ПОЛИТИКА
информационной безопасности
АО «Халык-Life»

ӨМІРДІ САҚТАНДЫРУ КОМПАНИЯСЫ

HALYK LIFE

КОМПАНИЯ ПО СТРАХОВАНИЮ ЖИЗНИ

Содержание

Политика информационной безопасности АО "Халык-Life" (далее – Политика) определяет цели, задачи и основные принципы построения системы управления информационной безопасностью, обеспечивающие сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в АО "Халык-Life" (далее – Компания). Также Политика излагает основные направления и требования к кибербезопасности Компании путем создания системы управления информационной безопасностью в Компании.

Положения Политики обязательны для исполнения всеми работниками Компании, а также должны доводиться до сведения иных третьих лиц, имеющих доступ к информационным системам и документам Компании, в той их части, которая непосредственно взаимосвязана с Компанией и их деятельностью. Компания обеспечивает функционирование системы управления информационной безопасностью, ее развитие и улучшение.

Политика охватывает все информационные системы и документы, владельцем и пользователем которых является Компания. Информация, циркулирующая в Компании, является одним из важнейших активов Компании. Система управления информационной безопасностью обеспечивает защиту информационных активов Компании.

Информационная безопасность Компании представляет собой состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Компании или повлечь нанесение иного ущерба Компании, ее акционерам, работникам или клиентам.

Являясь элементом общей политики управления Компанией, информационная безопасность основывается на требованиях бизнеса, разрабатывается и реализуется в соответствии с общими правилами управления рисками в Компании. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижению конкурентоспособности.

Обеспечение информационной безопасности включает в себя применение всех доступных средств и инструментов в рамках компетенции работников Компании, направленных на защиту информации и поддерживающих ее инфраструктуру.

Неотъемлемой частью организации информационной безопасности является непрерывный контроль эффективности предпринимаемых мер, определение для работников перечня недопустимых действий (бездействия), возможных последствий и ответственности.

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

При разработке и применении средств и методов информационной безопасности должны учитываться требования договорных обязательств и контрактов, заключенных Компанией с третьими сторонами.

Доступ третьей стороны к информационным ресурсам Компании осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер.

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 присущими информационным ресурсам Компании.

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 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 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 Компании;

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 Компании 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 Компании;

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

- 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 Компании 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 Компании;

- 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 Компании, 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 Компании признаются следующие элементы:

- информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Компании к тайне Компании, коммерческой тайне Компании, любая иная информация, необходимая для обеспечения нормального функционирования Компании (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 Компании, 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, помещения Компании, предназначенные для ведения закрытых переговоров и совещаний;

- персонал Компании, 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 Компании и третьим лицам, так или иначе имеющим доступ к информационным ресурсам Компании или вовлеченным в процессы информационного обмена.

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 тайну Компании, коммерческую тайну, тайну страхования Компании 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, отказа и 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 Компании и ее нормальное функционирование:

- финансовые потери, связанные с утечкой, разглашением или несанкционированной модификацией защищаемой информации;
- финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
- ущерб от дезорганизации деятельности Компании и потери, связанные с невозможностью выполнения ею 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.

Нарушители информационной безопасности классифицируются следующим образом:

- 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 или корыстных 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 клиентской и финансовой информации.

Основные типы внутренних нарушителей:

- «необученный/халатный работник» – работник Компании, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;

- «конкурирующий работник» – работник Компании, 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 Компания;

- «заинтересованный нарушитель» – работник Компании, который заинтересован в неправомерных действиях по отношении к Компании 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 (в случае заинтересованности собственной выгодой – финансовые мошенничества);

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

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

- «обиженный работник» – работник Компании, неудовлетворенный условиями 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 (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 Компании, 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 Компании. 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 Компании в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;

- «Партнер» – работник организации-партнера, имеющих 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.

Основными мерами по обеспечению информационной безопасности Компании 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 РК и внутренних документов Компании;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников Компании требованиям по работе с информационными системами в рамках 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 Компании.

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 Компании 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 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 числе привилегированных;
- применение средств криптографической защиты информации;
- обеспечение безотказной работы аппаратных средств;
- мониторинг состояния критичных элементов информационной системы;
- Организацию доступа к создаваемой, хранимой и обрабатываемой информации в информационных системах, мониторинга информации и доступа к ней.

Соответствие требованиям законодательства

Настоящая Политика и система информационной безопасности опираются на следующие нормативные правовые акты и международный стандарт (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы информационной безопасности Компании в целом):

- Закон Республики Казахстан от 18 декабря 2000 года № 126-2 «О страховой деятельности в Республике Казахстан»;

- Закон Республики Казахстан от 7 января 2003 года № 370-2 «Об электронном документе и электронной цифровой подписи»;

- Постановление Правления Национального Банка Республики Казахстан от 30 июля 2018 года № 164 «Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации»;

- Международный стандарт ISO/IEC 27001 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования».

Благодарим Вас за ознакомление
с Политикой информационной безопасности
АО «Халык-Life»!