УДК 347.73

КОНТРОЛЬ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В БАНКАХ

Полякова Любовь Григорьевна,
Могилевский государственный университет имени А. А. Кулешова
(г. Могилев, Республика Беларусь)

В статье анализируются важнейшее направление контрольной деятельности в банковской сфере, связанное обеспечением безопасности информационных ресурсов, требующее комплексного подхода их защиты, учитывая как технические, так и правовые аспекты.

В процессе банковской деятельности используется различная по своей правовой природе информация – информация о банке, его клиентах, иных субъектах, совершаемых платежах, об операциях по публичным обязательствам, которая имеет различный правовой режим и, как правило, высокую экономическую ценность. Осуществление банковской деятельности напрямую связано с получением, обработкой, хранением и использованием экономически ценной информации и образует информационные ресурсы банков.

Электронный архив библиотеки МГУ имени А.А. Кулешова

В условиях стремительного развития информационных технологий, которые охватывают практически все сферы человеческой деятельности, вопросы информационной безопасности в банках приобретают первостепенную важность. Информационная безопасность в банках должна быть приоритетом для всех участников банковских правоотношений, чтобы защитить конфиденциальность и целостность информационных ресурсов банков, а также доступность информации, обрабатываемой банками для целей банковской деятельности.

Основными целями обеспечения информационной безопасности банка являются повышение надежности защиты информации в процессе ее обработки, хранения и передачи; выявление уязвимостей системы обеспечения информационной безопасности; предупреждение реализации угроз, минимизация ущерба от реализации угроз информационной безопасности; повышение деловой репутации банка, которые достигаются при соблюдении правил и требований информационной безопасности, необходимых для получения оптимального баланса между надежностью и оперативностью функционирования банка.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации: доступности информации для легальных пользователей (устойчивого функционирования информационной системы банка, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время); целостности информации, хранимой и обрабатываемой в информационной системе банка и передаваемой по каналам связи; конфиденциальности – сохранение в тайне определенной части информации в процессе ее хранения, обработки и передачи.

Обеспечение информационной безопасности в банках – это системный процесс, требующий разработки комплекса мероприятий, которые направлены на снижение потерь до минимального уровня и уменьшат вероятность наступления рисков в будущем.

В соответствии со статьей 26 Банковского кодекса Республики Беларусь одной из важнейших функций Национального банка является установление для банков обязательных требований к защите информационных ресурсов и информации, распространение и предоставление которых ограничено, а также осуществление контроля за обеспечением безопасности и защиты информационных ресурсов в банках [1].

В этой связи для обеспечения защиты информационных ресурсов в банках разрабатывается политика информационной безопасности, включающая в себя обязательные требования к защите информации, используемой в процессе банковской деятельности, а также требования к защите информационных ресурсов и информационных систем банков.

Электронный архив библиотеки МГУ имени А.А. Кулешова

Политика информационной безопасности направлена на защиту субъектов информационных отношений банка от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизацию уровня операционного риска, риска нанесения урона деловой репутации банка, правового риска. Система обеспечения безопасности информации банка предусматривает комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

Одним из актуальных направлений обеспечения информационной безопасности банков Республики Беларусь является обеспечение кибербезопасности в банковской сфере [2]. Требования по защите информации и обеспечению кибербезопасности распространяются на автоматизированные системы, информационные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, используемые при оказании банковских услуг и применяемые для обработки защищаемой информации.

С целью своевременного выявления и предотвращения утечки информации по техническим каналам за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации, в банке осуществляется, прежде всего, внутренний контроль эффективности безопасности и защиты информации. Его основная цель – оценка системы обеспечения информационной безопасности банка, которая должна гарантировать эффективное решение ряда задач, среди которых своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности; создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации; защиту от вмешательства в процесс функционирования информационной системы банка посторонних лиц и др. Важная задача, которая решается в процессе осуществления контроля, – это оценка существующей системы и средств защиты, их анализ с целью совершенствования эффективности данных систем и средств.

Таким образом, осуществляемый банками внутренний контроль существующей системы безопасности и защиты информации, его эффективности является необходимым условием для выявления и предотвращения

Электронный архив библиотеки МГУ имени А.А. Кулешова

утечки информации по техническим каналам, несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, которые направлены на уничтожение информации, разрушение средств информатизации, и направлен на совершенствование критериев и методов оценки эффективности этих систем и средств.

Список использованных источников

1. Банковский кодекс Республики Беларусь : 25 окт. 2000 г., № 441-З : принят Палатой представителей 3 окт. 2000 г. : одобр. Советом Респ. 12 окт. 2000 г. : в ред. Закона Респ. Беларусь от 17 февр. 2025 г., № 62-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 03.10.2025).
2. Об утверждении Концепции обеспечения кибербезопасности в банковской сфере : постановление Правления Национального банка Респ. Беларусь от 20 нояб. 2019 г. № 466// ЭТАЛОН : информ.-поисковая система (дата обращения: 03.10.2025).
3. Станкуть, В. М. Проблемы обеспечения сохранности конфиденциальной информации // В. М. Станкуть, Е. С. Януль // Промышленно-торговое право. – 2015. – № 3. – С. 29–34.

Электронный архив библиотеки МГУ имени А.А. Кулешова