

УДК 004.418

ВЛИЯНИЕ БИОМЕТРИИ НА РЕЗУЛЬТАТИВНОСТЬ ЭКОНОМИКИ:
ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Котилко Валерий Валентинович,

доктор экономических наук, проф.,

академик РАЕН, главный научный сотрудник,

СОПС (г. Москва, Россия)

Аннотация: Статья посвящена проблемам и трудностям внедрения биометрии с позиций экономического эффекта и безопасности

Ключевые слова: Будущее биометрии, трансформирующие технологии, биометрические данные, единая система, утечка биометрических образцов, сферы применения, Единой биометрической системы, показатели результативности.

THE IMPACT OF BIOMETRICS ON ECONOMIC PERFORMANCE:
SECURITY ISSUES

Kotilko V. V. - Doctor of Economic Sciences, prof.,

Academician of the Russian Academy of Natural Sciences, chief researcher,

SOPS (Moscow, Russia)

Abstract: The article is devoted to the problems and difficulties of introducing biometrics from the standpoint of economic effect and security

Key words: The future of biometrics, transformative technologies, biometric data, unified system, leakage of biometric samples, areas of application, Unified Biometric System, performance indicators.

Развитие системы оплаты по биометрическим данным могло бы перевести Россию на новый экономический уровень, рассказал экономист Петр Заборцев. По его словам, эта технология в ближайшее время может появиться в финансовом и транспортном секторах, а также в торговле. Эксперт убежден, что подобные тенденции необходимо поддерживать всеми силами, даже если в итоге это окажется бесполезным, так как они способны создать новые формы

организации труда, пишет ФБА «Экономика сегодня». Экономист и предприниматель уточнил, что трансформирующие технологии — это «путь в будущее» для России. При этом эксперт добавил, что властям важно подготовить страну к изменениям на рынке труда, так как использование оплаты по биометрии еще больше усилит тенденцию на создание торговых точек с минимальным количеством кассиров и персонала.

Замглавы думского комитета по информационной политике Антон Горелкин в своем Telegram-канале опроверг слухи о введении в России обязательной сдачи биометрических данных. Он подчеркнул, что у властей таких планов нет, а также разъяснил суть внесенного в Госдуму законопроекта о правовых основах обработки биометрических данных.

Ранее в Минцифры также заявляли, что сбор биометрических данных россиян в единую систему (ЕБС) будет проводиться только с их согласия. В ведомстве подчеркнули, что будут тщательно следить за тем, чтобы при переносе данных из коммерческих систем в ЕБС граждане обязательно получали уведомления и могли по своему желанию потребовать их удаления. Защита будет организована на самом высоком уровне, за этим проследят ФСБ и ФСТЭК (Федеральная служба по техническому и экспортному контролю).

Коммерческими организациями уже собрано более 60 миллионов биометрических образцов. Государство не может допустить, чтобы случилась их утечка, и берет предоставление и хранение биометрии под свой контроль. Защита будет организована на самом высоком уровне, за этим проследят ФСБ и ФСТЭК. Коммерческий сектор будет оперировать не изображениями, не записью голоса граждан, а векторами – математически обработанными данными, из которых невозможно восстановить биометрические образцы. И, подчеркну, граждане имеют право отказаться от передачи биометрии в ГИС ЕБС.

И наконец, биометрия военных и сотрудников спецслужб не сдается в принципе, это запрещено внутренними приказами. А про отследить по

биометрическим образцам местоположение человека в режиме реального времени – это кто-то посмотрелся фантастических фильмов.

Зампредседателя комитета Госдумы по информационной политике Антон Горелкин перед пленарным заседанием заявил: «Компании обязаны будут незамедлительно реагировать на утечки данных в течение 24 часов и сообщать Роскомнадзору, уполномоченному органу о факте утечки, ответственных лицах и принятых мерах. Организациям и операторам персональных данных будет запрещено отказывать гражданам в предоставлении услуг, даже если гражданин по каким-то своим причинам не хочет давать согласие на обработку персональных данных, на их передачу третьим лицам. Каждая передача данных россиян за рубеж должна будет согласовываться с Роскомнадзором в сочетании с принципом экстерриториальности — это усилит защиту данных россиян за рубежом. Роскомнадзор будет вправе вмешиваться в зарубежный сегмент сети и решать вопрос незаконной обработки данных зарубежными ресурсами», - сказал он.

Антон Горелкин обратил внимание на участвовавшие случаи утечек персональных данных из разных компаний — это является нарушением конституционного права на частную жизнь.

Минцифры будет тщательно следить за тем, чтобы при переносе данных из коммерческих систем в ЕБС граждане обязательно получали уведомления и могли по своему желанию потребовать прекращения хранения данных в ЕБС и их удаления. Сама сдача биометрии также не будет носить обязательного характера.

Ранее «Коммерсант» сообщил, что разработанные Минцифры поправки к правилам сбора биометрии допускают отказ от необходимости получать согласие гражданина на передачу его биометрии в единую биометрическую систему из различных источников. По мнению авторов материала, в министерстве полагают, что это укрепит защищенность данных, а использовать их сможет только разместившая организация. По оценкам экспертов, отказ от

получения согласия гражданина на сбор и актуализацию биометрии может привести к тому, что она будет собираться непрерывно из любых возможных источников, включая камеры наблюдения, а последствия утечки данных могут оказаться катастрофическими.

Биометрия — ключ к удобным и простым потребительским и бизнес-сервисам, говорят эксперты. Основные сферы применения — госуслуги, телеком, транспорт, финансовый сектор, ретейл, образование, здравоохранение, миграционный контроль. В мировой практике биометрические технологии задействуют для обеспечения безопасности, доступа на объекты, противодействия мошенничеству, идентификации пользователя при совершении платежей, отмечают в пресс-службе Банка России. Ключевые модальности, используемые в системах разных стран, — лицо, отпечатки пальцев и ладони, рисунок вен, голос, радужная оболочка глаза.

По оценкам компании «Центр биометрических технологий» (ЦБТ), на сегодня объем мирового рынка биометрии достигает \$33–35 млрд, прогноз на конец текущего десятилетия — \$80–100 млрд.

Как регулируется биометрия в России.

В России сбор и обработка биометрических данных коммерческими организациями так или иначе осуществлялись довольно давно, говорит глава Национального совета финансового рынка (НСФР) Андрей Емелин: «Была совокупность коммерческих систем, которые работали на основании закона о персональных данных, допускающего при наличии специального согласия клиента сбор биометрии: фото, голоса, отпечатков пальцев, рисунка сетчатки глаза».

Но в регулируемые рамки биометрия попала лишь в конце 2017 года, после принятия соответствующего закона (482-ФЗ). В 2018-м по инициативе Минцифры была создана Единая биометрическая система (ЕБС), которая в конце 2021 года получила статус государственной информационной системы (ГИС), — Единая система идентификации и аутентификации физических лиц с

использованием биометрических персональных данных. В 2022-м постановлением правительства России оператором системы была назначена компания «Центр биометрических технологий», учрежденная Минцифры, ЦБ и «Ростелекомом».

К тому моменту к ЕБС были обязаны подключиться все кредитные организации страны. В качестве официально признаваемых и подлежащих верификации модальностей была выбрана совокупность голоса и изображения лица человека, для снятия «слепков» которых банкам надлежало закупить специальное оборудование, создать в офисах звукоизолированные помещения и обеспечить защищенные коммуникации.

В тоже время до сих пор не утверждены показатели результативности биометрии. Наиболее типичные подходы к проблеме эффективности решаются с помощью следующих методических приемов:

- оценивается эффективность затрат на управление производством и сферой услуг;
- эффективность управления сводится к показателям и критериям эффективности производства и сферы услуг, либо к доле какого-либо показателя, принятого за обобщающий;
- сравниваются показатели, характеризующие управляющую и управляемую подсистемы;
- путем соотношения целей и результатов;
- оценивается эффективность управленческих решений;
- через оценку эффективности управленческого труда;
- ориентируясь на методы оценки эффективности использования новой техники и капитальных вложений, а также на эффективность внедрения инноваций

Общим для всех существующих методик является использование главных показателей - таких как: рентабельность, трудоемкость функций управления, балансовая прибыль, реализованная продукция, соотношение результатов и

полученного эффекта. В результате практически невозможно сравнить эффективность деятельности аппарата в различных отраслях и сферах. Кроме того, эти методики даже не ставят задачу создания адаптивного механизма, позволяющего снизить негативные последствия от факторов-риска.

Все эти показатели характеризуют в совокупности степень приближения к эффективному управлению. В то же время в качестве исходной информации, характеризующей основные параметры управления эффективностью работы предприятия, должны использоваться следующие показатели:

- объем производства продукции (в том числе основное и побочное производство);
- валовой доход (основное и побочное производство);
- себестоимость продукции (основное и побочное производство);
- добавленная стоимость (основное и побочное производство);
- материалоемкость продукции;
- энергоемкость продукции;
- чистый доход;
- зарплатоемкость продукции, работ и услуг;
- балансовая прибыль;
- чистая прибыль.

Нельзя внедрить методы адаптивного управления рисками, оказывающих прямое и косвенное воздействие на результативность экономики через биометрию без выявления угроз, рисков и оценки безопасности работы предприятия или в рассматриваемом случае Единой биометрической системы (ЕБС). Реализовать идею адаптивного управления на практике (далее будем рассматривать термин предприятие, полагая, что под ним подразумевается ЕБС) можно только поэтапно, последовательно двигаясь к намеченной цели от классификации потенциальных и реальных угроз (с одной стороны) до реализации концепции экономической безопасности и эффективности ее

применения в рамках предлагаемого нами к реализации адаптивного менеджмента.

Этапы эффективного управления системой, через реализацию концепции безопасности предприятия в условиях функционирования адаптивного менеджмента, включают следующие шаги:

I шаг - оценка состояния предприятия и системы его управления с позиций способности реагирования на меняющиеся условия хозяйствования;

II шаг - ранжирование потенциальных и реальных угроз, классификация факторов риска (по степени значимости, величине ущерба, причинам угроз, негативным последствиям, размеру возможного ущерба);

III шаг - цель экономической безопасности и адаптивного менеджмента предприятия (формулировка задач, направлений стратегии, сценариев перспективного развития, разработка плана мероприятий по повышению эффективности управления в рамках категорий теорий рисков, адаптивного менеджмента, безопасности функционирования предприятия или сферы услуг);

IV шаг - построение системы экономической безопасности и внедрения адаптивного механизма на предприятии в условиях неопределенности (внешние и внутренние угрозы, их фиксация, предварительная оценка последствий, выработка механизма противостояния, снижение (предупреждение) ущерба, эффективность работы аппарата управления);

V шаг - разработка методики оценки рисков, состояния безопасности, способности органов управления своевременно реагировать на внешние и внутренние угрозы, группировка последствий и оценка слияния ущерба от рисков на эффективность управления предприятием, отбор показателей, характеризующих результативность работы предприятия и органов управления с адаптационных позиций;

VI шаг - учет влияния конкурентоспособности, производственной деятельности и сферы сбыта на способность предприятия адаптироваться к

внешним и внутренним условиям, факторам-риска и угрозам, снижающим эффективность работы аппарата управления предприятия;

VII шаг - определение размеров различных видов ресурсов, способов адаптации, нацеленных на снижение возможных негативных последствий факторов риска (материально-технических, финансовых, энергетических, кадровых, информационных ресурсов, средств защиты, финансовых затрат, необходимых для безопасности предприятия и эффективной работы органов управления предприятия);

VIII шаг - разработка мер по реализации концепции безопасности предприятия и внедрения адаптационного менеджмента для достижения безопасности:

- определение условий, целей, задач, функций и ожидаемых результатов;
- поиск источников ресурсного обеспечения;
- выделение финансовых средств для реализации «концепции» и повышения эффективности адаптационного менеджмента;
- разработка программы развития предприятия, включающей основные положения концепции безопасности, классификация угроз и факторов возможного риска, целей и задач внедрения адаптационного менеджмента на предприятии;
- контроль за эффективностью и своевременностью реализации концепции безопасности и результативностью внедрения адаптационного менеджмента;

IX шаг - анализ хода и результативности реализации концепции безопасности, ликвидация последствий действия факторов риска, оценка конкретных результатов после внедрения адаптационного менеджмента (в разрезе подразделений, рабочих мест, предприятия в целом, в работе с поставщиками, с позиций борьбы с конкурентами, в рамках защиты предприятия от различных угроз и посягательств).

Среди названных шагов решения проблемы эффективности предприятия с позиций безопасности предприятия (и среды и функционалов пользователя)

наименее проработанной и дискуссионной является проблема эффективности методов управления рисками. Она связана с проблемой совместимости различных предлагаемых классификаций рисков и факторов риска, а также с проблемой моделирования процессов управления рисками.

Следует правильно оценивать множество классификаций рисков, влияющих на результативность: чем их больше, тем сложнее процесс управления рисками, а, следовательно, труднее оценить эффективность этой работы.

Итак, анализ методов, показателей и критериев, применяемых на практике приемов оценки эффективности управления предприятием, позволил выявить сферы, которые оказывают достаточно сильное влияние на этот процесс, но которые почти не задействованы в рекомендуемых методических рекомендациях. Исходя из этого, в ходе поиска методических подходов к учету рисков при реализации и внедрении биометрии следует обратить внимание на такие аспекты внедрения адаптивного менеджмента, как совершенствование методов анализа и оценки рисков, а также поиск направлений адаптивного управления рисками при разработке конкурентной стратегии предприятия или объекта сферы услуг.

Учитывая условия неопределенности от внедрения биометрии, возможные риски от нарушения сроков ее реализации и возможного ущерба для экономической безопасности страны предлагаем разработать стратегию ее внедрения с поэтапной оценкой ее результативности и эффективности.

План включает информацию о сроках выполнения Стратегии и об ответственных исполнителях, обеспечивающих реализацию ее мероприятий.

Реализация I этапа плана характеризуется необходимостью нивелирования негативного воздействия от реализации биометрии в условиях неопределенности и возникающих рисков без оценки от получаемого эффекта.

На I этапе реализации плана должно быть осуществлено:

установление эффективной коммуникации с различными целевыми аудиториями для адресной мотивации населения, формирование потребности в активности у всех категорий населения;

обеспечение в рамках создаваемой Единой системы биометрии специальностей в вузах для подготовки специалистов в этой сфере на основе разработки и реализации дополнительных общеобразовательных программ для различных отраслей и регионов, а также методик оценивающих эффект от их внедрения на разных этапах реализации стратегии;

создание межотраслевой и межрегиональных систем, позволяющих комплексно мониторить результативность внедрения биометрии;

формирование и проработка мер по стимулированию развития отечественных форм биометрии и программ их программного обеспечения, опираясь на отечественные методы защиты информации.

На II этапе реализации плана предполагается адаптация системы российской системы биометрии под новые условия функционирования, сформировавшейся под влиянием различных вызовов, связанных с экономической и геополитической обстановкой, в том числе:

- проработка возможностей изменения законодательства с целью увеличения объема и числа источников бюджетного и внебюджетного финансирования;
- формирование механизма реализации необходимых мер экономического стимулирования внедрения биометрии;
- совершенствование инструментов системы бюджетирования деятельности субъектов, ориентированных на внедрение биометрии;
- совершенствование методик планирования и прогнозирования для различных отраслей и регионов;
- доработку законодательства в области биометрии, в том числе относящихся к нацпроектам;

- внедрение автоматизированных систем управления и защиты информации, используемых в системах биометрии.

На III этапе реализации плана предполагается использование эффекта от развития и мониторинга результативности биометрии на предыдущем этапе, активное содействие повышению качества жизни, качества работы и усиления методов защиты информации в ходе создания единой системы биометрии.

Итак, результативность биометрии должна оцениваться тремя группами показателей: безопасности, рисков и защиты информации.

ЛИТЕРАТУРА

1. Заборцев П. Экономист оценил влияние оплаты по биометрии на российскую экономику. 30 ноября 2022. // ФБА «Экономика сегодня».
2. Горелкин А. «Единая Россия» обеспечит новые меры защиты персональных данных, 24 мая 2022. Думский комитет по информационной политике.
3. Емелин А. Самиев П.А. Биометрические технологии: большой провал или большая надежда. 26 марта 2024. РБК.
4. Катмаков, П. С. Биометрия: учебное пособие для вузов / П. С. Катмаков, В. П. Гавриленко, А. В. Бушов ; под общей редакцией П. С. Катмакова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 186 с.
5. Вихман В.В., Якименко А. Внедрение биометрической идентификации в системы контроля и управления доступом. 2016, 48 - С.
6. Суомалайнен А.: Биометрическая защита. Обзор технологи. Издательство: ДМК-Пресс, 2019. -104 С.
7. Шаленков И.А. Группы по оказанию услуг в области кибербезопасности, Технологическая практика. 1 августа 2023. Керт – аудиторско-консалтинговая фирма.
8. Котилко В.В. РЕЗУЛЬТАТИВНОСТЬ УПРАВЛЕНИЯ БИОМЕТРИЕЙ В УСЛОВИЯХ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА // XVIII МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ ПЕРСПЕКТИВНЫЕ

НАУЧНЫЕ ИССЛЕДОВАНИЯ КАК ДВИГАТЕЛЬ СОВРЕМЕННОЙ НАУКИ (Санкт-Петербург, 22 Июнь, 2024). – Санкт- Петербург: МЕЖДУНАРОДНЫЙ ИНСТИТУТ ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ им. ЛОМОНОСОВА, 2024. – 60-63 С.

9. Котилко В.В., Мамаев В.Ю. ПРОБЛЕМЫ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ СТРУКТУРАМИ, ЗАНИМАЮЩИМИСЯ БИОМЕТРИЕЙ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ // Журнал «Системы безопасности», № 3, 2024.