УТВЕРЖДЕНО
Протокол правления
ОАО «Белагропромбанк»
27.08.2020 № 72
(в редакции
протокола правления
ОАО «Белагропромбанк»
04.04.2023 № 25)

ПОЛИТИКА
информационной безопасности
ОАО «Белагропромбанк»

ОАО «Белагропромбанк» (далее – банк) является универсальным банком и на основании лицензии Национального банка на осуществление банковской деятельности оказывает все основные виды банковских услуг.

Оказание банковских услуг осуществляется в соответствии с Уставом банка, с применением современных информационных технологий. В этих условиях банк уделяет особое внимание решению задачи обеспечения информационной безопасности (далее – ИБ).

Развитие сферы применения информационных технологий в банке осуществляется с учетом выполнения требований законодательства в области ИБ, защиты персональных данных, стандарта в области менеджмента ИБ ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Законодательной основой настоящей Политики являются Конституция Республики Беларусь, Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных», постановления правления Национального банка и приказы Оперативно-аналитического центра при Президенте Республики Беларусь в области ИБ.

Деятельность банка в области ИБ учитывает современное состояние и ближайшие перспективы развития информационных технологий, основные принципы создания систем ИБ, способных нейтрализовать современные вызовы и угрозы. Основополагающей целью ИБ является минимизация потенциального ущерба вследствие нарушения целостности, конфиденциальности или доступности информации, что достигается:

поддержанием функционирования системы защиты информации информационных систем банка в соответствии с требованиями законодательства, выполнением правовых, организационных мер, а также мер по технической и криптографической защите персональных данных;

реализацией комплекса мероприятий по подержанию функционирования системы информационной безопасности критически важного объекта информатизации (далее – СИБ КВОИ);

обеспечением функционирования системы менеджмента информационной безопасности (далее – СМИБ) в соответствии с требованиями стандарта ISO/IEC 27001;

минимизацией возможного ущерба от инцидентов информационной безопасности, регулярным анализом, оценкой и максимальным снижением рисков, оперативным реагированием на инциденты и ликвидацией их последствий.

Руководство банка осознает важность и необходимость развития и совершенствования мер и средств обеспечения ИБ в контексте развития законодательства, правил регулирования банковской деятельности, совершенствования международных стандартов в области ИБ, развития банковских технологий, а также ожиданий клиентов и других заинтересованных сторон. Обеспечение адекватного уровня ИБ является одним из ключевых факторов для банка.

В банке реализуется процессный и риск-ориентированный подходы к ИБ. Оценка рисков ИБ осуществляется с учетом общей стратегии и целей банка. Посредством оценки рисков ИБ выявляются угрозы активам, определяются уязвимости и степень вероятности их реализации, оценивается степень тяжести последствий в случае реализации угроз. Результаты оценки рисков ИБ учитываются при определении соответствующих управленческих решений и мер, выбранных для защиты от угроз, связанных с рисками. Работоспособность и улучшение СМИБ и СИБ КВОИ поддерживаются посредством мониторинга и оценки ее функционирования в соответствии со стратегией и целями банка.

В банке реализованы предусмотренные законодательством организационные, правовые и технические меры по защите информации, в том числе меры по идентификации и аутентификации, управлению доступом к информационным активам, обращению с носителями информации, защите от вредоносного программного обеспечения, управлению процедурами резервирования и восстановления работоспособности, управлению конфигурацией и обновлениями программного обеспечения, планированию мероприятий по обеспечению ИБ, реагированию на события ИБ, информированию и обучению персонала и другие.

Цели управления и средства управления ИБ подвергаются как внешнему, так и внутреннему аудиту на ежегодной основе. Департамент кибербезопасности контролирует соблюдение требований по ИБ в рамках деятельности банка, а также в отношениях с поставщиками и подрядчиками.

Настоящая Политика является документом, доступным любому работнику банка и пользователю его ресурсов, представляет собой официально принятую руководством банка систему взглядов на проблему обеспечения ИБ.

Требования Политики распространяются на все структурные подразделения банка, включая региональные дирекции, центры банковских услуг, дополнительные офисы, Центр сопровождения банковских операций, на всех работников, а также лиц, работающих с банком по договору подряда, стажеров, практикантов и т.д. Основные требования настоящей Политики также распространяются на другие организации и учреждения, взаимодействующие с

банком в качестве поставщиков и потребителей информационных ресурсов банка в том или ином качестве.

Требования настоящей Политики развиваются другими локальными правовыми актами банка, которые дополняют и уточняют ее.

Департамент кибербезопасности