Утверждена
решением Совета директоров
АО «КСЖ «Nomad Life»
Протокол № 300724/1 от «30» июля 2024г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «КСЖ «Nomad Life»

П-ДИТ-06

г. Алматы

ВЕДЕНИЕ

Под Политикой информационной безопасности АО «КСЖ «Nomad Life» (далее - Политика) понимается совокупность документированных управленческих решений, направленных на обеспечение информационной безопасности в информационной системе, включая бумажный и электронный документооборот и обмен речевой конфиденциальной информацией. Политика информационной безопасности представляет собой пакет документов, включающих основной документ – «Политика информационной безопасности» и документы, регламентирующие процессы обеспечения информационной безопасности, деятельность должностных лиц и пользователей информационной системы АО «КСЖ «Nomad Life» (далее – Общество).

Цель Политики – выработать и утвердить единые требования и правила, способные обеспечить надлежащую защиту информации и бесперебойную работу информационной системы Общества и свести к минимуму возможный ущерб от их эксплуатации посредством разработки эффективных превентивных и восстановительных мер противодействия угрозам информационной безопасности.

1. ОБЩИЕ НАПРАВЛЕНИЯ РАБОТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Политика разработана в соответствии с Требованиями 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, утвержденными постановлением Правления Национального Банка Республики Казахстан от 30 июля 2018 года № 164, Законом Республики Казахстан «О страховой деятельности», а также иными законодательными актами Республики Казахстан, а также внутренними документами Общества, устанавливает единые требования к порядку обеспечения защиты информации, закрепляет основные организационные решения по управлению информационной безопасностью (далее – ИБ) и определяет основные меры по защите информационных активов Общества.

1.2. Политика описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Общество в своей деятельности, определяет: должностных лиц и работников Общества, являющихся ответственными за реализацию политики ИБ и поддержание ее в актуальном состоянии, подразделения Общества, ответственные за создание и поддержание работоспособности информационных систем и системы защиты в Обществе, меры, предотвращающие нарушения режима безопасности информационных систем в случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, отключение электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия.

1.3. Требования Политики распространяются на все структурные подразделения Общества, а также работников, осуществляющих сопровождение, обслуживание и обеспечение функционирования информационной системы Общества. Политика распространяется также на другие организации и учреждения, осуществляющих взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг.

2. ОТВЕТСТВЕННОСТЬ

2.1. Ответственным за разработку и управление Политикой является Отдел информационной безопасности Общества.

2.2. Ответственность за правильное применение Политики возлагается на руководителей структурных подразделений Общества.

3. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3.1. В Политике используются следующие термины и определения:

Авторизация – определение по данным аутентификации полномочий лица или информационного ресурса и элементов, к которым им следует предоставить доступ;

Аутентификация – подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявляемых реквизитов доступа реализованными в системе;

Атака - попытка уничтожения, раскрытия, изменения, ограничения доступа, кражи, получения несанкционированного доступа или несанкционированного использования информационного актива;

Доступ - возможность использования информационных активов;

Информационная безопасность — состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры от внешних и внутренних угроз;

Информационный актив - совокупность информации и объекта информационной-коммуникационной инфраструктуры, используемого для хранения и (или) обработки информации;

Информационная система (ИС, АИС) - аппаратно-программный комплекс, предназначенный для реализации информационных процессов;

Информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

Информационные технологии - совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации;

Информационная система Общества - информационная система, в которой хранятся и обрабатываются данные Общества и его клиентов;

Информация с ограниченным распространением (служебная информация) - информация, для которой установлен специальный режим распространения, сбора, обработки и использования;

Инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов Общества;

Корпоративная сеть передачи данных - совокупность технических и аппаратно-программных средств обеспечения взаимодействия между информационными системами или между их составляющими, а также передачи электронных информационных ресурсов;

Несанкционированный доступ к информации – получение защищаемой информации, заинтересованным субъектом, с нарушением установленных правовыми документами правил доступа к ней;

Объекты информационной-коммуникационной инфраструктуры - информационные системы Общества, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

Резервная копия - копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае необходимости;

Информационно-коммуникационная инфраструктура (далее - информационная инфраструктура) - совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

Угроза информационной безопасности - совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

Обеспечение информационной безопасности - процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Общества;

Объект - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа;

Объект защиты – информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

Пользователь - субъект, обращающийся к информационной системе за получением необходимых ему информационных ресурсов и пользующийся ими;

Разграничение доступа - порядок доступа лиц к техническим и программным средствам, защищаемой информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами;

Средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, в том числе ввода или вывода, способных функционировать самостоятельно или в составе других систем;

Технологическая учетная запись - учетная запись в информационной системе, предназначенная для аутентификации между информационными системами;

Уполномоченный орган - уполномоченный орган по регулированию и развитию финансового рынка;

Ответственное лицо ОИБ - работник Отдела информационной безопасности.

3.2. В Политике применены следующие сокращения и обозначения в соответствии с таблицей 1 к Политики.

Таблица №1

№	Определения, обозначения и сокращения	Расшифровка приведенных определений, обозначений и сокращений
1	ИБ	Информационная безопасность
2	КСПД	Корпоративная сеть передачи данных
3	СП	Структурное подразделение
4	ИС	Информационная система
5	СВТ	Средства вычислительной техники
6	РГ	Рабочая группа
7	ЛВС	Локальная вычислительная сеть
8	НСД	Несанкционированный доступ
9	СКЗИ	Средство криптографической защиты информации
10	ПК	Персональный компьютер
11	ПЭВМ	Персональная электронно-вычислительная машина

12	АС	Автоматизированные системы
13	ОИБ	Отдел информационной безопасности
14	ЦОД	Специально выделенное помещение, в котором размещено серверное и коммуникационное оборудование информационной инфраструктуры Общества.

4. ТРЕБОВАНИЯ

4.1. Основные требования

4.1.1. К пользователям информационных систем ИС относятся:

4.1.1.1. работники Общества – работники, осуществляющие свою деятельность в Обществе и обладающие основными правами и обязанностями работника в соответствии с трудовым законодательством Республики Казахстан;

4.1.1.2. вспомогательный персонал - обслуживающий и технический персонал подведомственных и сторонних организаций, осуществляющих взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг. В том числе:

1) администраторы корпоративной сети передачи данных КСПД, ответственные за сопровождение телекоммуникационного оборудования;

2) системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;

3) разработчики прикладного программного обеспечения;

4) специалисты по информационной безопасности (специальных средств защиты) и др.

4.1.2 Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности информации АИС Общества и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

4.1.2.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации автоматизированных систем Общества в соответствии с действующим законодательством Республики Казахстан в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

Пользователи и обслуживающий персонал АИС Общества должны иметь представление об ответственности за нарушения в области систем автоматизированной обработки информации.

4.1.2.2. Системность

Системный подход к построению системы защиты информации в АИС Общества предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации АИС Общества.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.1.2.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

4.1.2.4. Непрерывность защиты

Защита информации – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АИС Общества, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

4.1.2.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АИС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АИС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

4.1.2.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АИС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.1.2.7. Разумная достаточность

(экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АИС, в которой эта информация циркулирует.

При достаточном количестве времени и средств возможно преодолеть любую защиту. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и

размер возможного ущерба были бы приемлемыми (задача анализа риска).

4.1.2.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.1.2.9. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

4.1.2.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах СП Общества. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

4.1.2.11. Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

4.1.2.12. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

4.1.2.13. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

4.1.2.14. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

4.1.2.15. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду

деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и соответствующую лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными работниками Общества (специалистами подразделений по безопасности).

4.1.2.16. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

4.1.3. Цели и задачи Политики информационной безопасности

4.1.3.1. Цели

Основной целью, на достижение которой направлены все пункты Политики, является надежное обеспечение информационной безопасности Общества и как следствие обеспечение конфиденциальности, целостности и доступности информационных активов Общества, защиты интересов Общества в информационной сфере.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной сети передачи данных:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование КСПД Общества;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой СВТ и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в ИС Общества и передаваемой по каналам связи.

4.1.3.2. Задачи

Для достижения указанной цели необходимо решить следующий комплекс задач:

1) развитие системы управления информационной безопасностью, позволяющей обеспечить защищенность информационной инфраструктуры Общества;

2) разработка и реализация единой технической политики в сфере обеспечения информационной безопасности ИБ, в т.ч. развитие и укрепление системы защиты информации;

3) защита прав работников и интересов Общества в информационной сфере;

4) защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Общества;

5) разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС Общества;

6) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

7) защита информации от несанкционированной модификации, искажения;

8) контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;

9) защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;

10) обеспечение авторизации и аутентификации пользователей, участвующих в

информационном обмене;

11) своевременное выявление угроз информационной безопасности ИБ, причин и условий, способствующих нанесению ущерба;

12) создание механизма оперативного реагирования на угрозы информационной безопасности ИБ и негативные тенденции;

13) создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности ИБ.

14) создание и обеспечения бесперебойной работы электронного документооборота.

15) постоянный аудит политики безопасности службой внутреннего аудита Общества не реже 1 раз в год.