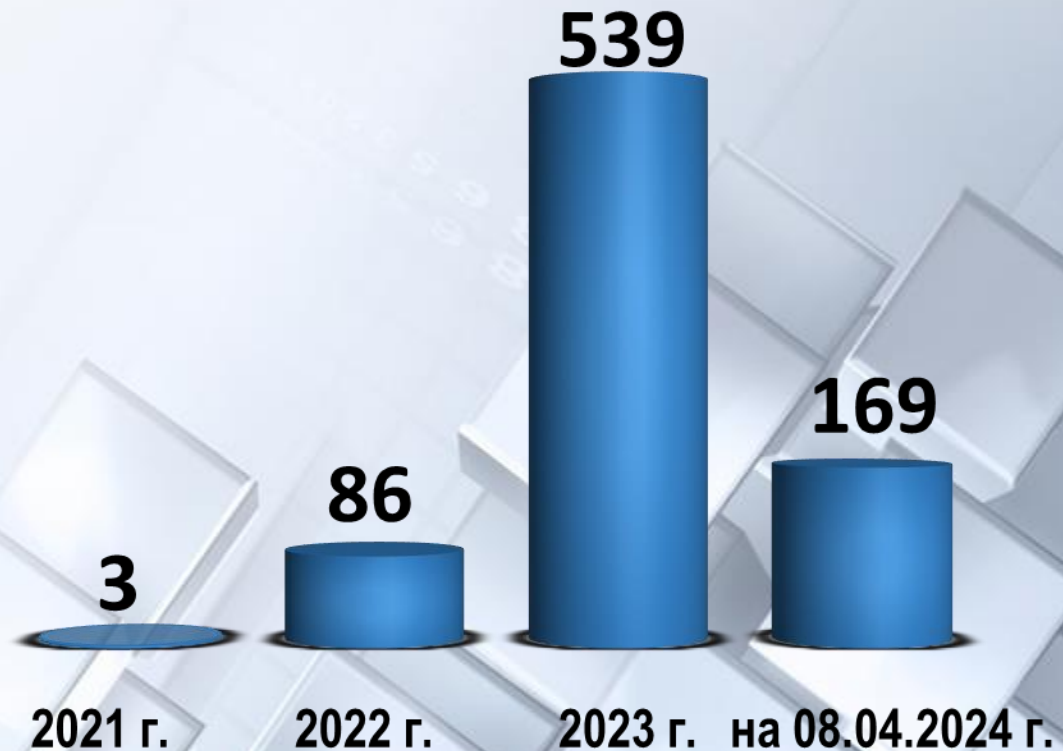
исключить возможность для физических лиц осуществлять P2P транзакции на зарубежных ПУВА



Сведения о количестве возбужденных уголовных дел по ст. 222 УК в 2021-2023 гг. и по состоянию на апрель 2024

Статья 222. Незаконный оборот средств платежа и (или) инструментов (УК)

Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам.



СТАТЬЯ 13.3. НЕЗАКОННАЯ ПРЕДПРИНИМАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ (КоАП)

3. Осуществление предпринимательской деятельности, когда в соответствии с законодательными актами такая деятельность является незаконной и (или) запрещается.



МЕРЫ

смещение акцента и реализация более широкого спектра мер защиты на уровне интернет-провайдеров, хостинг-провайдеров, криптобирж, а не на уровне конечного пользователя (например, физическое лицо, организация)

межгосударственный обмен опытом и взаимное **оказание правовой помощи**, направленной на **выявление, замораживание, арест и изъятие** цифровых финансовых активов

выработка норм, позволяющих **использовать изъятые цифровые финансовые активы**, (например, органами государств-участников соглашения), находящимися в распоряжении криптобиржи, для совершения транзакций с криптобиржами государств-участников соглашения без «понижения рейтинга» криптобиржи

выработка механизма по **оперативному блокированию транзакций** по обороту цифровых финансовых активов и других финансовых операций

совершенствование подходов при **определении идентификаторов сомнительных транзакций**

совершенствование и внедрение новых технологий **противодействия анонимизации** субъектов криптопреступности

оперативный **обмен достоверной информацией**, касающейся **сомнительных трансграничных операций** с использованием цифровых финансовых активов

комплексный **информационный ресурс**, специально посвященный противодействию преступности в области информационной безопасности



Факультет криминальной милиции

Повышение профессиональных навыков обучающихся по направлению
«Противодействие киберпреступлениям и компьютерная разведка»



Учебные дисциплины на базе БГУИР:
«Компьютерные системы и сети»
«Архитектура компьютерных сетей»
«Защита информационных сетей»

13 мая 2023 года подписан договор
о сетевом взаимодействии с БГУИР

Группа – 30 человек





ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛАХТИКОВ ДМИТРИЙ НИКОЛАЕВИЧ
начальник кафедры
информационного права ФКМ
учреждения образования «Академия
Министерства внутренних дел
Республики Беларусь»
кандидат юридических наук, доцент
полковник милиции