ПОЛИТИКА
информационной безопасности
ЗАО «Халык Банк Таджикистан»

Содержание

Общие положения

ЗАО «Халык Банк Таджикистан» 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.

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

Нормативно-правовую основу Политики составляют законы и положения Республики Таджикистан по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.

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

Политика охватывает все информационные системы и документы, владельцем и пользователем которых является Банк. Обеспечение информационной безопасности – одно из условий для успешного осуществления коммерческой деятельности Банка. Информация, циркулирующая в Банке, является одним из важнейших банковских активов.

Информационными ресурсами Банка являются:

- средства и системы хранения, обработки, передачи информации (вычислительные системы и сети, линии телефонной, факсимильной, радио и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

- банковская информация с ограниченным доступом, составляющая служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;

- банковская информация, с ограниченным доступом, составляющая служебную и коммерческую тайну непосредственно доступная работникам Банка.

Информационные ресурсы Банка представляют собой собственно объекты защиты информации.

Под угрозой информационной безопасности понимается потенциальная возможность нарушения основных качеств или свойств информации – конфиденциальности, целостности, доступности и юридической силы (значимости).

Цели, требования и основные принципы

Основной целью для обеспечения информационной безопасности является минимизация ущерба от событий обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Банка.

Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами, присущим информационным ресурсам Банка. С этой целью необходимо поддерживать главные свойства информации, а именно:

- **конфиденциальность** – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

- **целостность** – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

- **доступность** – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

Процесс создания надежной информационной защиты является непрерывным. В целях обеспечения достаточно надежной системы ИБ необходима постоянная регулировка ее параметров, адаптация для отражения новых угроз, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Политику по мере возникновения такой необходимости.

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

- **законность** – любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Банка;

- **ориентированность на бизнес** – ИБ рассматривается как процесс поддержки основной деятельности Банка. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Банка;

- **непрерывность** – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Банка должны осуществляться без прерывания или остановки текущих бизнес-процессов Банка;

- **комплексность** – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования во всех режимах функционирования;

- **обоснованность и экономическая целесообразность** – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;

- **приоритетность** – категорирование (ранжирование) всех информационных ресурсов Банка по степени важности при оценке реальных, а также потенциальных угроз ИБ;

- **необходимое знание и наименьший уровень привилегий** – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

- **специализация** – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами Банка, его функциональных и обслуживающих подразделений;

- **информированность и персональная ответственность** - в Банке установлены требования к владению, классификации и индивидуальной ответственности должностных лиц, так или иначе имеющих отношение к информационным ресурсам. Установлена персональная ответственность руководителей всех уровней и исполнителей за выполнение требований и соблюдение установленных мер информационной безопасности. Банк отвечает за создание условий, обеспечивающих информационную безопасность;

- **взаимодействие и координация** - меры информационной безопасности осуществляются на основе четкой взаимосвязи соответствующих структурных единиц Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями (органами государственного управления, другими организациями и предприятиями);

- **подтверждаемость** – важная документация и все записи – документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Объекты защиты, область применения

Основными объектами обеспечения ИБ в Банке признаются следующие элементы:

- информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Банка к банковской и коммерческой тайне, персональным данным, финансовой информации, и любой иной информации, необходимой для обеспечения нормального функционирования Банка (далее – защищаемая информация);
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Банка, с помощью которых производится обработка защищаемой информации;
- процессы Банка, связанные с управлением и использованием информационных ресурсов;
- помещения, в которых расположены средства обработки защищаемой информации;
- рабочие помещения и кабинеты работников Банка, помещения Банка, предназначенные для ведения закрытых переговоров и совещаний;
- персонал Банка, имеющий доступ к защищаемой информации;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может:

- размещаться на бумажных носителях;
- существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
- передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;
- присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.
- Политика применяется ко всем работникам Банка и третьим лицам, так или иначе имеющим доступ к информационным ресурсам Банка или вовлеченным в процессы информационного обмена.

Угрозы информационной безопасности

Под угрозами ИБ понимается потенциальная возможность нарушения главных свойств информации.

Угрозы ИБ подразделяются на:

- случайные – стихийные бедствия, непреднамеренные ошибочные действия со стороны работников Банка, ошибки аппаратных и программных средств и т.д.;
- преднамеренные, т.е. умышленная фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

К числу угроз ИБ относятся (но не ограничены ими):

- утрата информации, составляющей банковскую тайну, коммерческую тайну Банка и иную защищаемую информацию;
- искажение (несанкционированная модификация, подделка) защищаемой информации;
- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);
- несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);

В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Банка и его нормальное функционирование:

- финансовые потери, связанные с утечкой, разглашением, или несанкционированной модификацией защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- финансовые потери, связанные с несанкционированными действиями в информационных ресурсах Банка;
- ущерб от дезорганизации деятельности Банка, финансовые и репутационные потери, связанные с невозможностью выполнения им своих обязательств;
- ущерб от принятия управленческих решений на основе необъективной информации;
- ущерб от отсутствия у руководства Банка объективной информации;
- ущерб, нанесенный репутации Банка и иной вид ущерба.

Меры по обеспечению информационной безопасности

Основными мерами по обеспечению ИБ Банка являются:

- административно-правовые и организационные меры;
- меры физической безопасности;
- программно-технические меры.

Административно-правовые и организационные меры включают (но не ограничены ими):

- контроль исполнения требований законодательства РТ и внутренних документов;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников Банка работе с информационными ресурсами и требованиям ИБ;
- реагирование на инциденты, локализацию и минимизацию последствий;
- анализ новых рисков ИБ;
- отслеживание и улучшение морально-делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников Банка.

Меры физической безопасности включают (но не ограничены ими):

- организацию пропускного и внутри-объектового режимов;
- построение периметра безопасности защищаемых объектов;
- организацию круглосуточной охраны режимных объектов, в том числе с использованием технических средств безопасности;
- организацию противопожарной безопасности охраняемых объектов;
- контроль доступа работников Банка в помещения ограниченного доступа.

Программно-технические меры включают (но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра (firewall, Intrusion Prevention System (IPS) и т.п.);
- применение комплексной антивирусной защиты;
- использование средств ИБ, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль над правами и действиями пользователей, в первую очередь привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств;
- мониторинг состояния критичных элементов информационных систем.

Соответствие требованиям

Настоящая Политика и система информационной безопасности в целом основываются на следующие нормативные правовые акты и международные стандарты, непосредственно влияющие на процесс создания системы информационной безопасности Банка. В то же время существует ряд документов, которые либо описывают стратегические аспекты развития информационной безопасности на государственном уровне, либо регламентируют правила по информационной защите отдельных приложений/ услуг.

- Закон Республики Таджикистан «О банковской деятельности» от 19 мая 2009 года за № 524;
- Закон Республики Таджикистан «Об электронной цифровой подписи» от 30 июля 2007 года за № 320;
- Закон Республики Таджикистан «О защите информации» от 2 декабря 2002 года за № 71;
- Постановление Правительства Республики Таджикистан «О Программе обеспечения информационной безопасности Республики Таджикистан» от 30 июня 2004 г. за № 290;
- Закон Республики Таджикистан «Об информации» от 03 июля 2012 года за № 848;
- Концепция информационной безопасности Республики Таджикистан от 7 ноября 2003 года за № 1175;
- Закон Республики Таджикистан «Об электронном документе» от 31 декабря 2014 года за № 1174;
- Международный стандарт ISO/IEC 27001:2013 «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования».

На основании Политики разрабатывается ряд подчиненных внутренних нормативных документов, регламентирующих конкретные правила и методы обеспечения информационной безопасности, частные политики в области действия стандартов и т.п. Такие документы могут дополнять и расширять требования Политики, но не могут вступать с ними в противоречие.

Благодарим Вас за ознакомление
с Политикой информационной безопасности
ЗАО «Халык Банк Таджикистан»