УДК 347.73
DOI 10.18101/978-5-9793-1659-8-121-126

ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ В БАНКОВСКОМ СЕКТОРЕ СИНГАПУРА

© **Содномова Эржена Дмитриевна**
магистрант юридического факультета
Бурятский государственный университет имени Доржи Банзарова,
Россия, г. Улан-Удэ
esodnomova@yandex.ru

Данная статья посвящена способам противодействия и предупреждения кибер-угроз в сфере банковских услуг Сингапура. Актуальность статьи состоит в том, что в современном мире особую важность приобретают меры, принимаемые регуляторами в борьбе с информационными преступлениями и способах надежной защиты от мошеннических действий в интернет-пространстве. Важность данного вопроса подтверждается возросшим процентом преступлений, совершенных в области информационных технологий банковского сектора. Целью работы является установление методов, принимаемых денежно-кредитным управлением Сингапура в целях защиты банковского сектора от противоправных действий. Предмет исследования составляют основные нормативно-правовые акты в сфере обеспечения кибербезопасности Сингапура. В работе применяются формально-юридический, сравнительно-правовой методы. Методологическую основу статьи составляет совокупность методов научного познания, таких как анализ и синтез, обобщение. Высказывается предположение об использовании в отечественной практике идей криминализации и пресечения мошенничеств в киберпространстве, хищения персональных данных и их неправомерного использования.

Ключевые слова: Сингапур, киберпреступления, информационные технологии, кибербезопасность, обнаружение, предупреждение

В современном динамично развивающемся мире область банковской деятельности, как и все прочие сферы жизнедеятельности человека, тесно взаимосвязана с информационными технологиями, и стремительно меняется под воздействием виртуальной реальности. Сегодня банковская сфера не может существовать в отрыве от цифровых технологий, и как следствие, подвергается постоянным угрозам в цифровой реальности. Так, при современном состоянии развитости информационных технологий и распространенности коммуникационных сетей, все большее количество преступлений совершается в виртуальном пространстве. Банки несут значительные риски и могут оказаться жертвой мошеннических действий как в отношении каждого из клиентов, так и банка в целом.

Сингапур — современное государство, вступившее в век цифровых технологий и активно применяющее их в повседневной жизни. Банковский сектор Сингапура, вследствие этого, не застрахован от неправомерных действий киберпреступников.

Национальный правовой механизм кибербезопасности Сингапура имеет длительную историю становления. Это обусловлено темпами социально-экономического развития государства, его фактическим статусом регионального и международного торгово-экономического центра [1, 110].

Банковская сфера масштабно использует оборудование и технологии, что безусловно обеспечивает высокую технологичность, при этом повышая риск возможных кибернетических атак и хищения данных.

Переходя к законодательству Сингапура, в области киберпреступлений можем выделить следующие уголовные или административные правонарушения:

– взлом (несанкционированный доступ),
– отказ в обслуживании («DoS-атака»),
– заражение ИТ-систем вредоносным ПО (в том числе с выкупом ПО),
– распространение оборудования, используемого для совершения киберпреступлений,
– владение или использование оборудования, используемого для совершения киберпреступлений,
– мошенничество с использованием личных данных,
– электронная кража,
– незапрашиваемое тестирование на проникновение (использование ИТ-системы без разрешения ее владельца для определения уязвимости и слабых мест),
– любая другая деятельность, которая отрицательно влияет или угрожает безопасности, конфиденциальности, целостности или доступности любых ИТ систем, инфраструктуры, сетей связи, устройств или данных.

Мерой наказания по указанным правонарушениям обычно являются штраф в долларах США или лишение свободы, в некоторых случаях оба вида наказания. Указанные правонарушения классифицируются Законом о ненадлежащем использовании компьютеров («Computer Misuse Act») и Уголовным кодексом («Penal Code») [3, 6].

В Сингапуре также действует ряд нормативных правовых актов, касающихся кибербезопасности. Перейдем к рассмотрению основных из них. Закон о кибербезопасности 2018 г. («Cybersecurity Act») устанавливает рамки для мониторинга критически важных информационных инфраструктур («КИИ»), в том числе налагает на владельцев КИИ обязательства сообщать об инцидентах в области кибербезопасности и предусматривает назначение уполномоченного лица по кибербезопасности, среди прочего, для надзора и обеспечения кибербезопасности компьютеров и компьютерных систем в Сингапуре [5].

Кроме того, уполномоченное лицо по кибербезопасности также наделено властью издавать или утверждать кодексы стандартов эффективности для регулирования владельцев КИИ в отношении мер, которые должны быть приняты ими для обеспечения кибербезопасности КИИ. Однако эти своды правил предназначены для ознакомления и не имеют законодательной силы.

Закон о защите личных данных 2012 г. («PDPA») налагает на организации ряд обязательств по защите персональных данных. Важно отметить, что раздел 24 данного закона требует, чтобы организации защищали личные данные, находящиеся в их владении или под их контролем, путем принятия разумных мер безопасности для предотвращения несанкционированного доступа, сбора, использования, раскрытия, копирования, изменения, удаления или аналогичных рисков [7].

Закон о неправомерном использовании компьютеров («Computer Misuse Act») охватывает ряд киберпреступлений, включая, помимо прочего, такие преступле-

ния, как использование компьютерных уязвимостей для получения несанкционированного доступа к компьютерной системе [3].

Закон об авторском праве («Copyright Act») криминализирует нарушение авторских прав. В частности, правонарушением является то, что при наличии авторского права лицо использует его для продажи или найма; продает или сдает в аренду, или, посредством обмена, предлагает или выставляет на продажу или в аренду; или посредством торговли, выставляет на всеобщее обозрение любой предмет, который является копией произведения, нарушающий авторские права [4].

В законе о стратегических товарах (контроле) («Strategic Goods (Control) Act») излагаются положения, касающиеся передачи стратегических товаров и технологий, связанных со стратегическими товарами, и посредничества в их реализации. Список предметов, которые были определены министром в качестве стратегических товаров и технологий стратегических товаров [8].

Организации обязаны в соответствии с действующим законодательством Сингапура принимать меры по мониторингу, обнаружению, предотвращению или смягчению инцидентов. В соответствии с разделом 14(2) Закона о кибербезопасности владелец КИИ обязан создать механизмы и процессы с целью обнаружения угроз в отношении КИИ. В то же время PDPA налагает обязательства по защите: организации должны вводить разумные меры безопасности для защиты личных данных, находящихся в их владении и/или под их контролем. Однако в PDPA не указываются конкретные меры, которые следует предпринять организациям.

В руководстве по управлению утечками данных 2.0 («Managing and notifying data breaches») комиссия по защите персональных данных («PDPC») устанавливает действия организаций по предотвращению утечки данных [9].

В нем говорится, что организации должны применять меры и инструменты мониторинга для раннего обнаружения и предупреждения организаций.

Например:

- мониторинг входящего и исходящего трафика для веб-сайтов и баз данных на предмет аномальной сетевой активности;
- использование программного обеспечения для обнаружения вторжений в реальном времени, предназначенного для обнаружения несанкционированных действий пользователей, атак и компрометации сети;
- использование камер видеонаблюдения для наблюдения за внутренними и внешними периметрами защищенных зон, таких как центры обработки данных и серверные комнаты.

Руководство по утечке данных также призывает организации разрабатывать план управления утечками данных, который будет включать следующую информацию:

- конкретное и четкое понятие компрометации данных (и предполагаемое, и подтвержденное);
- порядок подачи сообщения о компрометации данных внутри организации;
- порядок действий при компрометации данных;
- обязанности группы работы с компрометированным данными.

Возможными мерами, принимаемыми для защиты ИТ-систем выступают:

Биконы (маячки) — незаметно и удаленно размещенные передатчики, вставленные в контент для установления контакта с удаленным сервером и выявления IP-адрес компьютера, просматривающего данный контент.

Предположительно, что данные, собранные такими маячками в целях защиты, не будут попадать под действие PDPA как личные данные. Согласно обязательству о согласии PDPA, организации требуется согласие (или предполагаемое согласие) от физического лица перед сбором, использованием и разглашением личных данных. Таким образом, маячки не будут разрешены, если они будут собирать личные данные без согласия (или предполагаемого согласия) лиц, о которых идет речь, за исключением исключений из согласия. Обязательство применяется в соответствии с PDPA.

Honeypots — цифровые ловушки, предназначенные для обмана злоумышленников, заманивающие их в синтетическую сеть, тем самым позволяя организации обнаружить и принять меры по противодействию на атаки своей сети, не нанося никакого ущерба реальной сети или данным организации. Ограничений на использование *honeypots* в целях защиты IT-систем, скорее всего, не будет. Ни закон о кибербезопасности, ни PDPA не ограничивают использование *honeypots,* как метода защиты ИТ-систем. В статье, опубликованной Агентством по киберзащите Сингапура (Cyber Security Agency of Singapore) в 2019 году, приводится понятие *honeypots* и их роль в киберзащите. Кроме того, руководство PDPC по защите личных данных в электронном носителе поощряет использование «средств защиты, которые могут использоваться для повышения безопасности сетей».

Воронки — меры по перенаправлению вредоносного трафика в даль от собственных IP-адресов и серверов организации, обычно используется для предотвращения «DoS-атак». Ограничений на использование воронок с целью защиты ИТ-систем, скорее всего, не будет. Как и в случае с honeypots, ни закон о кибербезопасности, ни PDPA не ограничивают использование воронок для защиты ИТ-систем.

Так же организациям разрешено отслеживать или перехватывать электронные коммуникации в их сетях (например, электронная почта и использование Интернета сотрудниками), чтобы предотвратить или смягчить последствия кибератак. Нет закона, запрещающего организации осуществлять мониторинг, прослушивание или перехват электронных сообщений в собственной сети. Однако, если такие данные подпадают под определение личных данных, то возможно организации потребуется согласие соответствующих лиц. В соответствии с обязательством по защите PDPA, организации должны принимать разумные меры безопасности для защиты личных данных, находящихся в их распоряжении. В зависимости от ряда факторов мониторинг или перехват электронных сообщений во внутренней сети организации могут считаться одними из таких разумных мер.

Особенности регулирования информационной безопасности в банковском секторе изложены в опубликованном денежно-кредитным управлением Сингапура, исполняющим функцию Центрального банка, руководстве по управлению технологическими рисками («MAS TRM Guidelines»). В указанном руководстве установлены принципы управления рисками и практические стандарты для руководства финансовыми учреждениями, заключающиеся в:

– создании надежной системы управления технологическими рисками,

– укреплении системной безопасности, надежности, отказоустойчивости и восстановлении,

– развертывании процессов строгой аутентификации для защиты данных клиентов, транзакций и системы в целом [11].

Так, каждая финансовая организация обязана с 18 января 2021 года оценивать своих поставщиков в области информационных технологий [11].

Указанный акт включает перечень требований к финансовым учреждениям по созданию системы управления технологическими рисками под надзором Совета директоров и высшего руководства для выявления, оценки, мониторинга и обработке технологических рисков.

Кроме того, денежно-кредитное управление Сингапура также выпустило уведомление о кибернетической безопасности («Notice on Cyber Hygiene»), которая требует от банков, среди прочего, обеспечения безопасных патчей, применяемых для устранения уязвимостей в их компьютерных системах [10].

Подводя итоги исследования правовых норм Сингапура в кибербезопасности, можно заключить, что в современном правовом поле Сингапура регулирующие органы постоянно актуализуют нормы в соответствии с меняющейся обстановкой, подстраиваясь под сложившуюся ситуацию и действуя в защиту гражданских прав и свобод и одновременном соблюдении публичных интересов. Преступления, совершаемые в виртуальном пространстве, не ограничиваются государственными границами и как следствие, на взгляд автора, не решаемы регуляторами одного конкретного взятого государства. Вместе с тем, лидирующая позиция Сингапура, обеспеченная запуском ряда успешных проектов в кибербезопасности и успешно-проводимой внутренней политике, позволит в будущем разработать государству универсальный международно-правовой механизм обеспечения кибербезопасности.

Проведенное исследование выявляет методы, принимаемые регулирующими органами для защиты ИТ-систем и позволяет спрогнозировать некоторые перспективные направления развития системы отечественных правовых норм и способам противодействия и предупреждения кибер-угроз в сфере банковских услуг. Так, представляется весьма вероятным прогрессирующее использование в отечественной нормотворческой и правоприменительной практике идей криминализации и пресечения мошенничеств в киберпространстве, хищения персональных данных и их неправомерного использования.

Литература

1. Горян Э. В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.

2. Денисова А.В. Уголовная ответственность за преступления в сфере финансовых рынков по законодательству Сингапура // Lex russica. 2021. Т. 74, № 1. С. 148–156. DOI: 10.17803/1729-5920.2021.170.1.148-156.

3. Computer misuse act // URL: https://sso.agc.gov.sg/Act/CMA1993 (дата обращения: 15.09.2021)

4. Copyright act // URL: https://sso.agc.gov.sg/Act/CA1987 (дата обращения: 15.09.2021)

5. Cybersecurity Act 2018 // URL: https://sso.agc.gov.sg/Act/CA2018 (дата обращения: 15.09.2021)

6. Penal code // URL: https://sso.agc.gov.sg/Act/PC1871 (дата обращения: 15.09.2021)

7. Personal data protection act 2012 // URL: https://sso.agc.gov.sg/Act/PDPA2012 (дата обращения: 15.09.2021)
8. Strategic goods (control) act // URL: https://sso.agc.gov.sg/Act/SGCA2002 (дата обращения: 15.09.2021)
9. Managing and notifying data breaches // URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf?la=en (дата обращения: 15.09.2021)
10. Notice on Cyber Hygiene // URL: https://www.mas.gov.sg/regulation/notices/notice-655 (дата обращения: 15.09.2021)
11. Technology Risk Management Guidelines // URL: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf (дата обращения: 15.09.2021)

CYBER ATTACK'S CONTRADICTION IN SINGAPORE BANKING SYSTEM

Erzhena D. Sodnomova
Master student of the Law Faculty
Banzarov Buryat State University
Russia, Ulan-Ude
esodnomova@yandex.ru

This article is devoted to contradiction methods and prevention of cyber threats in the banking sector of Singapore. The relevance of the article lies in the fact that in the modern world, measures taken by regulators in order to deal with cybercrimes and options for reliable protection against fraud in the Internet are of particular importance. Increased percentage of crimes committed in the field of information technology in the banking field confirms the importance of this issue. The aim of the paper is to establish the methods adopted by the Monetary Authority of Singapore in order to protect the banking sector from illegal actions. The subject of the research is the main regulatory legal acts in the field of cybersecurity in Singapore. The work uses formal legal, comparative legal methods. The methodological basis of the article is a set of methods of scientific knowledge, such as analysis and synthesis, generalization. In the paper, there is an assumption about the use in domestic practice ideas of criminalization and suppression of fraud in cyberspace, theft of personal data and their misuse.
Keywords: Singapore, cybercrimes, cybersecurity, information technology, detection, crime prevention, banking system