

Новые цифровые бизнес-модели, в основе которых лежит использование цифровых данных на всех этапах жизненного цикла продуктов, реализуются в рамках процессов цифрового производства.

Таким образом, процесс внедрения цифровых информационных технологий способствует появлению новых бизнес-моделей, оптимизирующих бизнес, и получению конкурентных преимуществ.

#### Источники

1. Китова, О. В. Модели и технологии цифровой трансформации предприятий / О. В. Китова // Цифровизация общества: состояние, проблемы, перспективы : материалы VI Всерос. науч.-практ. конф. — М. : РЭУ им. Г. В. Плеханова, 2019. — С. 102–108.

2. Акинфина, М. А. Перспективы использования цифровых технологий в деятельности предприятий / М. А. Акинфина // Экономический рост Республики Беларусь: глобализация, инновационность, устойчивость : материалы XIII Междунар. науч.-практ. конф., Минск, 16 мая 2020 г. / Белорус. гос. экон. ун-т ; редкол. : В. Ю. Шутилин (пред.) [и др.]. — Минск, 2020. — С. 367–368.

**А. В. Антоневиц**, магистр экон. наук  
*andreykaantonevich@gmail.com*  
ОАО «Белагпропромбанк» (Минск)

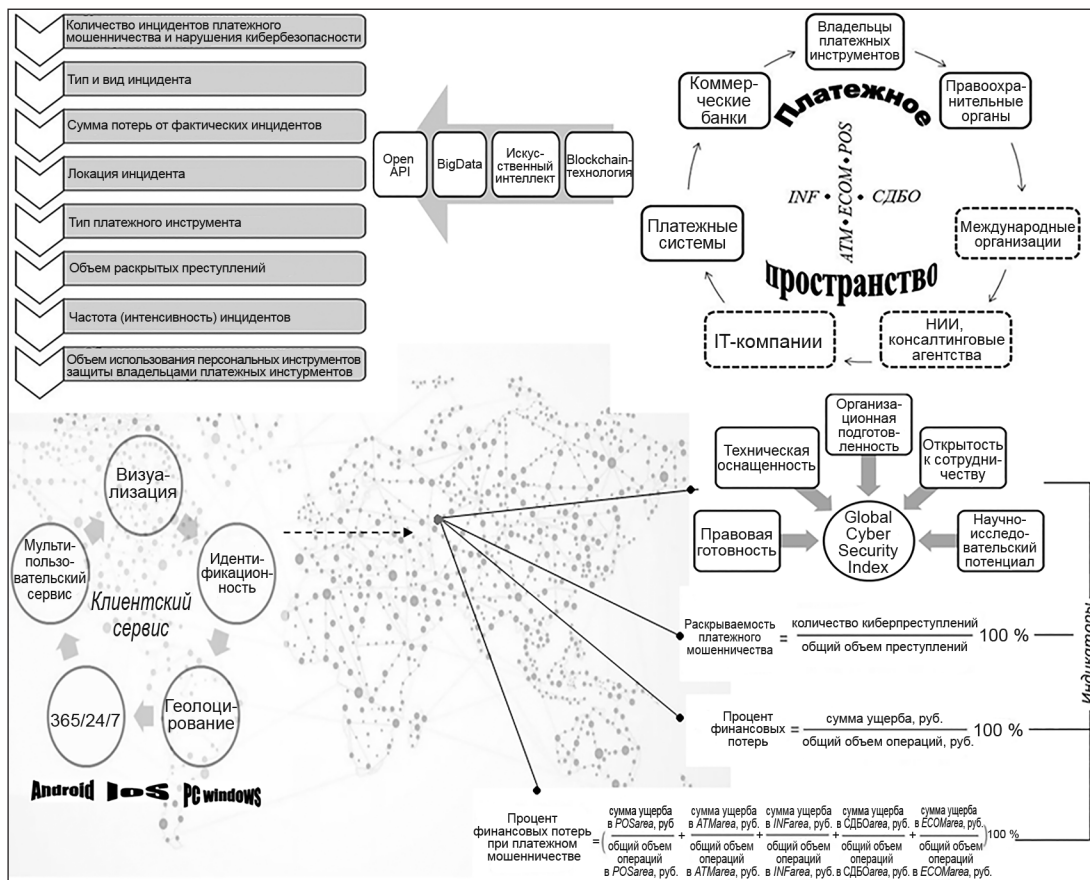
## ПЕРСПЕКТИВНЫЕ МЕХАНИЗМЫ И ТЕХНОЛОГИИ МИНИМИЗАЦИИ РИСКОВ МОШЕННИЧЕСТВА В ПЛАТЕЖНОМ КИБЕРПРОСТРАНСТВЕ

В современном цифровом пространстве несанкционированные действия злоумышленников (киберпреступность, кардинг), в том числе в платежном сегменте, являются ключевой угрозой экономического роста не только отдельных стран, регионов, но и мировой экономики в целом. Важная роль в борьбе с платежным мошенничеством наряду с правовыми, организационными и техническими мерами принадлежит сбору, накоплению, хранению сведений об инцидентах нарушения кибербезопасности и платежном мошенничестве, а также информационному обмену между всеми заинтересованными участниками (владельцы платежных инструментов, коммерческие банки, органы правоохранительной системы, разработчики программного обеспечения, научно-исследовательские, консалтинговые и рейтинговые агентства, международные организации, ассоциации, объединения, поставщики оборудования и др.) на локальном, государственном, региональном и глобальном уровнях.

В рамках построения глобальной экосистемы противодействия киберугрозам и мошенничеству в платежном пространстве значимым элементом является система индикативных виджетов с функцией оперативного оповещения. Существует множество индикативных показателей (простых и интегрированных), исчисляемых как в абсолютном, так и в относительном выражении с учетом действующих общемировых правил, подходов, лучших практик, применяемых в борьбе с платежным мошенничеством и киберпреступностью, среди которых: количество киберинцидентов и угроз платежного мошенничества, в том числе в каждом конкретном сегменте платежного пространства; суммы потерь, в том числе в общем объеме расходных операций, осуществляемых в платежном пространстве; интегрированный индекс кибербезопасности и др.

Следует отметить, что перспективным направлением по минимизации рисков и последствий, возникающих при осуществлении злоумышленниками несанкционированных действий, их заблаговременному предотвращению в платежном пространстве являются разработка, внедрение и функционирование специализированного клиентского сервиса-

приложения (для Android, Ios, PC Windows и др.) на базе глобальной мультипользовательской антитрод-платформы (см. рисунок). В развитие данного сервиса для клиентов могут быть активированы дополнительные гаджеты, например такие, как финансовый геолокатор и/или техническо-консалтинговый суппоринг и др. Банки в рамках предоставления такого сервиса смогут более оперативно реагировать на возникающие угрозы, повышать клиентскую финансовую киберграмотность и лояльность к бренду и др.



Архитектура пользовательской модели клиентского сервиса

Источник: собственная разработка автора.

Реальная апликация держателями платежных инструментов данного сервиса при осуществлении расчетов в платежном пространстве позволяет в режиме реального времени заблаговременно ознакомиться с фактическим уровнем безопасности их проведения в том или ином регионе или стране, а в случае путешествия, особенно за границу, с учетом геолоцирования и пользовательской поддержки получить рекомендации по безопасному осуществлению транзакций с применением платежных инструментов.

Таким образом, реализация в ближайшей перспективе предложенного решения по борьбе с возникающими инцидентами несанкционированных действий злоумышленников в отношении держателей платежных инструментов позволит минимизировать риски, вырабатывать и применять оптимальные и оперативные решения и инструменты по их устранению, а также будет способствовать развитию безналично-цифровой экономики.