Список использованных источников

1. Монж Г. Начертательная геометрия: Пер. с фр. – М.: Изд-во АН СССР, 1947.
2. Покровская М. В., Лунина И. Н. Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. №11. С. 175—188
3. Еськов К., «Наш ответ Фукуяме: «Конец истории?» - «Не дождетесь!..», Москва, АСТ, 2001
4. Бахтияров О., «Деконцентрация внимания», монография, Киев, ЭКСПИР.

УДК 336.7

Р.А. Туманян, Е.А. Малышева, Т.Н. Цапина
Национальный исследовательский Нижегородский
государственный университет имени Н.И. Лобачевского
Нижний Новгород, Россия

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Аннотация. *В статье рассмотрены особенности экономической безопасности кредитной организации, раскрыта сущность ее информационной составляющей, приведена классификация возможных угроз. Особое внимание уделено описанию инструментов защиты информационной безопасности. Предложены конкретные рекомендации по улучшению информационной безопасности кредитных организаций.*

R.A. Tumanyan, E.A. Malysheva, T.N. Tsapina
National Research Lobachevsky State University of Nizhni Novgorod
Nizhny Novgorod, Russia

FEATURES OF INFORMATION SECURITY OF A CREDIT INSTITUTION

Abstract. *The article examines the features of the economic security of a credit institution, reveals the essence of its information component, and provides a classification of possible threats. Special attention is paid to the description of information security protection tools. Specific recommendations for improving the information security of credit institutions are proposed.*

Экономическая безопасность кредитной организации – это состояние защищенности финансово-кредитного института от недобросовестной конкуренции, противоправной деятельности криминальных формирований и отдельных лиц, негативного влияния внешних и внутренних угроз, дестабилизирующих факторов, при котором обеспечивается устойчивая стабильность функционирования и развития организации, реализация основных коммерческих интересов и целей уставной деятельности, а именно оказание финансовых услуг юридическим и физическим лицам с целью получения прибыли [1]. Экономическая безопасность кредитной организации включает в себя ряд элементов, каждый из которых представляет определенный вид деятельности по обеспечению защищенности. Выделяют следующие составляющие: финансовая, силовая, маркетинговая, силовая, кадровая. Также важным элементом системы экономической безопасности банка выступает информационная безопасность.

Информационная безопасность (далее – ИБ) банка – это состояние защищенности, при котором не нарушаются 3 основных свойства информации: конфиденциальность, доступность, целостность. ИБ определяется отсутствием недопустимого риска, связанного с несанкционированными и непреднамеренными воздействиями на информацию и (или) на другие ресурсы информационной системы, используемые в банке. К банковской информации относят сведения о банке, его клиентах, сделках, платежах.

Систему условий и факторов, которые создают состояние опасности нарушения целостности информации банка, называют угрозами. На данный момент угрозы ИБ имеют разный характер. Они классифицируются по различным признакам. Классификация угроз ИБ банка представлена в таблице 1.

Таблица 1 – Классификация угроз ИБ банка

Признак	Виды угроз ИБ
Направленность угрозы ИБ	• Угрозы конфиденциальности (сведения становятся известными субъектами, которые не имеют к ней доступа, например, персональные данные клиента); • Угрозы целостности (сведения подвергаются модификации, причем, это может происходить как от умышленных действий, так и от нарушения работы оборудования); • Угрозы доступности (доступ к сведениям блокируется).
Расположение источника угрозы ИБ	• Внутренние (источник угрозы располагается в банковской организации, например, сотрудник); • Внешние (источник угрозы располагается во внешней среде, например, мошенники).

Природа возникновения	• Естественные (возникают в связи с воздействием объективных физических процессов, стихийных бедствий, т.е. они не зависят от воли человека); • Искусственные (возникают в связи с воздействием человека на информационную среду банка, например, хакерские атаки).
Объем наносимого ущерба	• Общие (т.е. ущерб наносится всей организации в целом, наносимый ущерб считается значительным); • Локальные; • Частные.

Источники угроз ИБ можно разделить на 2 группы: субъекты и объективные источники. Их цель – получения доступа к охраняемой информации, её изменение, уничтожение.

Обеспечение ИБ – важная задача банка, которая осуществляется посредством реализации различных мероприятий. К ним относят правовые, организационные, маркетинговые, кадровые, аналитические, прогностические и др. меры. Все они направлены на обнаружение, сдерживание, ликвидацию, минимизацию угроз и их последствий.

Рассмотрим некоторые инструменты защиты ИБ банка.

1. Программные средства. Данный инструмент позволяет ограничить доступ посторонних лиц. Он может быть реализован с помощью разграничения доступа на мандатной основе, то есть доступ должен быть только у тех пользователей, у которых есть официальное разрешение на работу с этими данными;

2. Аутентификация электронных данных; Аутентификация представляет собой процесс по проверке у субъекта наличия права доступа к информации. Это некий промежуточный этап предоставления доступа пользователю. Аутентификация может осуществляться разными способами: ввод логина и пароля, электронный сертификат, биометрические устройства. Как разновидность выделяют двухфакторную аутентификацию. Она работает следующим образом. Сначала вводится ключ №1, чаще это логин и пароль. Затем ключ №2, как правило, это цифровой код, который приходит на телефон через SMS.

3. Организация антивирусной защиты очень важна, так как постоянно появляются новые компьютерные вирусы. Система антивирусной защиты, которая используется в банке, должна быть надежной, масштабируемой, открытой, совместимой и унифицированной. Также она должна быть многофункционaльной (возможность удаленного управления, наличие системы оповещений о происходящих событиях, защита от разных видов вирусов). При этом

защите от вирусов подлежат все компоненты банковской информационной системы, связанные с передачей данных и/или их хранением: файл-серверы; рабочие станции; рабочие станции мобильных пользователей; сервера резервного копирования; сервера электронной почты.

4. К правовым мерам защиты информации банка относят разработка локальных нормативных актов, в которых прописаны задачи, права и обязанности сотрудников по работе с конфиденциальной информацией.

5. Регулярный контроль системы защиты информации с целью выявления изменений в сетевых компонентах, произошедших в нерабочее время;

6. Организация защиты помещений, в которых происходит работа с конфиденциальной информацией.

В поддержании защиты информации кредитных организаций важную роль играет ЦБ РФ. Одним из инструментов ИБ является структурное подразделение ЦБ РФ – ФинЦЕРТ. Данное подразделение представляет собой центр по мониторингу и реагированию на компьютерные атаки в кредитно-финансовой сфере. На данный момент в информационном обмене с ФинЦЕРТ принимают участие более 800 организаций, в т.ч. все российские банки. Автоматизированная система обработки инцидентов (АСОИ) сегодня является основным каналом передачи сведений об инцидентах в Банк России.

Деятельность, осуществляемая ФинЦЕРТом, помогает быстро среагировать на возникающие угрозы в финансовой сфере, не допустить их распространения, а также минимизировать потери. Работа ФинЦЕРТа происходит следующим образом. Сначала участник информационного обмена сообщает о выявленном инциденте, угрозе или совершенной атаке. Затем ФинЦЕРТ дает рекомендацию по противодействию угрозе.

На сегодняшний день состояние ИБ банков нельзя назвать удовлетворительным. Этот вывод можно сделать на основе статистики операций, совершенных без согласия клиентов. Данные о количестве операций без согласия клиентов представлены на рис.1 [2].

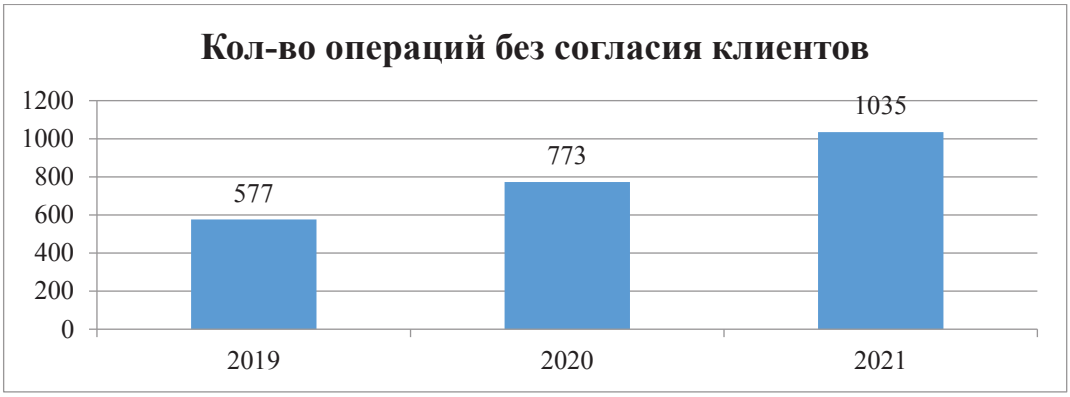

Рис. 1 – Данные о количестве операций без согласия клиентов за 2019-2021 гг. (тыс. ед.)

За анализируемый период рост составил 79,38%, в 2020 году - 33,37%. Одной из причин этого стал переход к дистанционным способам оплаты людьми, которые до введения карантинных мер оплачивали покупки в точках продажи. Данная категория оказались не готова к таким преобразованиям, в результате чего они были уязвимы перед мошенниками. В 2021 году также наблюдается рост количества операций без согласия клиентов (составил 33,89%). Данное изменение было на фоне развития дистанционных платежных сервисов, а также роста объема денежных переводов.

По данным департамента ИБ Банка России все операции без согласия клиентов (ОБС) делятся на 3 типа [3]:

1. Операции через банкоматы, терминалы и импринтеры;
2. Оплата товаров и услуг в Интернете (CNP-транзакции);
3. Операции в системе ДБО.

На основании проанализированных угроз, источников и инструментов, ИБ, а также статистки, предлагаются следующие рекомендации для банков по повышению уровня ИБ:

1. Создание в структуре банка подразделения, осуществляющего функции по защите конфиденциальных сведений;
2. Детальная работа с сотрудниками, работающими с конфиденциальной информацией. Сюда входит в первую очередь проверка кандидатов на данные должности, а также разработка банком положений для сотрудников, работающих с конфиденциальной информацией;
3. Внедрение в компьютерную сеть банка антивирусных программ (Kaspersky Internet Security, Avast Premium Security и др.);
4. Информирование клиентов о существующих мошеннических схемах.

Таким образом, обеспечение информационной безопасности — это одна из наиболее актуальных проблем для каждого банка. Несмотря

на возросший уровень угроз информационной безопасности, банки должны совершенствовать систему и инструменты по защите информации.

Список использованных источников

1. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. 1994. ЛИ- 12. С. 5. (1).

2. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году [Электронный ресурс] – Режим доступа: https://cbr.ru/analytics/ib/operations_survey_2021/

3. Аналитика ФинЦЕРТ [Электронный ресурс] – Режим доступа: https://cbr.ru/analytics/ib/fincert/#a_119486

УДК 364.013

А.Г. Цололо
Министерство финансов Нижегородской области
Нижний Новгород, Россия

ПРАВОВЫЕ ОСНОВЫ ГОСУДАРСТВЕННОГО (МУНИЦИПАЛЬНОГО) СОЦИАЛЬНОГО ЗАКАЗА НА ОКАЗАНИЕ ГОСУДАРСТВЕННЫХ (МУНИЦИПАЛЬНЫХ) УСЛУГ В СОЦИАЛЬНОЙ СФЕРЕ

Аннотация. *В статье рассматриваются правовые основы инструментов, используемых государством, с целью реализации поставленных в Конституции Российской Федерации задач, обеспечивающих доступ заинтересованных негосударственных организаций к реализации государственных (муниципальных) услуг в социальной сфере и средствам бюджета.*

A.G. Tsololo
Ministry of Finance of the Nizhny Novgorod Region
Nizhny Novgorod, Russia

LEGAL BASIS OF THE STATE (MUNICIPAL) SOCIAL ORDER FOR THE PROVISION OF STATE (MUNICIPAL) SERVICES IN THE SOCIAL SPHERE

Abstract. *The article examines the legal basis of the tools used by the state to implement the tasks set out in the Constitution of the Russian Federation, ensuring access*