Proceedings of International Scientific Conference on Multidisciplinary Studies
Hosted online from Moscow, Russia
Date: 11th October - 2024
ISSN: 2835-5733 **Website:** econferenceseries.com

РИСКИ И ОТВЕТСТВЕННОСТЬ БАНКОВ ПРИ ИСПОЛЬЗОВАНИИ BIG DATA ДЛЯ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА

Абдуназарова Ч. А.
Ташкент, Charosblackeyes303@gmail.com
+99891 956 56 27

Возникновение термина «Big Data» связывают с вышедшей в 2008 г. в научном журнале «Nature» статьей директора Коалиции сетевой информации (CNI) и по совместительству редактора указанного издания К. Линча, в которой последний, рассматривая явление экспоненциального прироста объемов и разнообразия информационных массивов, используемых в современной жизни, предложил использовать данную дефиницию, в рамках концепции будущих изменений в системах обработки данных, для описания круга проблем, связанных с качественной и эффективной обработкой таких массивов[1].

Следовательно, использование, анализ и обработка больших объемов информаций затрагивают ряд вопросов, связанной с определением источников данных информаций и ответственность за обработку и использованию их. Невозможно опустить риски утечки информации если речь идет об обработке и использовании информации, особенно когда такие информации представляют собой персональные данные. Защита персональных данных в нынешнее время, в котором мошенничество путем разных технологий широко распространено не только в нашем государстве, но и во всем мире, является одной главной задачей финансовых организаций.

Такую защиту необходимо осуществлять с двух точки зрения: технологическую и правовую.

Финансовый сектор все чаще использует технологии больших данных и технологии искусственного интеллекта для их обработки. Этому способствует увеличение объема информации в целом: домохозяйства и компании производят беспрецедентное количество данных, которые постоянно накапливаются; социальные сети позволяют отслеживать скорость распространения информации, компании подробно фиксируют процесс производства и продажи товаров и услуг; платежные транзакции и

1. Электронный ресурс https://www.nature.com/nature/volumes/455/issues/7209

интернет-торговля также имеют свой «цифровой след». Растут инвестиции в большие данные компаний финансового сектора: по некоторым расчетам, в 2021 году они составят 14 млрд долларов США по сравнению с 9 млрд долларов США в 2018 году.

Согласно исследованию Европейского банковского управления (EBA), банки ЕС заинтересованы в использовании аналитики больших данных: растет доля как организаций, которые уже используют большие данные в своей деятельности (рост с 60 до 64% с 2018 по 2019 год), так и доля компаний, тестирующих, разрабатывающих и обсуждающих внедрение новых технологий. Всего лишь 2% банковских институтов ответили, что они не занимаются внедрением аналитики больших данных[2].

Если рассматривать законодательство ряд стран не поставлены ограничения к внедрению какой-то конкретной технологии анализа данных, при этом только обусловив обеспечения надлежащей защиты информации, представляющие собой персональные данные. Для обеспечения защиты информации в первую очередь необходимо определить или сортировать информации исходя из их источников и защищенности.

В соответствии с подходом UNECE[3] можно классифицировать различные виды больших данных следующим образом:

• информация из социальных сетей, блогов и интернет-сообщений;
• данные о деятельности в Интернете (в том числе поисковые запросы пользователей, данные о посещенных сайтах);
• информация традиционных бизнес-процессов (информация о транзакциях, покупках, заказах, платежах, регистрации клиентов, банковских операциях и тому подобном);
• данные государственных организаций (административные данные, в том числе таможенные, налоговые и другие, медицинские данные);
• данные мобильных и прочих устройств (данные геолокации, данные о трафике, данные систем типа «умный дом», камер видеонаблюдения, данные сенсоров, трекеров и тому подобного).

В финансовых организациях подобно больше накапливаются информация традиционных бизнес-процессов (информация о транзакциях, покупках,

[2] ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ В ФИНАНСОВОМ СЕКТОРЕ И РИСКИ ФИНАНСОВОЙ СТАБИЛЬНОСТИ. Москва.2021// Consultation_Paper_10122021.pdf (cbr.ru)
[3] United Nations Economic Commission for Europe – Европейская экономическая комиссия ООН.

заказах, платежах, регистрации клиентов, банковских операциях и тому подобном). Однако, хотя благодаря своей функции финансовые организации владеют и получают информации традиционных бизнес процессов, в своей деятельности финансовые организации нуждаются и часто пользуются других видов информации как данные государственных организаций и информация из социальных сетей, блогов и интернет-сообщений.

В общественности и для официального пользования в последнее время лояльно использования термин «кибербезопасность».

В Законе Республики Узбекистан предусмотрено определение к понятию «кибербезопасность» — состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве.

С правовой точки зрения в странах Европы и СНГ приняты ряд нормативно-правовых актах, касающихся киберпезопасности информации:

1. **GDPR (Общий регламент о защите данных)** — регламент Европейского Союза, который регулирует обработку персональных данных и устанавливает права субъектов данных.
2. **ePrivacy Directive (Директива о конфиденциальности в электронных коммуникациях)** — регулирует конфиденциальность и защиту данных в сфере электронных коммуникаций.
3. **NIS Directive (Директива о безопасности сетевых и информационных систем)** — касается повышения уровня кибербезопасности в ЕС.
4. **European Data Protection Board (EDPB)** — орган, регулирующий применение GDPR и обеспечивающий его соблюдение в странах ЕС.
5. **Федеральный закон № 152-ФЗ "О персональных данных" (Россия)** — регулирует обработку персональных данных и устанавливает требования к их защите.
6. **Закон "Об информации, информационных технологиях и о защите информации" (Россия)** — содержит нормы, касающиеся защиты информации в различных сферах.
7. **Закон Республики Беларусь "О защите персональных данных"** — устанавливает правила обработки и защиты персональных данных.
8. **Закон "О защите информации" (Казахстан)** — регулирует вопросы защиты информации, в том числе персональных данных.

9. Закон "О персональных данных" (Узбекистан) — определяет правила и механизмы защиты персональных данных.

10. Закон «О киберпезосности» (Узбекистан) - регулирование отношений в сфере кибербезопасности.

Однако, в Законе «О персональных данных» ограничивается регулированием информации о физических лицах, не включая юридических лиц, как это определяется в самом законе «персональные данные — зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации».

В общем защита информации о юридических лицах остались открытым, хотя имеется некоторые нормативно-правовые акты, частично регулирующие обработку и использование данных юридических лиц. К таким относятся Закон РУз «Об обществах с ограниченной и дополнительной ответственностью», Закон РУз «Об акционерных обществах» и т.д. Точнее юридическое лицо дает информации, относящие к своей деятельности только по заявлению своего учредителей и государственным органом в порядке и в объеме, установленным нормативным актам определяющие порядок и полномочие запроса данных информации. Именно, нормативный акт, регулирующий порядок предоставления информации о своих клиентах, включая юридические и физические лица, к любым третьим лицам является Закон РУз «О банковской тайне». К таким информациям употребляется специальный термин «банковская тайна»

Согласно Закону РУз «О банковской тайне», **банковской тайной** являются защищаемые банком сведения:

- об операциях, счетах и вкладах своих клиентов (корреспондентов);
- о своем клиенте (корреспонденте), полученные банком в связи с оказанием ему банковских услуг;
- о наличии, характере и стоимости имущества клиента (корреспондента), находящегося на хранении в сейфах и помещениях банка;
- о межбанковских операциях и сделках, совершенных по поручению клиента (корреспондента) или в его пользу;
- о клиенте (корреспонденте) другого банка, ставшие известными в результате обращения сведений, составляющих банковскую тайну, между банками;

- об участниках накопительной пенсионной системы, размере и движении сумм пенсионных взносов, пенсионных накоплениях на индивидуальных накопительных пенсионных счетах граждан.

Если раскрыть вышеперечисленные категории информации, то можно узнать, что банки обладает огромным кругом и объемом информации о своих клиентах.

И в данном законе устанавливается порядок разглашение данных информации третьим лицам. Разглашением банковской тайны считается опубликование через средства массовой информации, распространение или сообщение в устной либо письменной форме или иным способом сведений, составляющих банковскую тайну, доведение их до третьих лиц, прямое или косвенное предоставление третьим лицам возможности для добывания таких сведений, в том числе вследствие нарушения порядка их хранения лицами, которым эти сведения были доверены или стали известны в связи с выполнением ими служебных обязанностей[4].

Такое разглашение банком запрещено законом за исключением следующих случаев: сообщение или предоставление банком сведений, составляющих банковскую тайну, третьим лицам, оказывающим банку юридические, бухгалтерские, аудиторские, информационные и консультационные услуги, при условии, что это необходимо для оказания данной услуги и что эти лица обязаны воздерживаться от действий, установленных законодательством;

обмен сведениями, составляющими банковскую тайну, между органами прокуратуры, предварительного следствия, дознания и органами, осуществляющими оперативно-розыскную деятельность, а также компетентными органами иностранных государств в порядке, предусмотренном законодательством и международными договорами Республики Узбекистан.

Главными органами раскрывающие преступления, связанной с мошенничеством являются вышеперечисленные органы исходя из круг их функциональной обязанности. Банки также для предотвращения мошенничества разглашают информации, представляющие собой банковскую тайну только соблюдав установленный порядок законом.

[4] Закон Республики Узбекистан «О банковской тайне» от 30.08.2003 г. № 530-II// 530-II-сон 30.08.2003. О банковской тайне (lex.uz)

Такие сведения предоставляются только с санкции прокурора по мотивированному постановлению следователя или дознавателя в целях установления обстоятельств по находящимся в их производстве уголовным делам, а также обеспечения взыскания нанесенного ущерба или наложения ареста на имущество: органом прокуратуры, предварительного следствия и дознания; органам, осуществляющим оперативно-розыскную деятельность - на основании мотивированного постановления, утвержденного руководителем этого органа.

Такого рода получения информации о наличии счетов вышеперечисленным органом можно осуществлять в автоматизированным режиме из информационной базы данных Центрального Банка Республики Узбекистан. Потому что, именно данным законом установлено, что Центральный банк не является третьем лицом в данных отношениях.

Однако, в законах ограничивается категория сведении, представляющие банковскую тайну вследствие чего, сотрудники банка иногда допускают ошибки связанной с утечкой информации, служащие осуществление мошеннических действий.

Таким образом, анализировав нынешнее ситуацию и проводив исследование, предлагается: конкретизировать систему предоставления информации, применив новые технологии, включая искусственного интеллекта, обеспечивающие уведомление самого клиента о предоставлении таких информации о себе, также именно какие информации предоставляются органом. Кроме того, разрабатывать новый нормативно-правовой акт, в котором перечислены конкретно какие сведения в каком порядке и обстоятельствам и объемах можно предоставить сведения, то есть конкретизировать категории сведения, представляющие собой банковскую тайну.

Использованные литературы

1. Электронный ресурс https://www.nature.com/nature/volumes/455/issues/7209,
2. Использование больших данных в финансовом секторе и риски финансовой стабильности. Москва.2021// Consultation_Paper_10122021.pdf (cbr.ru)
3. United Nations Economic Commission for Europe – Европейская экономическая комиссия ООН.

4. Закон Республики Узбекистан «О банковской тайне» от 30.08.2003 г. № 530-II// 530-II-сон 30.08.2003. О банковской тайне (lex.uz)
5. Закон Республики Узбекистан «Кибербезопасности» от 15.04.2022 г. № ЗРУ-764// ЗРУ-764-сон 15.04.2022. О кибербезопасности (lex.uz)
6. Закон Республики Узбекистан «о персональных данных» от 02.07.2019 г. № ЗРУ-547// ЗРУ-547-сон 02.07.2019. О персональных данных (lex.uz)