LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

ОСНОВНЫЕ СУБЪЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

Махмудов Жахонгир Махмуд угли
Магистр Ташкентского государственного юридического университета
maxmudov.johongir602@gmail.com

Аннотация: *цифровая трансформация финансового сектора сопровождается ростом киберугроз, особенно в отношении банковской инфраструктуры. В данных условиях особое значение приобретает формирование эффективной системы правового и институционального обеспечения кибербезопасности. В статье рассматриваются ключевые субъекты, вовлечённые в обеспечение кибербезопасности в банковской сфере, а также определяются их функции, полномочия и сферы ответственности.*

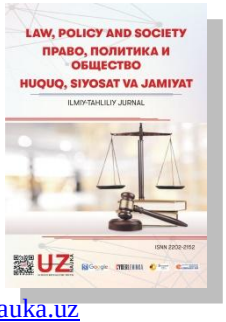
Ключевые слова: *кибербезопасность, банковская система, регуляторы, субъекты, правовое регулирование, Центральный банк, киберугрозы.*

MAIN ENTITIES IN ENSURING CYBERSECURITY IN THE BANKING SECTOR

Makhmudov Jakhongir Makhmud ugli
Master's student of Tashkent State University of Law
maxmudov.johongir602@gmail.co

Abstract*: the digital transformation of the financial sector is accompanied by an increase in cyber threats, especially in relation to the banking infrastructure. In these conditions, the formation of an effective system of legal and institutional support for cybersecurity is of particular importance. The article examines the key entities involved in ensuring cybersecurity in the banking sector, and defines their functions, powers and areas of responsibility.*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz



Keywords: *cybersecurity, banking system, regulators, entities, legal regulation, Central Bank, cyber threats.*

В условиях стремительной цифровизации финансового сектора вопросы кибербезопасности приобретают первостепенное значение. Современные банки не только хранят и обрабатывают огромные массивы персональных и финансовых данных, но и являются одними из главных целей кибератак. Защита от киберугроз требует комплексного подхода, в котором участвуют как сами банки, так и органы государственной власти, регулирующие структуры, международные организации и частные ИТ-компании.

Изучив соответствующую литературу, был сделать вывод что кибербезопасность представляет собой защиту электронных серверов и сетей, а также персональные данные от криминального вмешательства.

С переходом к цифровой экономике кибербезопасность в банковском секторе становится серьезной проблемой. Использование методов и процедур, разработанных для защиты данных, имеет важное значение для успешной цифровой революции. Эффективность кибербезопасности в банках влияет на безопасность нашей личной информации (PII), будь то непреднамеренное нарушение или хорошо спланированная кибератака. Основной целью кибербезопасности в банковском секторе является обеспечение защиты личных данных и активов клиентов, особенно в условиях растущего онлайн-банкинга и цифровых платежей. Люди совершают транзакции, используя цифровые способы оплаты, такие как

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

дебетовые и кредитные карты, которые должны быть защищены средствами кибербезопасности.[1]

Для начала необходимо рассмотреть, что национальное законодательство предусматривает под субъектом кибербезопасности. Согласно части 8 статьи 3 Закона «О кибербезопасности» Республики Узбекистан, «субъект кибербезопасности — юридическое лицо или индивидуальный предприниматель, имеющий определенные права и обязанности, связанные с владением, пользованием и распоряжением национальными информационными ресурсами и оказанием информационных электронных услуг по их использованию, защитой информации и кибербезопасностью, в том числе субъекты критической информационной инфраструктуры». Таким образом, субъектами являются как физические так и юридические лица, имеющие доступ к определенной информации и возможностью оказывать услуги по их защите.

Известно что, Служба государственной безопасности Республики Узбекистан является уполномоченным государственным органом в сфере кибербезопасности. К его полномочия входит разработка нормативно-правовых актов, осуществление контроля, проведение оперативно-розыскных мероприятий, организация работ по обеспечению кибербезопасности, определение требований по обеспечению кибербезопасности и иные полномочия, указанные в национальной законодательстве, регулирующее кибербезопасность.

[1] БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ: КЛЮЧЕВЫЕ АСПЕКТЫ И РОЛЬ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ. Кочаева А.Р. Международный научный журнал «Вестник науки» №1, Том 2. Январь 2024. С. 142

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Субъекты кибербезопасности имеют как права, так и обязанности. В права субъекта входят получение от уполномоченного государственного органа сведения о киберугрозах, получение консультации уполномоченного государственного органа о средствах и методах защиты от кибератак и предотвращение их, а также инициировать методы обеспечения кибербезопасности. Обязанностями являются предотвращение незаконного распространения данных, их хранение и распространение, своевременное уведомление уполномоченных органов об инцидентах кибербезопасности, предоставление уполномоченному государственному органу право доступа в мониторинговые системы и иные обязанности предусмотренные в национальном законодательстве.

Основными субъектами кибербезопасности в настоящее время являются должностные лица государственных органов, органов местного самоуправления, наделенных соответствующими полномочиями, среди которых особо выделяются правоохранительные структуры, а также специальные службы.[2] Перечисленные и другие субъекты кибербезопасности обеспечивают ее посредством правовых, организационных, технических, оперативно-розыскных, кадровых, разведывательных, контрразведывательных, научных, информационно-аналитическихмероприятий.

К основными субъектами обеспечения кибербезопасности в банковской сфере относятся Центральный банк Республики Узбекистан, коммерческие банки и финансовые учреждения, государственные органы и

[2] Кибербезопасность современной россии: теоретические и организационно-правовые аспекты. Ковалев Олег Геннадьевич. Столыпинский вестник 2021.

правоохранительные структуры, и частные ИТ-компании и поставщики решений в сфере кибербезопасности.

Центральный банк в каждой стране играет ключевую роль в формировании политики кибербезопасности в финансовом секторе. Он разрабатывает нормативно-правовые акты, устанавливает обязательные стандарты безопасности, проводит аудит цифровых систем банков и может применять санкции в случае нарушений. В их полномочия могут входить разработка требований по защите и сохранности информации, осуществление мониторинга по соблюдению стандартов безопасности банками, и проведение тестов и оценки рисков информационной безопасности. Центральный банк Республики Узбекистан могут издавать положения, регламентирующие порядок защиты электронных платежей и операционных систем банков.

Первыми и непосредственными субъектами обеспечения кибербезопасности являются коммерческие банки и финансовые учреждения. Они в свою очередь создают внутреннюю службу информационной безопасности путем внедрения средств защиты данных, например, антивирусные системы или шифрование. Также проводятся регулярные мониторинги ИТ-систем, обучение персонала различным методам предотвращения киберугроз и проведение инструкции клиентам. Следует отметить что, банки несут юридическую ответственность за утечку клиентской информации и нарушение требований по защите данных.[3]

[3] Безопасность в банковской сфере: ключевые аспекты и роль кибербезопасности в эпоху цифровой экономики. Кочаева А.Р. Международный научный журнал «Вестник науки» №1, Том 2. Январь 2024. С. 140-143.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Государственные органы выступают в качестве субъекта и участвуют в создании условий для борьбы с киберпреступностью. К таким субъектам относятся:

1. Министерства юстиции и внутренних дел.
2. Специализированные агентства по кибербезопасности.
3. Органы прокуратуры, осуществляющие надзор за соблюдением законодательства.

Правоохранительные органы изучают и расследуют кибератаки и киберпреступления, разрабатывая стратегические документы в области кибербезопасности и работают в сотрудничестве с финансовыми учреждения для выявления будущих потенциальных угроз.

Известно, что кибербезопасность в банковской сфере является новым видом направления, требующих своевременного изучения и регулирования. В связи с небольшим опытом Узбекистана в данной области и учитывая глобальный характер киберугроз, международное сотрудничество играет важную роль. Обращение к международному опыту и сотрудничество с такими организациями, как Международная организация по стандартизации или Международный валютный фонд и Всемирный банк, имеют ключевое значение для разработки эффективных стратегий в области кибербезопасности. Это сотрудничество позволяет заимствовать лучшие практики, использовать передовые технологии и стандарты, а также обеспечивать соответствие международным требованиям. Кроме того, совместная работа с международными организациями способствует укреплению национальной системы киберзащиты, повышению доверия к финансовым институтам и снижению рисков, связанных с кибератаками, что

особенно важно для устойчивости и развития финансовой системы Узбекистана. Приобретение данных навыков будет иметь положительный результат при формировании национального законодательства, регулирующее вопросы обеспечения кибербезопасности в банковской сфере.

Коммерческие банки и финансовые учреждения рассматривают сотрудничество с Частными ИТ-компаниями и поставщиками решений в сфере кибербезопасности в целях разработки программного обеспечения для защиты персональных данных и осуществление внешнего тестирования и аудита системы безопасности банков. Нельзя забывать об осторожности при сотрудничестве с внешними подрядчиками и контролировать их работу при передаче чувствительной информации, в целях предотвращения ее утечки.

После тщательного изучения литературы и нормативно-правовых актов, мы пришли к выводу, что обеспечение кибербезопасности в банковской сфере — это результат скоординированной работы целой сети субъектов: от регуляторов и самих банков до международных организаций и ИТ-компаний. В условиях постоянной эволюции киберугроз только комплексный и межведомственный подход способен обеспечить устойчивость банковской системы и защиту интересов клиентов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764.

2. Закон Республики Узбекистан «О банках и банковской деятельности» от 25 апреля 1996 года № 216-I, с изменениями и дополнениями от 05.11.2019 г. № ЗРУ-580.

3. Закон Республики Узбекистан «О Центральном банке Республики Узбекистан» от 21 декабря 1995 года № 154-I, с изменениями и дополнениями от 11.11.2019 г. № ЗРУ-582.

4. Безопасность в банковской сфере: ключевые аспекты и роль кибербезопасности в эпоху цифровой экономики. Кочаева А.Р. Международный научный журнал «Вестник науки» №1, Том 2. Январь 2024. С. 140-143.