УДК 336.719.2

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Романова П.А., студентка 4 курса экономического факультета
Научный руководитель – Голубева С.А.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *банковская деятельность, информационная безопасность, кредитная организация, угрозы, правовое регулирование, платежные процессы, риск.*

В условиях развития финансовых технологий и усиления экономической нестабильности все чаще поднимается вопрос безопасности банков. В данной статье мы подробно разберем, как же обеспечить информационную безопасность в сфере банковской деятельности.

Информационная безопасность банка – это состояние защищенности информационных активов финансового учреждения от различных рисков.

Достаточная степень обеспечения информационной безопасности финансовой организации благотворно влияет на минимизацию следующих видов рисков:

- риск утечки/разглашения сведений, составляющих коммерческую банковскую тайну;
- риск использования неполной или недостоверной информации в деятельности банковской структуры;
- риск распространения во внешней среде информации, которая может угрожать репутации или престижу финансового учреждения [1].

К основным источникам угроз информационной безопасности банковских структур можно отнести:

1. внешние и внутренние нарушители правил безопасности информационной базы, злонамеренные и незлонамеренные;

2. технические сбои и поломки программного обеспечения и компьютеров, составляющих основу информационных систем безопасности банка;

3. непредвиденные природные и техногенные катастрофы, влияющие на нормальное функционирование информационных базовых систем [1].

Для повышения экономической безопасности особое внимание уделяют кадровым вопросам, в том числе подбору и изучению сотрудников, как наемных, так и действующих, проверке различной информации, которая может свидетельствовать об их сомнительном поведении и компрометирующих отношениях. В рамках повышения экономической безопасности обязательны также разъяснительные беседы и инструктажи с персоналом, регулярные инструктажи по правилам и мерам безопасности, частые, но неожиданные для работников, опросы различных категорий работников.

Программно-аппаратный элемент защиты информации используется для защиты конфиденциальной информации, которая обрабатывается и хранится в персональных компьютерах, компьютерных сетях и различных информационных системах, используемых в банковской деятельности. Аппаратные средства защиты информации – это специальное техническое устройство, используемое для защиты информации от неправомерного распространения, утечки или доступа.

Правовая защита информации необходима для обеспечения государственной правовой базы и нормативного обоснования общей системы защиты информации. Помимо законодательных и нормативных актов и документов, правовое обеспечение комплекса защиты сведений, составляющих коммерческую тайну, включает систему внутренней документации, которая состоит из следующих элементов:

- устав банковской структуры;
- коллективный трудовой договор;
- трудовые договоры с работниками финансового учреждения и др. [1].

Если говорить о модели угроз, уменьшающих стабильность банковского сектора, можно утверждать, что внешние риски

признаются более существенными, чем инсайдерские. С учетом понимания модели угроз формируются требования к обеспечению информационной безопасности банковской системы:

- адекватность, создание жизнеспособных ответов на внутренние и внешние угрозы;

- комплексный подход, требующий внимания ко всем элементам банковской системы – от сервиса быстрых платежей до ежедневного резервного копирования баз данных;

- высокая производительность – система должна мгновенно обрабатывать огромные объемы данных, не создавая чрезмерной нагрузки на инфраструктуру;

- надежность, отказоустойчивость, способность восстанавливаться после сбоев в кратчайшие сроки;

- наличие широкого набора средств мониторинга, способных выявлять все виды уязвимостей в системе информационной безопасности банков [1].

В настоящее время в соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, Банк России определен как орган, формирующий организационную основу информационной системы безопасности Российской Федерации, а организации кредитно-финансового сектора – как участники этой системы.

В процессе рассмотрения мер по обеспечению конфиденциальности персональных данных можно выделить следующие рекомендации:

– никому не сообщайте свой пароль и ПИН-код (даже сотрудникам банка, так как они ни при каких обстоятельствах не имеют права требовать пароль пользователя);

- использовать один компьютер (избегайте смены паролей и совершения платежей с неизвестных компьютеров, имеющих доступ ко многим пользователям);

– при работе на чужом компьютере, ни в коем случае не сохранять ключ электронно-цифровой подписи;

– если существуют подозрения о том, что кто-то подсмотрел пароль, обратиться в банк и заблокировать доступ в систему;

– в случае хищения личных данных или денежных средств со счетов проинформировать банк о случившемся и подать заявление.

В условиях сложившейся геополитической ситуации налицо тенденция к переходу на национальную платежно-карточную систему. Это, в свою очередь, требует повышения надежности и безопасности банковских информационных систем. Все эти факторы привели к последующему переизданию стандартов СТО БР ИББС. Этот стандарт является очень важной вехой в эволюционном развитии системы домашней информационной безопасности. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы является одним из первых отраслевых стандартов, адаптированных к российской действительности. Многие банки соблюдают требования стандарта и готовятся к международной сертификации безопасности платежных систем PCI DSS, чтобы обеспечить защиту персональных данных в соответствии с последними требованиями регуляторов [1].

Резюмируя, можно сказать, что, поскольку банковские системы очень важны в экономическом смысле, их ИТ-безопасность обязательно будет гарантирована. Поскольку информация в базе данных банков представляет реальную материальную ценность, требования к хранению и обработке этой информации всегда будут повышены.

Специфика и особенности системы безопасности, безусловно, индивидуальны для каждой банковской организации, поэтому комплексное и профессиональное обеспечение системами безопасности является необходимым условием функционирования всей банковской системы.

Библиографический список:

1. Борисова, Е.С. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы / Е.С. Белоусова, А.Л. Белоусов // Актуальные проблемы экономики и права. – 2019. – Том 13, № 3. – С. 1330 – 1343.

ENSURING INFORMATION SECURITY IN THE FIELD OF BANKING

Mikhailova A.V.

Keywords: *banking, information security, credit organization, threats, legal regulation, payment processes, risk.*

In the context of the development of financial technologies and increased economic instability, the issue of bank security is increasingly being raised. In this article, we will analyze in detail how to ensure information security in the field of banking.