ПОЛИТИКА информационной безопасности

ТОО «Дочерняя организация Народного Банка Казахстана «Halyk Инкассация»

ҚАЗАҚСТАН ХАЛЫҚ БАНКІНІН ЕНШІЛЕС ҰЙЫМЫ

HALYK ИНКАССАЦИЯ

ДОЧЕРНЯЯ ОРГАНИЗАЦИЯ НАРОДНОГО БАНКА КАЗАХСТАНА

Содержание

Общие положения

ТОО «Дочерняя организация Народного Банка Казахстана «Halyk Инкассация» уделяет особое внимание вопросам обеспечения информационной безопасности, постоянно совершенствует систему обеспечения информационной безопасностью, применяемые средства и способы защиты от угроз информационной безопасности, а также обеспечивает непрерывное обучение своих работников для поддержания компетенции в области защиты информации на высоком уровне.

Настоящий документ разработан в соответствии с требованиями стандарта ISO 27001:2013 и предназначен для открытой публикации на корпоративном веб-сайте Компании.

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)*, проводимой руководством Компании.

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

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

Политика охватывает все информационные активы и документы, владельцем и пользователем которых является Компания. Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Компании.

Информация является одним из важнейших активов Компании.

Цели, требования и основные принципы

Основной целью, на достижение которой направлена Политики, является минимизация ущерба Компании от реализации идентифицированных рисков ИБ, посредством их предотвращения или сведения к минимуму их последствий.

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

- **конфиденциальность** – обязательное для выполнения субъектом, получившим доступ к защищаемой информации требование – не передавать такую информацию третьим лицам без согласия ее обладателя. А также свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью информационной системы/среды сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
- **целостность** – состояние информации, при котором любое её изменение осуществляется только преднамеренно и только субъектами, имеющими на это права/полномочия;
- **доступность** – состояние информационной системы Компании, при котором субъекты, имеющие права доступа к информации, могут реализовать эти права беспрепятственно, в рамках своих полномочий.

Процесс создания информационной защиты никогда не бывает законченным. Система обеспечения информационной безопасности, выстраиваемая Компанией постоянно совершенствуется и корректируется. Признаётся необходимость непрерывной регулировки её текущих параметров, адаптация СОИБ для отражения новых угроз, исходящих как из внешней среды, так и изнутри Компании.

Необходимые мероприятия по совершенствованию и корректировке настоящей Политики производится беспрепятственно, по мере возникновения такой необходимости

Политика определятся следующие этапы непрерывного цикла обеспечения информационной безопасности (модель PDCA: Plan-Do-Check-Act):

Plan – Планирование *(разработка)* – анализ рисков, определение 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 Компании;

Do – Реализация *(внедрение и эксплуатация)* – применение механизмов контроля, процессов, процедур, программно-аппаратных средств, для достижения запланированных целей;

Check – Проверка *(мониторинг и анализ)* – контроль, оценка и измерение характеристик процессов, проводимых в соответствии с Политикой. Анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов;

Act – Корректировка *(сопровождение и совершенствование)* – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния информационной безопасности, требований законодательства, иных факторов, в целях обеспечения непрерывного совершенствования системы информационной безопасности.

Цели, требования и основные принципы

Построение системы обеспечения информационной безопасности и её функционирование осуществляются в соответствии со следующими основными принципами:

- **Законность** – любые действия, предпринимаемые в рамках обеспечения ИБ, осуществляются на основе действующего законодательства Республики Казахстан с применением всех дозволенных методов предупреждения, обнаружения, пресечения и локализации негативных воздействий на объекты защиты информации Компании;

- **Бизнес-ориентированность** – обеспечение ИБ рассматривается как поддерживающий процесс основной деятельности Компании. Меры по обеспечению ИБ являются необходимо достаточными, при этом не препятствуют осуществлению деятельности Компании;

- **Комплексность** – обеспечение безопасности информационных материалов и ресурсов в течение всего их жизненного цикла на всех этапах их использования, во всех режимах функционирования;

- **Целесообразность** – используемые методы и средства защиты обоснованы с точки зрения заданного уровня безопасности, соответствуют предъявляемым экономическим требованиям и реализуются на современном уровне развития науки и техники. Стоимость мер и систем ИБ всегда меньше размера возможного ущерба от любых видов риска;

- **Приоритетность** – категорирование всех информационных материалов и ресурсов Компании по степени важности при оценке реальных угроз ИБ;

- **Достаточность** – уполномоченный субъект получает доступ исключительно к той информации и в том виде, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

Цели, требования и основные принципы

Построение системы обеспечения информационной безопасности и её функционирование осуществляются в соответствии со следующими основными принципами:

- **Специализация** – реализация мер информационной безопасности и связанная с этим эксплуатация технических средств осуществляются профессионально подготовленными специалистами Компании;

- **Ответственность** – сотрудники всех уровней руководствуются требованиями обеспечения информационной безопасности и несут персональную ответственность за нарушения и недостатки в данной сфере деятельности;

- **Координация** – информационная безопасность достигается во взаимодействии структурных подразделений Компании, а также АО «Народный Банк Казахстана», его дочерних организаций и координации их усилий для достижения поставленных целей, а также установления необходимых связей с государственными органами Республики Казахстан, прочими ведомствами, профессиональными ассоциациями и сообществами, юридическими и физическими лицами.

Основные объекты обеспечения информационной безопасности в Компании:

- защищаемая информация;
- информационные ресурсы, содержащие сведения, отнесенные к коммерческой, служебной, банковской тайне Компании, её партнёров и клиентов, персональные данные работников, партнёров и клиентов, любая иная информация, необходимая для обеспечения нормального функционирования Компании;
- персонал Компании, имеющий доступ к защищаемой информации;
- средства и системы информатизации, на которых производится обработка, передача и хранение защищаемой информации;
- программные средства, с помощью которых производится обработка защищаемой информации;
- процессы Компании, связанные с управлением и использованием информационных ресурсов;
- помещения, в которых расположены средства обработки защищаемой информации; рабочие помещения и кабинеты работников Компании, иные помещения, предназначенные для ведения закрытых переговоров и совещаний;
- технические средства и системы, предназначенные для обработки открытой информации, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может быть представлена в любом виде: электронном, письменном, устном и т.д.

Угрозы ИБ

(потенциальная возможность нарушения главных свойств информации)

подразделяются на:

Случайные

– ошибки аппаратных и программных средств; обстоятельства непреодолимой силы (форс-мажор); ошибки по невнимательности (человеческий фактор);

Преднамеренные

– умышленная фальсификация или уничтожение данных; неправомерное использование данных; компьютерные преступления и т.д.

К числу угроз ИБ относятся

(но не ограничиваются ими):

утрата защищаемой информации

искажение *(несанкционированная модификация, подделка)* защищаемой информации

несанкционированное ознакомление с защищаемой информацией посторонних лиц *(доступ, копирование, хищение)*

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, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств, а также злонамеренных действий;

В результате воздействия угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Компании и её 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 Компании;

- ущерб от дезорганизации деятельности Компании, финансовые и репутационные потери, связанные с невозможностью выполнения ей своих обязательств;

- ущерб от принятия управленческих решений на основе необъективной информации;

- ущерб от отсутствия у руководства Компании объективной информации;

- ущерб, нанесенный репутации Компании;

- иной вид ущерба.

В Компании принята следующая классификация моделей вероятных нарушителей ИБ:

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

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 служебной, клиентской и финансовой информации.

Основные типы внутренних нарушителей:

- «необученный/халатный» – работник Компании, по незнанию или по халатности допускающий нарушение, не несущее в себе злого умысла;
- «конкурирующий» – работник Компании, по каким либо причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и в целом Компания;
- «заинтересованный» – работник Компании, который заинтересован в неправомерных действиях третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Компанией трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение – утечка информации;

- «внедренный» – работник, поступивший в Компанию с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Компанией;

- «увольняющийся» – работник Компании, прекращающий с ней трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел непосредственный доступ;

- «ущемлённый» – работник Компании, резко неудовлетворенный параметрами трудовой деятельности либо, как вариант, руководство Компании явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений.

Основные типы внешних нарушителей:

- «кибер-преступник» или «хакер» – лицо, занимающееся взломом информационных ресурсов, как правило из глобальной сети Интернет, имеющее всевозможные цели: от любопытства до извлечения финансовой выгоды, и различную степень квалификации: от студента, использующего общеизвестные уязвимости, до высококвалифицированного кибер-преступника, действующего «под заказ» криминальных структур либо конкурирующих организаций;

- «консультант» – работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;

- «партнёр» – работник организации-партнёра, имеющей доступ к информационным системам Компании. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях информационной безопасности, принятых в Компании;

- «стажер/практикант» – как правило, ограничен в доступе к информации и информационным системам, однако постоянно находится на территории Компании и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Компании, курирующего данного стажера/практиканта;

- «клиент» – клиент Компании, имеющий доступ к её сервисам. Может нанести урон при неправильном использовании данных сервисов, утере идентификационных данных либо действовать как первые три типа внешних нарушителей, имея доступ к информационным ресурсам, хоть и ограниченный. Наименее вероятный тип нарушителя.

Меры обеспечения безопасности

Основные меры по обеспечению информационной безопасности Компании подразделяются на:

- административно-правовые и организационные;
- физические;
- программно-технические.

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

- контроль исполнения требований законодательства Республики Казахстан и внутренних документов;
- разработку, внедрение и контроль исполнения правил, требований, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников Компании работе с информационными системами и требованиям информационной безопасности;
- реагирование на инциденты ИБ, локализацию, минимизацию последствий нарушения ИБ;
- 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 Компании.

Меры обеспечения безопасности

Меры физической безопасности включают
(но не ограничены ими):

- организацию пропускного и внутри-объектового режимов;
- построение периметра безопасности охраняемых объектов, включающего как технические средства охраны и сигнализации, так и организацию круглосуточной дежурной службы, если такая необходимость продиктована интересами Компании;
- организацию противопожарной безопасности охраняемых объектов;
- контроль доступа работников Компании в помещения ограниченного доступа.

Программно-технические меры включают процессы ИТ и ИБ
(но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра (firewall, IPS, DLP и т.д.);
- применение комплексной антивирусной защиты;
- 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 опирается на следующие *(и другие)* нормативные правовые акты Республики Казахстан и международные стандарты *(в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы обеспечения информационной безопасности Компании; в то же время существует ряд документов, который либо описывает стратегические аспекты развития ИБ на государственном уровне, либо регламентирует правила по информационной защите отдельных отраслей, направлений и видов деятельности)*:

Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;

Закон Республики Казахстан от 31 августа 1995 года № 2444 «О банках и банковской деятельности в Республике Казахстан»;

Закон Республики Казахстан от 21 мая 2013 года № 94 –V «О персональных данных и их защите»;

Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;

Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

Постановление Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах»;

Постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 30 сентября 2005 года № 359 «Об утверждении Инструкции о требованиях к наличию систем управления рисками и внутреннего контроля в банках второго уровня»;

Международный стандарт ISO/IEC 27001:2013 «Системы управления информационной безопасностью – Требования»;

Компанией неукоснительно соблюдаются требования нормативных правовых актов Республики Казахстан в сфере защиты информации, соблюдения прав интеллектуальной собственности, защиты, охраняемой законодательством, персональной информации, соблюдения ограничений по использованию криптографических средств.

При разработке и применении СОИБ учитываются требования договорных обязательств и контрактов, заключенных Компанией с третьими сторонами.

Положения настоящей Политики содержатся в должностных инструкциях работников Компании, а также в договорах на выполнение работ/предоставление услуг, заключаемых со сторонними организациями и физическими лицами, задействованными в обслуживании и эксплуатации информационной системы Компании. Доступ третьей стороны к информационным ресурсам Компании 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), Компания проводит проверку контрагентов (второй стороны заключаемых договоров) на соответствие требованиям, определенным законодательством Республики Казахстан, а также принятым в «Группе «Халык».

Благодарим за внимание!