ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОАО «ХАЛЫК БАНК КЫРГЫЗСТАН»

СОДЕРЖАНИЕ

ОАО «Халык Банк Кыргызстан» 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 требованиями стандарта ISO 27001:2013 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования» и предназначен для открытой публикации на корпоративном веб-сайте Банка.

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 положения законодательства Кыргызской Республики и требования Национального Банка КР по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.

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

Основной целью, на достижение которой направлены все положения Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, 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 имеющимся информационным ресурсам Банка.

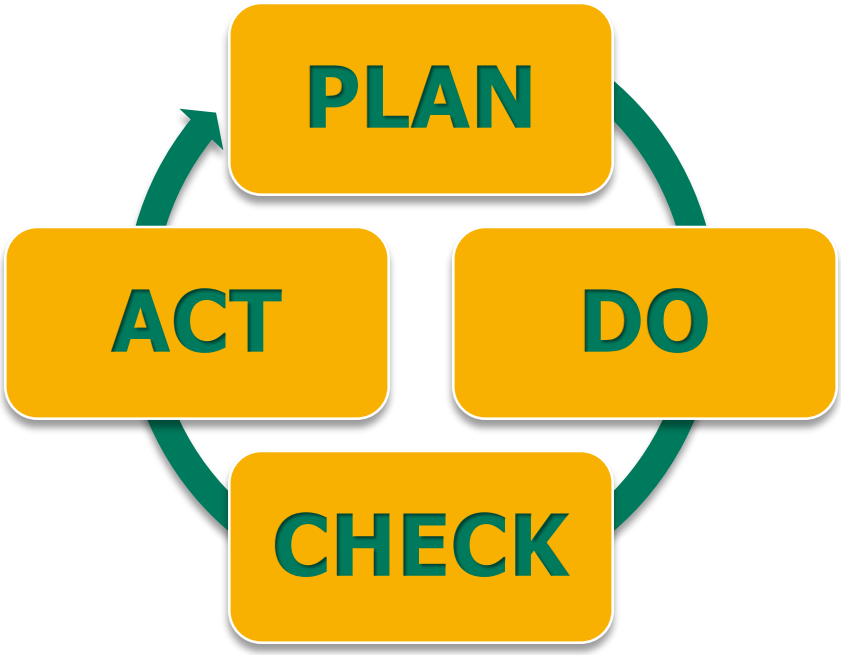
С этой целью необходимо поддерживать главные свойства информации, а именно:

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

Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, 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.

В соответствии с данным положением, определяются следующие этапы цикла управления информационной безопасностью (модель PDCA: Plan-Do-Check-Act).



PLAN – Планирование (разработка) – анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общей стратегией и целями Банка;
DO – Реализация (внедрение и эксплуатация) – внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно-аппаратных средств;
CHECK – Проверка (мониторинг и анализ) – оценка и там, где это применимо, измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;
ACT – Корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния информационной безопасности, требований со стороны руководства, иных факторов, в целях обеспечения непрерывного совершенствования системы информационной безопасности.

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

- законность – любые действия, предпринимаемые для обеспечения информационной безопасности, 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 – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности 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 и 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 должны 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 информационной безопасности;
- 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;
- информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;
- взаимодействие и координация – 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;
- подтверждаемость – важная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Основными объектами обеспечения информационной безопасности в Банке признаются следующие элементы:

- информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Банка к банковской тайне, коммерческой тайне Банка, любая иная информация, необходимая 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.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под угрозами информационной безопасности понимается потенциальная возможность нарушения главных свойств информации.

Угрозы информационной безопасности подразделяются на:

- случайные – стихийные бедствия, ошибки по невниманию, ошибки аппаратных и программных средств и т.д.;
- преднамеренные, т.е. фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

К числу угроз информационной безопасности относятся (но не ограничены ими):

- утрата информации, составляющих 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.);
- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств и злонамеренных действий.

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

- финансовые потери, связанные с утечкой или разглашением защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности Банка и 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;
- иной вид ущерба.

Нарушители информационной безопасности классифицируются следующим образом:

- внутренние нарушители – работники Банка, неосознанно либо злонамеренно нарушающие режим информационной безопасности;
- внешние нарушители – лица, не связанные с Банком трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Банка.

Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.
Основные типы внутренних нарушителей:

- «необученный/халатный работник» – работник Банка, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;
- «конкурирующий работник» – работник Банка, по личной неприязни либо по иным причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и в целом Банк;
- «заинтересованный нарушитель» – работник Банка, который заинтересован в неправомерных действиях по отношении к Банку третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Банком трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение – утечка информации (в случае заинтересованности собственной выгодой – финансовые мошенничества);

- «внедренный злоумышленник» – работник Банка, поступивший на работу с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Банком;
- «увольняющийся работник» – работник Банка, прекращающий с ним трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел непосредственный доступ;
- «обиженный работник» – работник Банка, резко неудовлетворенный параметрами трудовой деятельности либо, как вариант, руководство Банка явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений.

Основные типы внешних нарушителей (в данном разделе используется терминология, принятая на настоящий момент в сообществе специалистов по информационной безопасности):

- «Script Kiddie» или «Начинающий» – лицо, интересующееся взломом любого информационного ресурса, имеющего общеизвестные уязвимости. Не нацелен на взлом информационных ресурсов именно Банка, легко прекращает атаку в случае обнаружения серьезных средств защиты. Как правило, использует широко распространенные методы взлома, не разрабатывает собственных средств;
- «Black hat» – «Черный хакер» – в отличие от «Script Kiddie» более упорен во взломе конкретного ресурса, обход систем защиты считает «делом чести», может разрабатывать простые атакующие средства. Действует с целью самоутверждения или для извлечения личной выгоды, может продавать свои услуги криминальным структурам;
- «Консультант» – работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;

- «Elite hacker» или «Гуру» – высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае будет нацелен на проведение финансового мошенничества, во втором – либо на утечку информации, либо на недоступность серверов и компрометацию Банка в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;
- «Партнер» – работник организации-партнера либо дочерней организации, имеющих доступ к информационным системам Банка. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях информационной безопасности, принятых в Банке;
- «Стажер/практикант» – как правило, ограничен в доступе к информации и информационным системам, однако постоянно находится на территории Банка и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Банка, курирующего данного стажера/практиканта;
- «Клиент» – клиент Банка, имеющий доступ к его сервисам дистанционного банковского обслуживания. Может нанести урон при неправильном использовании данных сервисов, утере идентификационных данных, либо действовать как первые три типа внешних нарушителей, имея, пусть и ограниченный, доступ к информационным банковским ресурсам.

Основными мерами по обеспечению информационной безопасности 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 КР и ВНДБ;
- 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 системами и требованиям информационной безопасности;
- реагирование на инциденты, локализацию и минимизацию последствий;
- анализ новых рисков информационной безопасности;
- 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 внутриобъектового режимов;
- построение периметра безопасности защищаемых объектов;
- организацию круглосуточной охраны охраняемых 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, IPS и т.п.);
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей, в первую очередь, привилегированных;
- применение систем криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств;
- мониторинг состояния критичных элементов информационной системы.

Настоящая Политика и система информационной безопасности в целом опираются на следующие нормативные правовые акты и международные стандарты (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы информационной безопасности Банка в целом; в то же время существует ряд документов, который либо описывает стратегические аспекты развития информационной безопасности на государственном уровне, либо регламентирует правила по информационной защите отдельных приложений/ услуг):

- Закон Кыргызской Республики от 16 декабря 2016 года № 206 "О Национальном банке Кыргызской Республики, банках и банковской деятельности";
- Закон Кыргызской Республики от 19 июля 2017 года № 128 "Об электронной подписи";
- Закон Кыргызской Республики от 19 июля 2017 года № 127 "Об электронном управлении";
- Закон Кыргызской Республики от 14 апреля 2008 года № 58 "Об информации персонального характера";
- Положение о требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики утв. Постановлением Правления НБКР № 2021-П-20/72-8-(НПА) от 22 декабря 2021 года
- Стратегии кибербезопасности Кыргызской Республики на 2019-2023 годы утв. Постановлением Правительства КР № 369 от 24 июля 2019 года;
- Концепции цифровой трансформации "Цифровой Кыргызстан 2019-2023", одобренной решением Совета безопасности Кыргызской Республики от 14 декабря 2018 года № 2
- Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы утв. Постановлением Правительства КР № 209 от 3 мая 2019 года;
- Положение НБ КР "Об электронных деньгах в Кыргызской Республике" от 30 марта 2016 года № 15/6;
- Положение НБ КР "О минимальных требованиях по управлению рисками в банках Кыргызской Республики" от 15 июня 2017 года № 2017-П-12/25-8-(НПА)

- Международный стандарт по информационной безопасности ISO/IEC 27001:2013 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования»;
- Международный стандарт PCI DSS, версии 3.2.1 (Payment Card Industry Data Security Standard – стандарт безопасности данных индустрии платежных карт);
- Международный стандарт PCI 3DS (Core Security Standard) - стандарт безопасности для организаций, выполняющих или предоставляющих функции платежей без физического предоставления платежной карты;
- Концепция обеспечения безопасности пользователей (CSCF) SWIFT (далее – CSCF SWIFT);

В Банке внедрены соответствующие процессы для обеспечения соблюдения требований нормативных правовых актов, соблюдения прав интеллектуальной собственности, защиты охраняемой законом персональной информации, соблюдения ограничений по использованию криптографических средств.

Все требования и положения международных стандартов ISO/IEC 27001 и PCI DSS являются обязательными для исполнения в области их применения, определяемой соответствующими документами.

При разработке и применении средств и методов информационной безопасности учитываются требования договорных обязательств и контрактов, заключенных Банком с третьими сторонами.

Доступ третьей стороны к информационным ресурсам Банка осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер. В случае необходимости (в частности, при наличии требований нормативных правовых актов или международных стандартов), Банк проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям (например, проверку документов, подтверждающих соответствие предоставляемых услуг требованиям стандарта PCI DSS).

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 ОАО «ХАЛЫК БАНК КЫРГЫЗСТАН»