ПОЛИТИКА
информационной безопасности
АО «Jusan Bank»

АО «Jusan Bank» (далее – Банк) уделяет особое внимание вопросам обеспечения информационной безопасности, постоянно совершенствует систему управления информационной безопасностью, применяемые средства и способы защиты от угроз информационной безопасности, а также обеспечивает непрерывное обучение работников Банка для поддержания компетенции в области защиты информации на высоком уровне.

Данный документ разработан в соответствии с законодательством Республики Казахстан, требованиями стандарта Payment Card Industry Data Security Standard[1] и предназначен для открытой публикации на корпоративном веб-сайте Банка.

Документ описывает систему взглядов на вопросы обеспечения безопасности информации, основные принципы, направления и требования по защите информации и содержит основные разделы Политики информационной безопасности (далее - Политика), утвержденной Правлением Банка.

Политика охватывает все информационные активы/ресурсы, информацию и документы, владельцем и пользователем которых является Банк.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления коммерческой деятельности Банка. Информация является одним из важнейших банковских активов.

Основной целью, на достижение которой направлены положения Политики, является обеспечение надлежащей защиты информационных ресурсов Банка, недопущение и/или минимизация рисков информационной безопасности, и ущерба/вреда от событий, угрожающих безопасности информационных ресурсов Банка, посредством их предотвращения или сведения их последствий к минимуму.

Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами информационным ресурсам в ходе достижения стратегических целей Банка.

С этой целью необходимо поддерживать главные свойства информации, а именно:

1) доступность – свойство информации быть доступной и готовой к использованию по запросу авторизованного субъекта;

2) конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованных лиц объекта;

3) целостность – состояние неизменности данных.

Процесс создания надежной информационной защиты является непрерывным.

Построение системы обеспечения информационной безопасности Банка и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1) законности – любые действия, предпринимаемые для обеспечения информационной безопасности, основываются на действующем законодательстве Республики Казахстан с применением всех разрешенных мер, способов и методов обнаружения, предупреждения, локализации и пресечения незаконных, несанкционированных и иных негативных воздействий на информационные ресурсы Банка и иные объекты обеспечения информационной безопасности;

2) ориентированности на бизнес – информационная безопасность рассматривается, как процесс поддержки основной деятельности Банка; предпринимаемые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий для деятельности Банка;

3) непрерывности – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной безопасности осуществляются без прерывания или остановки текущих бизнес-процессов Банка;

---

[1] PCI DSS – стандарт безопасности данных индустрии платежных карточек, разработанный Советом по стандартам безопасности индустрии платежных карточек (Payment Card Industry Security Standards Council, PCI SSC), учрежденным международными системами Visa, MasterCard, American Express, JCB и Discover.

4) комплексности – обеспечение информационной безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических ресурсах и этапах их использования, и во всех режимах функционирования;

5) обоснованности - используемые возможности и средства защиты реализуются на соответствующем и достаточном уровне, обоснованы с точки зрения заданного уровня безопасности и соответствуют предъявляемым требованиям и нормам;

6) приоритетности – категорирования (ранжирования) всех информационных ресурсов Банка по их статусу и степени важности;

7) наименьшего уровня привилегий – пользователь (работник Банка) получает минимальный уровень привилегий и доступ только к тем данным, информационным системам и оборудованию Банка, которые являются необходимыми для выполнения им деятельности в рамках своих функциональных обязанностей;

8) специализации – эксплуатация технических средств осуществляется профессионально подготовленными работниками Банка;

9) информированности и персональной ответственности – руководители подразделений всех уровней и исполнители осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за невыполнение этих требований и несоблюдение установленных мер информационной безопасности;

10) взаимодействия и координации – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11) подтверждаемости – важная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, создаются и хранятся с возможностью оперативного доступа и восстановления;

12) эшелонированности защиты – комплекс различных механизмов защиты, дополняющих функционал друг друга, предназначенных для защиты информационного актива от несанкционированного доступа, обнаружения атак и реагирования на них, тем самым снижающий риск возникновения инцидента.

Основными объектами обеспечения информационной безопасности в Банке являются:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с законодательством Республики Казахстан и внутренними документами Банка к банковской коммерческой или иной охраняемой законом тайне, к персональным данным, к инсайдерской информации (далее – защищаемая информация);

2) средства и системы информатизации (средства вычислительной техники, информационно-коммуникационная инфраструктура, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) Банка, с помощью которых производится обработка, передача и хранение защищаемой информации;

4) бизнес-процессы Банка, связанные с управлением и использованием информационных ресурсов;

5) помещения, в которых расположены средства создания, обработки, передачи и хранения защищаемой информации;

6) рабочие помещения и кабинеты работников Банка, помещения Банка, предназначенные для ведения закрытых переговоров и совещаний;

7) работники Банка, имеющие доступ к защищаемой информации;

8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Виды информации, подлежащие защите:

1) на бумажных носителях;

2) в электронном виде (обрабатываемая, передаваемая средствами вычислительной техники, записываемая, хранимая и воспроизводимая с помощью технических средств и т.п.).

Положения Политики обязательны для исполнения всеми работниками Банка, стажерами, практикантами, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным активам Банка, в той их части, которая непосредственно взаимосвязана с их деятельностью в Банке.