Утверждено Советом Банка
Протокол № 8 от 24.04.2020

ПОЛИТИКА

информационной безопасности

ООО КБ «Евроазиатский Инвестиционный Банк»

(редакция от «30» апреля 2020 г.)

г. Москва

СОДЕРЖАНИЕ

I.ВВЕДЕНИЕ

1. Общие положения

1.1. «Политика информационной безопасности (далее - Политика) ООО КБ «Евроазиатский Инвестиционный Банк» (далее - Банк)» разработана в соответствии с законодательством Российской Федерации в части обеспечения информационной безопасности и защиты информации, требованиями Банка России, Федеральных служб, уполномоченных в области безопасности, надзора в сфере связи, информационных технологий и массовых коммуникаций.

1.2. Настоящая Политика является основополагающим документом, определяющим официально принятую руководством Банка систему приоритетов, целей, принципов и методов обеспечения информационной безопасности Банка. Наряду с другими документами системы менеджмента информационной безопасности, Политика определяет взаимосвязанною совокупность общих требований, основополагающих принципов, а также регламентов и инструкций в области обеспечения информационной безопасности и защиты информации, которыми Банк руководствуется в своей деятельности.

1.3. Руководство Банка осознает важность защиты конфиденциальной информации, необходимость развития, совершенствования принимаемых организационных мер и используемых технических средств обеспечения информационной безопасности в контексте совершенствующегося законодательства, норм регулирования банковской деятельности, развивающихся информационных технологий.

2. Термины и определения

2.1. **Автоматизированная система (АС)** — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая заданную технологию.

2.2. **Аудит информационной безопасности (аудит ИБ)** — систематический, независимый и документируемый процесс получения свидетельств деятельности Банка по обеспечению информационной безопасности, установления степени выполнения в Банке критериев информационной безопасности, а так же допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности Банка.

2.3. **Информационная безопасность (ИБ)** — безопасность, связанная с угрозами в информационной сфере.

2.4. **Информационный актив (ресурс) —** информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для Банка; находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи формы.

2.5. **Информационная сфера —** представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

2.6. **Система менеджмента информационной безопасности (СМИБ) —** часть

менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

2.7. **Система информационной безопасности (СИБ)** — совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

2.8. **Система обеспечения информационной безопасности (СОИБ)** — совокупность СИБ и СМИБ Банка.

3. Роли сотрудников в ИБ

3.1. **Куратор информационной безопасности (Куратор СМИБ)** — назначается из состава руководителей Банка и курирует в Банке вопросы обеспечения информационной безопасности, разработки и поддержки СМИБ.

3.2. **Координатор СМИБ** — сотрудник Банка, ответственный за планирование, реализацию, мониторинг, анализ, поддержку и совершенствование СМИБ.

3.3. **Контролер документации СМИБ** — сотрудник Банка, ответственный за контроль исполнения документации СМИБ.

3.4. **Сотрудник** — работник Банка, а также лицо, приравненное к работнику в правах и обязанностях, имеющий доступ к информационным ресурсам.

II. ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ

4. Область применения

4.1. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна к исполнению всеми его сотрудниками и должностными лицами при использовании информационных ресурсов Банка.

4.2. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Банка, а также в договорах с контрагентами.

4.3. Положения настоящей Политики обязательны для исполнения сотрудниками и представителями других организаций, являющихся контрагентами Банка, при использовании ими информационных ресурсов Банка в рамках заключенных Банком договоров.

5. Объекты защиты

5.1. Информация, составляющая коммерческую, банковскую тайну, относящаяся к переводам денежных средств, содержащая персональные данные или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы (конфиденциальная информация), а также любая открытая (общедоступная) информация, необходимая для деятельности Банка, независимо от формы и вида ее представления.

5.2. Процессы обработки информации в информационных системах Банка, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации.

5.3. Информационная инфраструктура, включающая автоматизированные системы обработки и анализа информации; технические и программные средства вычислительной

техники; средства передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникационное оборудование; системы и средства защиты информации; объекты и помещения, в которых размещены компоненты информационной инфраструктуры Банка.

6. Цели обеспечения ИБ

6.1. Под обеспечением ИБ или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

6.2. Целями обеспечения ИБ являются:

– защита от несанкционированного доступа и распространения конфиденциальной информации и её использования в личных целях;

– обеспечение целостности информации;

– обеспечение доступности информационных ресурсов;

– минимизация ущерба от реализации угроз ИБ;

– повышение деловой репутации и корпоративной культуры Банка.

7. Принципы обеспечения ИБ

7.1. Информация является важнейшим активом Банка, и ее защита является обязанностью каждого сотрудника.

7.2. Обеспечивается защита конфиденциальной информации от несанкционированного доступа и распространения, а также от использования в личных целях.

7.3. Доступ к информации предоставляется только тем лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

7.4. Для информационных ресурсов определяются уполномоченные лица, отвечающие за предоставление к ним доступа и эффективное функционирование мер защиты информации.

7.5. Сотрудники Банка проходят инструктаж, обучение и проверку знаний в области информационной безопасности.

7.6. Система управления ИБ Банка строится на основе отраслевых, национальных и международных стандартов в области обеспечения и управления ИБ.

7.7. Риски, связанные с ИБ, рассматриваются как часть операционного риска и контролируются в рамках существующей в Банке системы оценки и управления банковскими рисками.

7.8. Необходимость внедрения мер защиты информации определяется требованиями нормативных документов, а также возможным влиянием реализации угроз ИБ на финансовые результаты деятельности Банка и его деловую репутацию.

III. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

8. Система менеджмента информационной безопасности

8.1. СМИБ представляет собой составную часть корпоративной системы управления Банком, которая направлена на содействие достижению целей Банка путем обеспечения защищенности его информационной сферы.

8.2. Отдел информационной безопасности инициирует пересмотр порядка обеспечения защиты информации, в связи с изменениями требований к защите информации, определенных правилами платежной системы и иными новыми нормативными документами регуляторов.

8.3. Отдел информационной безопасности производит плановую проверку актуальности всех внутренних нормативных документов в зоне ответственности своего отдела, раз в два года, с целью определения необходимости ее пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обеспечению информационной безопасности по требованиям регуляторов. Плановая проверка актуальности проводится Координатором СМИБ. В результате проверки устанавливается возможность продления или необходимость пересмотра действующей редакции документа. Информация о проведенной проверке заносится в прилагаемый Лист записей о проверках актуальности документа (см. Приложение 1).

8.4. Пересмотр документов производится по решению Председателя Правления Банка по результатам плановой проверки актуальности, в случае выявления несоответствия определенного Политикой комплекса защитных мер фактам зафиксированных инцидентов информационной безопасности, при существенных изменениях в бизнес-задачах или при изменениях нормативной базы в области обеспечения информационной безопасности.

IV. УПРАВЛЕНИЕ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9. Руководство

9.1. Общее руководство обеспечением информационной безопасности Банка осуществляют Совет Банка, Правление и Председатель Правления Банка.

9.2. Правление Банка назначает Куратора информационной безопасности (Куратора СМИБ) из числа руководства Банка. Куратор информационной безопасности (Куратор СМИБ) не должен быть одновременно куратором информационных технологий Банка.

9.3. Председатель Правления назначает Координатора СМИБ, который организует текущую деятельность по созданию и поддержке функционирования СМИБ.

9.4. Ответственность за реализацию мероприятий СИБ и общий контроль за соблюдением требований ИБ в Банке несет Отдел информационной безопасности Банка, который разрабатывает и вносит предложения по изменению политик информационной безопасности Банка, а также участвует в создании, поддержании, эксплуатации и совершенствовании СОИБ Банка.

9.5. Руководители структурных подразделений Банка несут ответственность за обеспечение выполнения требований ИБ в своих подразделениях.

10. Контроль и аудит

10.1. Председатель Правления назначает приказом Контролера документации СМИБ, который контролирует исполнение документов СМИБ.

10.2. Для оценки СМИБ применяется самооценка и внешний аудит.

10.3. Служба внутреннего аудита Банка в соответствии с планом проверок, утвержденным Советом Банка, осуществляет проверку надежности функционирования системы внутреннего контроля за использованием автоматизированных информационных систем, включая контроль целостности баз данных и их защиты от несанкционированного доступа и (или) использования.

11. Ответственность

11.1. Сотрудники Банка, виновные в нарушении требований Политики и иных внутренних нормативных документов Банка, входящих в СМИБ, а также в несоблюдении мер, предусмотренных СОИБ, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

V. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12. Условия и порядок контроля актуальности и пересмотра

12.1. Плановая проверка актуальности Политики проводится раз в два года или по мере изменения в законодательстве, с целью определения необходимости ее пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обеспечению ИБ. В результате проверки устанавливается возможность продления или необходимость пересмотра действующей редакции Политики.

12.2. Пересмотр Политики производится по решению Правления Банка по результатам плановой проверки актуальности, в случае выявления несоответствия определенного Политикой комплекса защитных мер фактам зафиксированных инцидентов ИБ, при существенных изменениях в бизнес-задачах или при изменениях нормативной базы в области обеспечения ИБ.

12.3. Пересмотр Политики осуществляет Координатор СМИБ или специально назначаемая Правлением рабочая группа, которые готовят предложения по частичной переработке документа (выпуск/издание редакции с изменениями), либо полной (существенной) переработке документа (перевыпуск/переиздание в новой редакции).

12.4. Контроль исполнения Политики осуществляет Контролер документации СМИБ.

13. Приложения

13.1. Лист записей о версиях документа.

№ п.п.	Дата создания версии	Должность ответственного за разработку.	ФИО ответственного за разработку.
1.			
2.			
3.			
4.			
5.			